Prescribed Entity and Prescribed Person Triennial Review Report

September 15, 2017

CCO Legal & Privacy Office
620 University Avenue, 15th floor
Toronto, Ontario M5G 2L7
Phone: (416) 217-1816
Fax: (416) 971-6888
Email: legalandprivacyoffice@cancercare.on.ca

Ontario
Cancer Care Ontario
Action Cancer Ontario

Table of Contents

Table of Abbreviations 4

Introduction 10

CCO's Privacy Governance Framework 13

Governance Structure 13

Operational Governance – Privacy Program Controls 17

CCO 2014 PRESCRIBED ENTITY AND PRESCRIBED PERSON TRIENNIAL REVIEW REPORT – OVERVIEW AND METHODOLOGY 23

CCO's Privacy Policy Framework 25

Part 1: Privacy Documentation 26

Privacy Documentation Matrix 26

IPC Requirements 33

Part 2: CCO's Information Security Program 50

CCO's Information Security Governance Framework 52

Security Documentation 56

Security Documentation Matrix 56

IPC Requirements 63

Part 3: Human Resources Documentation 77

Human Resources Documentation Matrix 77

IPC Requirements 79

Part 4: Organizational and Other Documentation 86

Organizational and Other Documentation Matrix 86

IPC Requirements 89

Privacy, Security and Other Indicators 95

Part 1 – Privacy Indicators 95

Part 2 – Security Indicators 112

Part 3 – Human Resources Indicators 120

Part 4 – Organizational Indicators 125

Appendix A: Current Organizational Structure for the Legal and Privacy Office 130

Appendix B: Current Organizational Structure for the Enterprise Information Security Office 131

Appendix C.1: Privacy – Log of Policy Reviews, Revisions & New Documents 132

Appendix C.2: Security – Log of Policy Reviews, Revisions and New Documents 137

Appendix D: Indicators – List of Data Linkages 146

Appendix E: Indicators – Log of Privacy Impact Assessments 148
Appendix F: Indicators – Summary from the Log of Legal & Privacy Engagement Request Forms / Privacy Service Engagement Requests 287
Appendix G: Indicators – Log of PHI Access and Privacy Audits 342
Appendix H: Indicators – Summary from the Log of Privacy Breaches 349
Appendix I.1: Indicators- Summary from the Log of Security Audits 744
Appendix I.2: Indicators – Summary from the Log of Security Incidents 751
Appendix J: Indicators – Log of Statements of Purpose 762
Appendix K: Log of Privacy Complaints 771
Appendix L: Checklist 854
Conclusion 1073
Sworn Affidavit 1074
Appendix i – Supporting Documentation 1075
Appendix ii - Supporting Tools 1090

Table of Abbreviations

A&I	Analytics & Informatics
ACCU	Aboriginal Cancer Control Unit
ADT	Admission Discharge and Transfer
AHAC	Aboriginal Health Access Centre
ALC	Alternate Level of Care
ALR	Activity Level Reporting
ATC	Access to Care
BN	Briefing Note
BRD	Business Requirement Document
CAPE	Client Agency Program Enrolment
CBCRP	Case-by-Case Review Program
CC	CSP Contact Centre
CCAC	Community Care Access Centre
CCC	Colon-Cancer-Check
CCO	Cancer Care Ontario
CHDB	Claims History Database
CIHI	Canadian Institute for Health Information
CIRT	Colonoscopy Interim Reporting Tool
CKD	Chronic Kidney Disease
CPDB	Corporate Provider Database
CPO	Chief Privacy Officer
CPQI	Clinical Programs and Quality Initiatives
CPSO	College of Physicians and Surgeons of Ontario
CRM	Customer Relationship Management
CSR	Client Services Representative
CSP	Cancer Screening Program (formerly known as ICS)

CTO	Chief Technology Officer
DDSC	Data Disclosure Subcommittee
DAD	Discharge Abstract Database
DAP	Diagnostic Assessment Program
DAP-EPS	Diagnostic Assessment Program – Electronic Pathway Solution
DDUT	Diagnostic Data Upload Tool
DOB	Date of Birth
DSA	Data Sharing Agreement
EB-PET	Positron Emission Tomography Scan Evidence-Based Program
EBP	Evidence Building Program
EDW	Enterprise Data Warehouse
EISO	Enterprise Information Security Office
EISP	Enterprise Information Security Program
EMPI	Enterprise Master Patient Index
EMRs	Electronic Medical Records
EPIC	Expanded Prostate Cancer Index
ePREM	Electronic Patient Reported Experience Measure
ERM	Enterprise Risk Management
ERNI	Emergency Room National Ambulatory Reporting System Initiative
ET	CCO's Executive Team
FAQs	Frequently Asked Questions
FH	Fulfillment House for CSP
FHT	Family Health Team
FIT	Fecal Immunochemical Test
FIPPA	*Freedom of Information and Protection of Privacy Act*
FOBT	Fecal Occult Blood Test
HIC	Health Information Custodian
HIN	(Ontario) Health Insurance Number

HINP	Health Information Network Provider
HL7	Health Level 7
ICMS	Integrated Client Management System
ICR	Interval Cancer Review
ICSP	Integrated Cancer Screening Program (former name of the CSP)
ID	Identification
IDAR	Internal Data Access Request
IM	Information Management
IM/IT	Information Management and Information Technology
IPC	Information and Privacy Commissioner/Ontario
ISAAC	Interactive Symptom Assessment and Collection
IT	Information Technology
ITCS	IT Change Subcommittee
ITIL	IT Infrastructure Library
LHIN	Local Health Integration Network
LMAS	Logging, Monitoring, and Auditing System
LPER	Legal & Privacy Engagement Request
LPO	Legal & Privacy Office
LRA	Local Registration Authority
LRT	Laboratory Reporting Tool
LTC	Long-Term Care
LTCH	Long-Term Care Home
Manual	*Manual for the Review and Approval of PPs and PEs*
MCC	Multidisciplinary Cancer Conference
MD	Doctor
MDSA	Master Data Sharing Agreement
MFT	Managed File Transfer
MHA	Mental Health and Addictions

MMs	Mammograms and Mammogram Reports
MOHLTC	Ministry of Health and Long-Term Care
MOU	Memorandum of Understanding
MRI	Magnetic Resonance Imaging
MRN	Medical Record Number
NACRS	National Ambulatory Care Reporting System
NDFP	New Drug Funding Program
OACCAC	Ontario Association of CCACs
OBIEE	Oracle Business Intelligence Enterprise Edition
OBSP	Ontario Breast Screening Program
OCR	Ontario Cancer Registry
OCRAT	Online Cancer Risk Assessment Tool
OCRIS	Ontario Cancer Registry Information System
OCSMC	Ontario Cancer Symptom Management Collaborative
OCSP	Ontario Cervical Screening Program
OCSR	Ontario Cancer Screening Registry
ODB	Ontario Drug Benefit
ODDAR	Online Direct Data Access Request (the former version of IDAR)
OICR	Ontario Institute for Cancer Research
OLIS	Ontario Laboratories Information System
OOC	Out-of-Country
OPDP	Ontario Provincial Drug Programs
OPIS	Oncology Patient Information System
ORN	Ontario Renal Network
O.Reg.	Ontario Regulation
ORRS	Ontario Renal Reporting System
P&CC	Prevention and Cancer Control
P&RP	Planning and Regional Programs

PAF	Personnel Action Form
PCCIP	Prevention & Cancer Control Information Program
PCP	Primary Care Provider/Physician
PDRP	Provincial Drug Reimbursement Program
PE	Prescribed Entity
PEM	Patient Enrolment Model
PET	Positron Emission Technology
PHI	Personal Health Information
PHIPA	*Personal Health Information Protection Act, 2004*
PI	Personal Information
PIA	Privacy Impact Assessment
PIMS	Pathology Information Management System
PMH	Princess Margaret Hospital
PNAW	Privacy Needs Assessment and Work plan
PP	Prescribed Person
PSC	People, Strategy and Communications
PSER	Privacy Services Engagement Request
QA	Quality Assurance
QMP	Quality Management Partnership
RAI	Resident Assessment Instrument
RBIL	Regional Breast Imaging Lead
RCC	Regional Cancer Centre
RD	Regional Director
REB	Research Ethics Board
RFC	Request for Change
RFP	Request for Proposals
RMP	Risk Mitigation Plan
RPDB	Registered Persons Database

SAR	Screening Activity Report
SAS	Statistical Analysis System
SCT	Stem Cell Transplant
SDM	Substitute Decision-Maker
SEER*Stat	Surveillance, Epidemiology, and End Results Statistical
SETP	Surgical Efficiency Targets Program
SNMP	Simple Network Management Protocol
SOWG	Security Operations Working Group
SQL DB	Structured Query Language Data Base
Sr.	Senior
SRI	Sunnybrook Research Institute
SSO	Specialized Services Oversight
SSOIS	Specialized Services Oversight Information System
STIP	Systemic Treatment Information Program
STFM	Systematic Treatment Quality-Based Procedure Funding Model
TRA	Threat Risk Assessment
UHN	University Health Network
VA	Vulnerability Assessment
VIP	Very Important Person
WTIS	Wait Times Information Strategy/System

Introduction

Cancer Care Ontario (**CCO**) is the provincial agency responsible for continually improving cancer and chronic kidney disease (CKD) services and acts as the Ontario Government's advisor on cancer and renal systems. Formally launched and funded by the Ontario government in 1997, CCO is governed by the Ontario *Cancer Act* and the *Corporation Act*. Further, as an Operational Service Agency of the Ontario government, CCO's mandate is determined pursuant to a Memorandum of Understanding (**MOU**) between CCO and the Ministry of Health and Long-Term Care (**MOHLTC**) dated December 2, 2009, however, an agreement is under negotiation and will supersede the current version of the MOU.

In furtherance of its mandate CCO:

- Directs and oversees public health care dollars to hospitals and other cancer care providers to deliver high quality, timely cancer services;
- Implements provincial cancer prevention and screening programs designed to reduce cancer risks and raise screening participation rates;
- Works with cancer care professionals and organizations to develop and implement quality improvements and standards;
- Uses electronic information and technology to support health professionals and patient self-care and to continually improve the safety, quality, efficiency, accessibility and accountability of cancer services;
- Plans cancer services to meet current and future patient needs, and works with health care providers in every Local Health Integration Network (**LHIN**) to continually improve cancer care for the people they serve; and
- Rapidly transfers new research into improvements and innovations in clinical practice and cancer service delivery.

In addition to cancer, CCO has other core lines of business including supporting and hosting the provincial Access to Care (**ATC**) program, which is a part of the Government of Ontario's Wait Times Information Strategy (**WTIS**). In 2015, the MOHLTC assigned ATC with the task of developing and implementing a provincial electronic triage system. The electronic Canadian Triage and Acuity Scale (**eCTAS**) system will support triage nurses to assess and prioritize patients requiring urgent care in a standardized manner according to the eCTAS guidelines.

In 2010, the MOHTLC formally transferred the provincial oversight and co-ordination of the **CKD** Management Program to the Ontario Renal Network (**ORN**) under the auspices of CCO. As part of this process, CCO entered into an accountability agreement with the MOHLTC dated January 29, 2010 in order for CCO to establish, manage and coordinate the ORN as a work unit within CCO and to support the growth of CKD services across Ontario.

CCO also administers the Provincial Drug Reimbursement Program (**PDRP**), which includes the New Drug Funding Program (**NDFP**), the Evidence Building Program (**EBP**), and the Case-by-Case-Review Program (**CBCRP**) for cancer drugs, on behalf of the MOHLTC. Beyond CBCRP, CCO has developed the Out-of-Country (**OOC**) program, which it administers on behalf of the MOHLTC, in order to enhance timeliness, consistency, and quality of decision-making; ensure decisions are being guided by best evidence; reduce inappropriate requests, and support patient access to treatments/services offered outside of Ontario or Canada. The program also supports integration and introduction of new cancer programs/services into Ontario.

Each of these programs are governed by Master Accountability Agreements between CCO and the MOHLTC.

In order to fulfill its mandate, CCO requires access to personal health information (**PHI**) from across Ontario. CCO derives its authority to collect, use, and disclose this information from its designations under the Ontario *Personal Health Information Protection Act, 2004* (**PHIPA**).

Prescribed Entity

Subsection 45(1) of PHIPA permits health information custodians (**HIC**) to disclose PHI without consent to prescribed entities for the purpose of analysis or compiling statistical information with respect to the management, evaluation or monitoring of the allocation of resources to or planning for all or part of the health system, including the delivery of services ("health system planning and management purposes"), provided the prescribed entities meet the requirements of subsection 45(3).

CCO is designated as a 'prescribed entity' for the purposes of subsection 45(1) of the Act, under subsection 18(1) of Ontario Regulation (**O.Reg**.) 329/04 (**Prescribed Entity or PE**). Many of CCO's programs operate under its Prescribed Entity authority. In this capacity, CCO collects PHI from health care organizations that are directly involved in the care and treatment of patients and from government institutions and agencies, such as the MOHLTC or the Canadian Institute for Health Information (**CIHI**), for health system planning and management purposes.

Prescribed Person

CCO is also designated as a 'prescribed person' under subsection 39(1)(c) of PHIPA with respect to its role in compiling and maintaining screening information for colorectal, cervical and breast cancer in the Ontario Cancer Screening Registry (**OCSR**) under subsection 13(1) of O.Reg. 329/04 (**Prescribed Person or PP**). This designation grants CCO the authority to collect, use and disclose PHI for the purposes of facilitating or improving the provision of health care with respect to colorectal, cervical and breast cancer.

The cancer screening program (**CSP**) encompasses CCO's Colon-Cancer-Check (**CCC**), Ontario Breast Screening Program (**OBSP**) and Ontario Cervical Screening Program (**OCSP**). As a PP, CCO has the authority to collect, use and disclose PHI for the purpose

of facilitating or improving the provision of breast, cervical and colorectal cancer screening services and care for Ontarians. The CSP mandate includes:

- Identification of the target screening population for each type of cancer (breast, cervical and colorectal);
- Inviting the identified population to engage with their primary care provider (**PCP**) to discuss screening;
- Notifying participants who are screened of their test results; and
- Communicating with program participants when it is time to be re-screened.

All three screening programs are fully operational and have been integrated into the existing screening infrastructure. The CCC program was launched in 2008. The OCSP was launched in September 2013 and the OBSP was launched in March 2014.

The privacy practices for the screening programs were reviewed and approved by the Information and Privacy Commissioner of Ontario (**IPC**) in 2008, 2011 and 2014.

All three screening programs have robust privacy controls embedded within the administrative, processing and technical infrastructure. The collection, use and disclosure of PHI by the screening programs has been assessed in a number of privacy impact assessments (**PIA**s) conducted for each of the screening programs.

PE and PP Triennial Review

Subsection 45(3) of PHIPA requires each PE to have in place practices and procedures to protect the privacy of individuals whose PHI it receives and to maintain the confidentiality of that information. Subsection 45(3) further requires each PE to ensure that these practices and procedures are approved by the IPC on a triennial basis in order for HICs, and other persons authorized under PHIPA, to disclose PHI to the PE without consent and for the PE to collect, use and disclose such PHI, as permitted under PHIPA and O.Reg. 329/04. CCO's privacy practices and procedures must be reviewed by the IPC every three years from the date of their initial approval.

Similarly, subsection 13(2) of O. Reg. 329/04 requires each PP to have in place practices and procedures to protect the privacy of the individuals whose PHI it receives and to maintain the confidentiality of that information. Subsection 13(2) further requires each PP to ensure that these practices and procedures are approved by the IPC on a triennial basis in order for HICs, and other persons authorized under PHIPA, to disclose PHI to the PP without an individual's consent.

The first three-year approval of CCO's practices and procedures as a PE was received from the IPC effective November 1, 2005. CCO had its status renewed by the IPC on October 31, 2008, October 31, 2011 and on October 31, 2014 for additional three-year terms, respectively. This report constitutes CCO's submission to the IPC for the 2017 approval process in respect of its PE and PP roles.

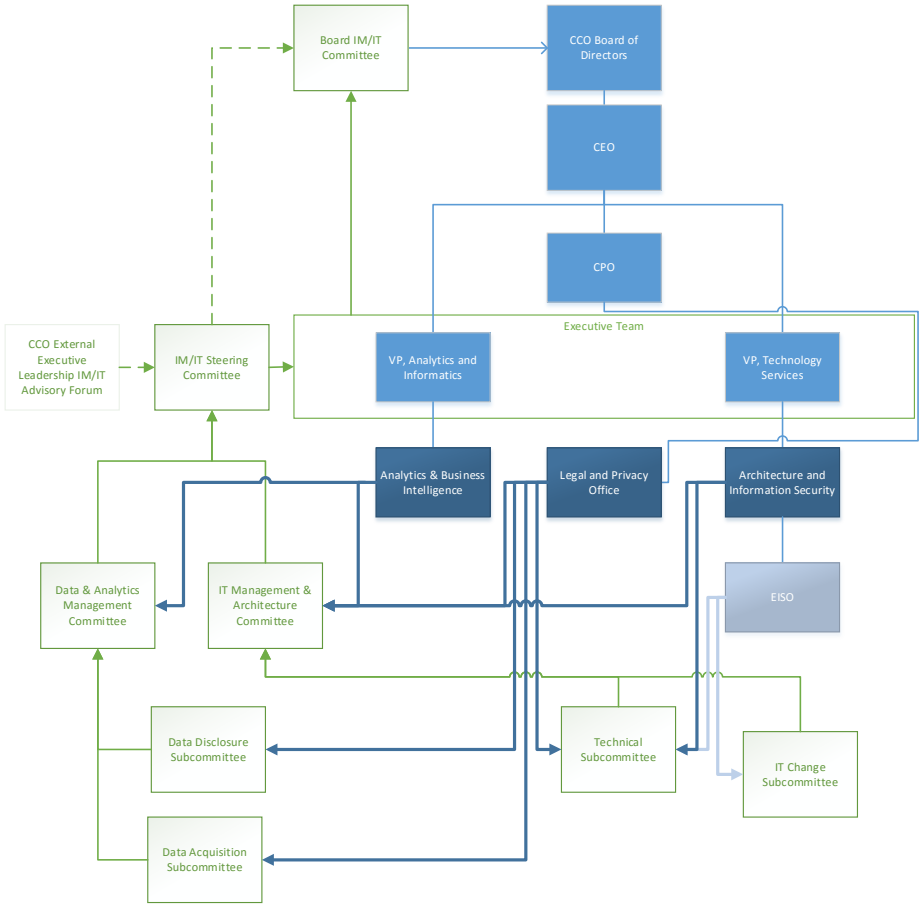
CCO's Privacy Governance Framework

The CCO Privacy Governance Framework (**Framework**) is a core element of CCO's privacy program. The Framework is designed to give effect to CCO's Privacy Policy ("**CCO's Privacy Policy**") and, more generally, to its commitment to privacy. The Framework enables the effective integration and coordination of CCO's Legal & Privacy Office (**LPO**), policies, and programs with the organization as a whole.

Governance Structure

CCO's privacy governance structure informs its overall privacy management practices, including leadership, strategy, priorities and risk management. The privacy governance structure provides assurance that the strategies, policies, standards, processes and resources to manage privacy risks are aligned with CCO's objectives and are consistent with applicable laws, standards and best practices. The chart below sets out how privacy governance is organized at CCO, followed by more detail about key aspects of the governance structure

Figure 1 - Privacy and Security Governance Structure



CCO Board of Directors

CCO's accountability for sound privacy governance practices resides at the highest level of the organization, its Board of Directors (**Board**).

The Corporate Governance Nominating Committee of the Board receives an Annual Privacy Report on privacy matters including new initiatives, privacy audits and PIA**s** undertaken by the LPO, the results of the privacy audits and PIAs as well as the number and type of privacy breaches and complaints investigated.

The Chief Privacy Officer (**CPO**) (who is also CCO's General Counsel), also provides the Board with relevant information on privacy matters as required, any significant privacy breaches, privacy audit reports, new privacy legislative, regulatory and industry developments of note, and the status of the IPC's triennial review and any recommendations arising therefrom.

CCO maintains an up-to-date enterprise risk register that is reported on semi-annually to the Board. The Board receives regular briefings or progress reports on the status of mitigating actions and any applicable risk issues, including privacy and information security issues and reviews and approves the enterprise risk register, including all privacy and information security risks therein, semi-annually.

*Executive Team (**ET**)*

The CCO ET supports and champions the privacy program at CCO, actively advocating a privacy respectful culture. The ET is briefed on privacy matters as required by the CPO, and at least annually, through the Annual Privacy Report.

CPO

Accountability for privacy compliance with PHIPA and with CCO policies, at the operational level, ultimately resides with CCO's President and CEO. This function has been formally delegated to CCO's CPO who is accountable to the President and CEO. The CPO is able and expected to provide privacy representation on the most senior decision-making bodies within CCO. The CPO also acts as Head under the Ontario *Freedom of Information and Protection of Privacy Act* (**FIPPA**), under delegation of authority of the Board Chair.

The CPO oversees the day-to-day operations of the privacy program through the Director, Legal & Privacy, and provides recommendations on all enterprise-level privacy-related policy decisions.

Director, Legal & Privacy

The Director, Legal & Privacy manages the LPO and reports directly to the CPO. The Director, Legal & Privacy is supported by the Group Manager, Privacy. The Director, Legal & Privacy is specifically responsible for:

- Managing the day-to-day operations of CCO's privacy program;

- Ensuring that Business Unit Managers establish, implement, monitor and assess privacy program controls on an ongoing basis;
- Overseeing the provision of privacy advice and support to all business functions;
- Ensuring that the suite of privacy policies is comprehensive, up-to-date and compliant with applicable law and standards;
- Overseeing the development and provision of privacy training;
- Advocating for privacy within the organization;
- Ensuring high quality and consistent privacy reviews, audits/compliance monitoring, and benchmarking, are conducted as appropriate and in accordance with CCO's policies and procedures;
- Ensuring that appropriate vendor management and other privacy-related agreements are in place as required;
- Overseeing the management of access to information requests; and
- Monitoring legal and other developments in the privacy arena.

LPO

The Privacy Group within the LPO is comprised of the Director, Legal & Privacy; the Group Manager, Privacy; Privacy Managers and Privacy Specialists. The complete organizational structure for the LPO is set out in *Appendix "A".* The LPO has been designed to enable the establishment, maintenance and monitoring of a privacy program that meets PHIPA and FIPPA requirements and other key privacy drivers. More specifically, the LPO has the following privacy objectives:

- Build a culture of privacy within the organization;
- Deliver privacy-advisory services across CCO; and
- Ensure CCO's compliance with privacy legislation and policies.

The LPO meets these objectives through its close ties to the Business Units and programs at CCO. Every Business Unit at CCO has an assigned Privacy Manager or Specialist, who meets regularly with each Business Unit Manager to discuss business initiatives and associated privacy needs and challenges which are reported to the Group Manager, Privacy.

The LPO is supported by the ET at CCO, all of whom champion privacy within their respective divisions. The LPO is further supported by:

- Information governance partners, including the:
    - Enterprise Information Security Office (**EISO**);
    - Architecture Services; and
    - Analytics & Informatics (**A&**I) Division.

- Information Management (**IM**) /Information Technology (**IT**) governance committees.

Information Governance Partners

Information governance at CCO falls jointly with the LPO, the Architecture and Information Services Department, which houses the EISO and Architecture Services, and the A&I Division. Each of these departments have their own set of responsibilities as described below, however they also have significant points of intersection with respect to protecting PHI and personal information (**PI**) held by CCO.

- EISO provides a leadership role in defining policies, process and safeguards (administrative, technical and physical) aimed at protecting CCO's information assets, meeting regulatory obligations and achieving business objectives.

- Architecture Services establishes and implements technical standards that facilitate CCO in meeting its business objectives.

- The A&I Division leads CCO's data collection, reporting and analytics capabilities. This Division ensures that data is managed following precise standards and business rules, which align with CCO's privacy requirements.

Effective communication and integration between these departments is vital to successful information governance at CCO. Consequently, these departments meet at least monthly to review and monitor CCO IM policies, procedures and practices. They also provide consultation and advice related to: (i) the triennial review by the IPC; (ii) the implementation of recommendations or orders by the IPC; (iii) privacy and security breach management, and (iv) other IM initiatives.

The Architecture and Information Security Services Department, A&I Division, and the LPO have created an information governance structure to facilitate CCO in complying with CCO's privacy policies, privacy legislation and regulation, and privacy best practices. This structure includes Information Management and Information Technology (**IM/IT**) governance committees described below that have representation from all three departments.

IM/IT Governance Committees

CCO's IM/IT governance is provided through a number of committees that facilitate CCO in achieving its strategic goals through the use of IM/IT. Through these committees,

CCO's information governance partners provide oversight for IM/IT solutions and services to ensure that:

- Established processes and technology for data privacy and security are in place;
- Privacy and security risks are identified; and
- New controls are identified and implemented to address these risks as required.

As part of these committees, requests for the disclosure of CCO data, including PHI for the purpose of research studies, are reviewed by privacy members of the LPO to ensure PHI disclosures are compliant with PHIPA and *CCO's Data Use & Disclosure Policy*. The Committees include:

- IM/IT Steering Committee
- Data & Analytics Management Committee
- Data Disclosure Subcommittee (**DDSC**)
- Data Disclosure Working Group
- IT Management and Architecture Committee
- Technical Subcommittee
- IT Change Management Committee

Operational Governance – Privacy Program Controls

The following constitute CCO's key privacy program controls:

(i) *Policies, Standards, Procedures and Guidelines*

CCO's privacy policies set the tone for, and approach to, its privacy management practices. These policies communicate, at a high level, the goals and directions set by the Board and the ET and the general means by which these goals will be achieved. The privacy policies are an extension of the governance structure, setting out the overall accountability for privacy. Certain policies, standards, procedures and guidelines also set the controls and specific means by which CCO will meet: (i) the commitments set out in the *CCO's Privacy Policy*; (ii) privacy legislative and regulatory requirements; and (iii) other goals in relation the protection of PHI and PI. To continue to meet these purposes, the privacy policies and supporting standards, procedures, and guidelines are reviewed regularly and revised as necessary following risk assessments, regulatory recommendations or orders, in response to a breach or complaint, new guidance, or changes to industry-based best practices. Following CCO's last IPC Triennial Review in 2014, the LPO has reviewed a number of its policies, standards and procedures and made amendments where necessary. The amendments to policies, standards and

procedures are noted as an indicator in the "Privacy Indicator" section of this report.

(ii) *Projects, Program and Process Change Controls*

Privacy assurance and risk management are core services provided by the LPO to ensure that project, program and process changes comply with applicable privacy legislation and CCO's privacy policies. The LPO provides the following services to support privacy assurance and risk management: (i) develop privacy risk management plans (**RMPs**) for projects/initiatives; (ii) contribute to business requirement and architecture documents; (iii) review Legal & Privacy Engagement Request Form (**LPER**); (iv) conduct PIAs; (v) draft data sharing agreements (**DSA**s); (vi) provide procurement support; (vii) provide input into communication materials; and (viii) standard operating procedures.

All initiatives or changes to existing programs, projects or processes are required to submit a *Legal & Privacy Engagement Request Form*, which allows the LPO to determine the type of privacy services that are required to support the initiative, if any. Accordingly, the LPO can ensure that the necessary privacy controls are built into programs and projects. The single, streamlined request format facilitates the engagement of the LPO and better ensures that privacy issues are identified. The LPO is also engaged at checkpoints throughout the project gating lifecycle, applicable to larger IM/IT projects. Both of these processes ensure that projects or programs are analyzed and assessed for privacy risk and permit the inclusion of privacy mitigating steps in the project or program design stage.

A PIA provides a framework to ensure that privacy is considered throughout program or system design. In accordance with CCO's *Privacy Impact Assessment Standard*, a PIA is conducted when material changes are made to an existing program or system, or when a new program or system that will collect PHI or PI is developed. A PIA highlights any privacy risks associated with a program or system and, where required, details mitigating strategies and an action plan. An Addendum to a PIA is conducted to assess changes to existing programs or information systems for which a PIA has already been conducted, but where the proposed changes are found to be minor and there are no identified changes to the legislative authority.

Privacy RMPs are embedded within the IM/IT Gating Process to ensure that projects with an IM/IT component are considered by the LPO for compliance, authority to collect, use and/or disclose the data required, and to ensure that appropriate privacy controls are in place.

(iii) *External Requests – Controls that Limit Access*

External requests for CCO data may be made by the public. The *Research Data Request Form* is used for requests for data for *research studies*. Requests for data for other purposes may be made on the *General Data Request Form*. Forms

must be signed by the Primary Investigator and submitted to CCO's IM Coordinator. The request is then reviewed by the Data Disclosure Working Group, which is comprised of research, privacy and data subject matter experts. The Working Group recommends the request for approval/denial, or requests further information to make a recommendation. The final recommendation is reviewed, discussed and approved by the DDSC at CCO. Copies of the *Data Use & Disclosure Policy* are available by request from the IM Coordinator and also from CCO's website.

Access to and use of PHI and PI is also governed by comprehensive confidentiality agreements, research agreements, DSAs and other similar agreements, as applicable.

(iv) *Inventory of Data Holdings*

CCO maintains a central, online repository which describes all CCO data holdings, both PHI and non-PHI. The Data Catalogue provides a single location for obtaining information about CCO data, including associated programs and subjects, data start and end dates.

(v) *Technical and Physical Safeguards*

In order to protect PHI and PI, the LPO works in close partnership with the EISO and Architecture Services to ensure the integrity, availability and confidentiality of PHI as well as to ensure that technical specifications align with regulatory requirements.

(vi) *Training and Awareness*

The LPO provides ongoing privacy communications and training to maintain a culture of privacy across the organization. There are three components to the LPO training program, including:

- In-person privacy training for new employees;
- Core privacy and security training eLearning curriculum for new employees; and
- Annual privacy & security refresher training eLearning curriculum.

Privacy and security training is mandatory for new employees, including service providers with access to PHI, students, researchers and others with access to CCO systems. Individuals must complete the new-employee training before being provisioned with access to PHI. The new-employee training, delivered through an in-person session and a web-based component, covers the following topics:

- Governance structure of the LPO
- CCO's obligations under PHIPA and FIPPA
- Privacy and security requirements, best practices and frequently asked questions (**FAQs**)
- Services offered by the LPO

- Important terms, such as ‘PHI’ and ‘privacy breach’
- Examples of privacy breaches and how to contact the LPO in the event of a real or suspected privacy breach or incident

Annual web-based refresher training is also mandatory for CCO employees. If a CCO employee does not complete the refresher training by the stated due date they will have their access to CCO’s systems revoked.

When individuals complete the mandatory or refresher web-based training they are required to read and digitally accept the *Privacy and Security Acknowledgement Form* to acknowledge that they understand *CCO’s Privacy Policy* and the *Information Security Code of Conduct & Acceptable Use Policy* as well as completed and understood the Core Privacy & Security Training eLearning Curriculum. The form also includes terms relating to access, use and disclosure of PHI during the individual’s employment or affiliation with CCO.

(*vii)* *Breach Management*

Another important component of the LPO is the identification, management, investigation and resolution of privacy breaches that occur as a result of the misuse or improper/unauthorized collection, use, retention, disclosure or disposal of PHI in CCO’s custody or control. CCO policies stipulate that it is mandatory for employees, and third parties working under contract with CCO, to report all privacy breaches or suspected privacy breaches to the LPO. Employees and third parties are trained on what constitutes a privacy breach through CCO’s privacy and security training program and they are made aware of each individual’s responsibility for reporting a breach or suspected breach.

The CCO *Privacy Breach Management Procedure* was amended in 2016. The Procedure has been split into two distinct components, the *Privacy Breach Management Policy* and the *Privacy Breach Management Manual*. The *Privacy Breach Management Manual* includes step by step procedures to investigate, notify and mitigate privacy breaches.

(viii) *Vendor Management*

The LPO is engaged in the procurement process for every requested procurement that may involve the use or disclosure of PHI or PI to ensure that CCO only selects and retains service providers that are capable of appropriately safeguarding PHI and PI and that CCO has in place appropriate contractual controls in relation to the service provider’s overall privacy practices. Embedded within the eProcurement Tool, the Procurement Privacy and Security Intake form must be completed, along with a Procurement PIA, prior to the business unit receiving approval and moving forward with their requested procurement.

Where PHI or PI will be used or disclosed, a Privacy Manager or Specialist will work with the requesting business unit to ensure that appropriate controls are in

place through a variety of mechanisms, including specific privacy requirements for vendors within the Request for Proposals (**RFPs**), involvement in the selection of vendors, privacy and security training of vendors, and the signing of confidentiality agreements. In addition, all third-parties that handle PHI or PI on behalf of CCO must agree to CCO's third-party privacy schedule (*Principles and Procedures for the Provision and Use of Personal Information and Personal Health Information*), which includes requirements to comply with CCO's privacy policies.

(ix) *External Communication & Transparency*

CCO has a privacy page on its external website that outlines CCO's commitment to and obligations in respect of privacy as well as the means by which CCO fulfills that commitment. CCO is currently in the process of updating its external website including the privacy content. This update is expected to be completed by early 2017. CCO maintains the following documents on its public website:

- CCO's Privacy Policy;
- FAQs related to its privacy policies, procedures and practices;
- A list of the data holdings of PHI that CCO maintains;
- CCO's *Statement of Information Practices;*
- Contact information for the LPO for inquiries;
- Information about the CCO's approval status based on the IPC triennial review and the contact information for the IPC;
- Program-specific privacy information, where necessary to clarify privacy practices related to a specific initiative; and
- Most current *Annual Privacy Reports.*

(x) *Privacy and Information Security Risk Management*

CCO's *Privacy and Information Security Risk Management Procedure* defines the approach by which CCO identifies, assesses, treats and monitors privacy and information security risks. This procedure establishes a foundation for mitigating and managing privacy and information security risks and sets the boundaries for risk-based decisions in respect of privacy and security within CCO. This procedure is designed to assist CCO business units in meeting their obligations under CCO's *Enterprise Risk Management Framework* through the proper identification, assessment and treatment of privacy and information security risks.

Together, the *Enterprise Risk Management Framework* and the *Privacy and Information Security Risk Management Procedure* provide CCO with a comprehensive process to: (i) manage privacy and information security risks; and (ii) document the roles and responsibilities of CCO staff, management and Board members in identifying, assessing, treating and monitoring privacy and information security risks.

Through the implementation of the *Privacy and Information Security Risk Management Procedure*, the assessment of privacy and information security risks are embedded in privacy and information security deliverables and are centrally logged in the privacy and information security risk registers.

Status of the CCO 2014 Prescribed Entity and Person Triennial Review Recommendations

The IPC's 2014 triennial review of CCO's practices and procedures resulted in 2 recommendations, both of which apply to CCO's role as a PE and PP. The following charts provide:

- a detailed description of the recommendations;
- the manner in which the recommendations have been addressed or will be addressed; and
- the status of each recommendation.

Figure 2 Status of 2014 IPC Recommendations

2014 IPC Compliance Recommendation	CCO Enhancement	Status		Expected Date of Completion
		Complete	In Progress	
PE and PP				
1. It is recommended that CCO ensure that its reporting of indicators, especially as related to privacy complaints and security audits, are provided in full compliance with the *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities ("Manual")* at the start of the next review period.	CCO has updated the Privacy Complaints Log and Security Audit Log to meet the requirements as noted in the IPC Manual. The Log is attached in *Appendix "I"* and *Appendix "K"*.	✓		
2. It is recommended that CCO provide to the IPC, no later than December 31, 2014, indicators which are complete up to and including October 31, 2013, in compliance with the IPC Manual.	CCO provided indicators complete up to and including October 31, 2013 to the IPC in December 2014.	✓		

CCO 2014 PRESCRIBED ENTITY AND PRESCRIBED PERSON TRIENNIAL REVIEW REPORT – OVERVIEW AND METHODOLOGY

The Manual for the Review and Approval of Prescribed Persons and Prescribed Entities (**Manual**) was developed by the IPC for the following purposes:

- to outline the process to be followed by the IPC in reviewing the practices and procedures implemented by PPs and PEs , such as CCO, to protect the privacy of

individuals whose personal health information they receive and to maintain the confidentiality of that information..

- to set out the obligations imposed on PPs and PEs and that it is the responsibility of the PPs and PEs to ensure continued compliance with the Manual.

The Manual states that PPs and PEs must ensure their practices and procedures include the policies, procedures, agreements and documentation set out in *Appendix "A" - List of Required Documentation*, of the Manual, and contain the minimum content set out in *Appendix "B" - Minimum Content of Required Documentation*. In order to verify if CCO has developed and implemented all requirements set out in the Manual, a written report and sworn affidavit will be submitted to the Commissioner.

The LPO undertook the review of CCO's procedures and practices along with other supporting departments. The LPO added further detail to the comprehensive reference checklist that it had created in 2008 based on the full requirements outlined in the Manual for the purposes of creating a tracking mechanism for each requirement. This checklist is included as Appendix L. Process improvements, organizational changes, and technological upgrades had changed some of CCO's practices and resulted in new policies and procedures. There were multiple stages of the review process; the main stages of the review process can be broken down as follows:

i. *Engaging departments* – The LPO engaged departments across CCO and provided them a full briefing on the scope of the review, the IPC requirements in terms of documentation/logs concerning their program area and timelines.

ii. *Document collection and checklist reconciliation* – All relevant documentation was gathered, reviewed and compared against the requirements set out in the checklist and Manual.

iii. *Policy drafting* – Where the documentation could more explicitly meet a requirement, minor amendments were made or new documents were developed.

iv. *Report drafting* – The final CCO 2017 PE and PP Triennial Review Report was drafted and finalized, after all of the requirements were reviewed and responded to.

The structure of the CCO 2017 PE and PP Triennial Review Report follows the *List of Required Documentation* provided in *Appendix "A"* of the Manual. The Report is presented in a table format, wherein each required document listed in *Appendix "A*" is organized in a separate table. It is recommended that this report be reviewed along with the Manual, as requirements have not been duplicated verbatim in this report.

As noted in the Manual, each requirement includes a minimum set of criteria or content, as provided in *Appendix "B"* of the Manual. CCO complies fully with every applicable requirement, and all documents which meet the criteria of that requirement are listed. A quick matrix grid has been included to highlight CCO's compliance to the IPC requirements by mapping each requirement to the appropriate CCO documentation or tool.

The Privacy, Security, Human Resources and Organizational Indicators, as outlined in *Appendix "C"* of the Manual, are reported within a separate table. An explanation is provided if certain indicators are not reported on and, where appropriate, the measures to be implemented to permit future reporting of such indicators.

Lastly, a list and summary of all CCO documents and tools that were reviewed as part of this exercise has been included in the appendices of this report.

CCO's Privacy Policy Framework

The ability of the LPO to fulfill its commitment to respecting personal privacy, safeguarding confidential information, and ensure the security of PHI within its custody or control, is supported by EISO and the Human Resources, Facilities, Legal and Strategic Sourcing departments within CCO. This Privacy Policy Framework as described in the matrices set out in each part below demonstrates this interconnectivity between these groups, as illustrated through the policies, standards, procedures and guidelines that support Privacy's initiatives. Moreover, it shows the depth and collaboration within CCO as the LPO works towards fulfilling its commitment.

The Privacy Policy Framework follows a tiered approach with enterprise policies at the top. Each subordinate tier draws its authority from a higher tier, whereby the subordinate tiers support the higher tiers by providing additional detail but not establishing conceptually new principles, requirements or responsibilities. Policies are formal, brief and high-level statements or plans that embrace an organization's general beliefs, goals and objectives. Standards are mandatory actions or rules designed to support and conform to a policy. Procedures are a series of steps taken to accomplish an end goal. Guidelines consist of recommended, non-mandatory controls or instructions.

Please see *Appendix "I" – Supporting Documentation*, where supporting documentation referenced in the Report has been summarized.

Part 1: Privacy Documentation

Privacy Documentation Matrix

CCO Privacy Matrix	Requirement 1	Requirement 2	Requirement 3	Requirement 4	Requirement 5	Requirement 6	Requirement 7	Requirement 8	Requirement 9	Requirement 10	Requirement 11	Requirement 12	Requirement 13	Requirement 14	Requirement 15	Requirement 16	Requirement 17	Requirement 18	Requirement 19	Requirement 20	Requirement 21	Requirement 22	Requirement 23	Requirement 24	Requirement 25	Requirement 26	Requirement 27	Requirement 28	Requirement 29	Requirement 30	Requirement 31	Requirement 32	Requirement 33
Annual Privacy Report			**x**																														
Application for Disclosure of Information from CCO for Research Purposes													**x**	**x**																			
Business Process for Data Requests												**x**	**x**											**x**									
Cancer Screening Privacy Frequently Asked Questions			**x**																														
CCO Procurement Policy																			**x**														
CCO's Internal Direct Access Request on-line tool									**x**																								
CCO's Privacy Policy	**x**	**x**	**x**	**x**		**x**	**x**	**x**								**x**	**x**	**x**	**x**					**x**	**x**		**x**		**x**	**x**	**x**	**x**	**x**

CCO Privacy Matrix	Requirement 1	Requirement 2	Requirement 3	Requirement 4	Requirement 5	Requirement 6	Requirement 7	Requirement 8	Requirement 9	Requirement 10	Requirement 11	Requirement 12	Requirement 13	Requirement 14	Requirement 15	Requirement 16	Requirement 17	Requirement 18	Requirement 19	Requirement 20	Requirement 21	Requirement 22	Requirement 23	Requirement 24	Requirement 25	Requirement 26	Requirement 27	Requirement 28	Requirement 29	Requirement 30	Requirement 31	Requirement 32	Requirement 33
Consulting Agreement - Template																				**x**													
Contract System Management																					**x**												
Data Access Committee: Terms of Reference & Decision Criteria for CCO Data Requests												**x**																					
Data and Record Destruction Certificate														**x**																			
Data Disclosure Subcommitte e Terms of Reference													**x**																				
Data Linkage Policy																						**x**											
Data Linkage Procedure																						**x**											
Data Sharing Agreement Initiation Form																	**x**	**x**															
Data Sharing Agreement Initiation Procedure				**x**								**x**				**x**	**x**												**x**				
Data Sharing Agreement Standard												**x**																					

CCO Privacy Matrix	Requirement 1	Requirement 2	Requirement 3	Requirement 4	Requirement 5	Requirement 6	Requirement 7	Requirement 8	Requirement 9	Requirement 10	Requirement 11	Requirement 12	Requirement 13	Requirement 14	Requirement 15	Requirement 16	Requirement 17	Requirement 18	Requirement 19	Requirement 20	Requirement 21	Requirement 22	Requirement 23	Requirement 24	Requirement 25	Requirement 26	Requirement 27	Requirement 28	Requirement 29	Requirement 30	Requirement 31	Requirement 32	Requirement 33
Data Sharing Agreement Template				**x**								**x**					**x**																
Data Use & Disclosure Standard	**x**							**x**				**x**	**x**						**x**					**x**									
Decision Criteria for Data Requests	**x**											**x**	**x**											**x**									
De-Identification Guidelines	**x**											**x**	**x**											**x**									
Digital Media Destruction Procedure	**x**																																
Digital Media Destruction Standard	**x**																																
Digital Media Disposal Procedure								**x**				**x**																					
Digital Media Disposal Standard								**x**				**x**																					
Digital Personal Health Information Handling Procedure																			**x**														
Digital Personal Health Information Handling Standard																			**x**														
Employee Exit Process								**x**																									

CCO Privacy Matrix	Requirement 1	Requirement 2	Requirement 3	Requirement 4	Requirement 5	Requirement 6	Requirement 7	Requirement 8	Requirement 9	Requirement 10	Requirement 11	Requirement 12	Requirement 13	Requirement 14	Requirement 15	Requirement 16	Requirement 17	Requirement 18	Requirement 19	Requirement 20	Requirement 21	Requirement 22	Requirement 23	Requirement 24	Requirement 25	Requirement 26	Requirement 27	Requirement 28	Requirement 29	Requirement 30	Requirement 31	Requirement 32	Requirement 33
IM/IT Technology Stage - Gating Policy				x																													
Information Security Policy	x																																
Internal Data Access Policy								x																									
Internal Data Request Form									x																								
Internal Data Sharing Procedure								x				x																					
Internal Data Access Procedure								x																									
List of Data Linkages																						x	x										
Log of Access Requests on the eCCO Data Access Request Tool								x																									
Log of Data Sharing Agreements																		x															
Log of Privacy Breaches																												x	x				
Log of Privacy Impact Assessments																								x	x								
Log of Privacy																															x	x	

CCO Privacy Matrix	Requirement 1	Requirement 2	Requirement 3	Requirement 4	Requirement 5	Requirement 6	Requirement 7	Requirement 8	Requirement 9	Requirement 10	Requirement 11	Requirement 12	Requirement 13	Requirement 14	Requirement 15	Requirement 16	Requirement 17	Requirement 18	Requirement 19	Requirement 20	Requirement 21	Requirement 22	Requirement 23	Requirement 24	Requirement 25	Requirement 26	Requirement 27	Requirement 28	Requirement 29	Requirement 30	Requirement 31	Requirement 32	Requirement 33
Inquiries and Complaints																																	
Log of Research Agreements														**x**	**x**																		
Log of Third Party Service Providers with Access to PHI																					**x**												
Privacy & Security Acknowledgement Form																								**x**									
Privacy and Information Security Risk Management Procedure	**x**		**x**																								**x**	**x**					
Privacy Audit and Compliance Policy		**x**		**x**		**x**		**x**				**x**	**x**			**x**			**x**			**x**		**x**	**x**		**x**		**x**		**x**		**x**
Privacy Breach Management Form																											**x**		**x**	**x**			
Privacy Breach Management Manual				**x**		**x**		**x**					**x**						**x**			**x**		**x**	**x**				**x**	**x**	**x**		**x**
Privacy Breach Management Policy													**x**																				
Privacy Breach Report Form				**x**		**x**		**x**					**x**						**x**			**x**		**x**	**x**				**x**	**x**	**x**		**x**

CCO Privacy Matrix	Requirement 1	Requirement 2	Requirement 3	Requirement 4	Requirement 5	Requirement 6	Requirement 7	Requirement 8	Requirement 9	Requirement 10	Requirement 11	Requirement 12	Requirement 13	Requirement 14	Requirement 15	Requirement 16	Requirement 17	Requirement 18	Requirement 19	Requirement 20	Requirement 21	Requirement 22	Requirement 23	Requirement 24	Requirement 25	Requirement 26	Requirement 27	Requirement 28	Requirement 29	Requirement 30	Requirement 31	Requirement 32	Requirement 33
Privacy Impact Assessment Standard																									**x**								
Privacy Inquiries and Complaints Procedure	**x**		**x**																												**x**	**x**	**x**
Privacy Risk Register																											**x**	**x**					
Procurement Documentation and Records Management Procedure																			**x**														
Research Data Disclosure Agreement													**x**	**x**																			
Retention of Records Containing Personal Health Information Policy																	**x**																
Secure Transfer of Personal Health Information Policy																	**x**																
Secure Transfer of Personal Health Information Standard														**x**			**x**																

CCO Privacy Matrix	Requirement 1	Requirement 2	Requirement 3	Requirement 4	Requirement 5	Requirement 6	Requirement 7	Requirement 8	Requirement 9	Requirement 10	Requirement 11	Requirement 12	Requirement 13	Requirement 14	Requirement 15	Requirement 16	Requirement 17	Requirement 18	Requirement 19	Requirement 20	Requirement 21	Requirement 22	Requirement 23	Requirement 24	Requirement 25	Requirement 26	Requirement 27	Requirement 28	Requirement 29	Requirement 30	Requirement 31	Requirement 32	Requirement 33
Statement of Information Practices	**x**		**x**																														
Template Schedule for Third Party Agreements																			**x**														

IPC Requirements

Privacy: Requirements of Section 1 of the Manual: Privacy Policy in Respect of CCO's Status as a PE and PP.

CCO is committed to respecting personal privacy, safeguarding confidential information and ensuring the security of PHI within its custody. A key component of CCO's Privacy Program is **CCO's *Privacy Policy***, which is supported by related policies and procedures that provide additional information on the Privacy Principles in the CCO context and how it is operationalized.

CCO has also implemented a formalized Privacy Governance Framework. The Privacy Governance Framework is the second key component of CCO's Privacy Program. The Privacy Governance Framework is designed to give effect to CCO's *Privacy Policy*, and, more generally, to its commitment to privacy. The Privacy Governance Framework enables the effective integration and coordination of CCO's LPO, policies, and programs with the organization as a whole.

The following documents outline CCO's compliance with this requirement:

1. *CCO's Privacy Policy*, LPO
2. *Privacy Governance Framework,* LPO
3. *Data Use & Disclosure Standard,* LPO and A&I
4. *Decision Criteria for Data Requests,* A&I
5. *Statement of Information Practices*, LPO
6. *Privacy Inquiries and Complaints Procedure*, LPO
7. *De-identification Guidelines*, LPO
8. *Information Security Policy,* EISO
9. *Digital Media Disposal Standard,* EISO
10. *Digital Media Disposal Procedure*, EISO
11. *Job descriptions: Director, Legal & Privacy; Group Manager, Privacy; Senior Privacy Specialist; Privacy Specialist*

	**All requirements for this section have been met.**

Privacy: Requirements of Section 2 of the Manual: Policy and Procedures for Ongoing Review of Privacy Policies, Procedures and Practices.

CCO's *Privacy Audit and Compliance Policy* establishes a rigorous program for the review of policies and procedures as well as the auditing of compliance. As well, all policies and procedures indicate the next required review date.

The following documents outline CCO's compliance with this requirement:

1. *CCO's Privacy Policy*, LPO
2. *Privacy Audit and Compliance Policy,* LPO
3. *Logging, Monitoring and Auditing Standard and Procedure*, EISO

All requirements for this section have been met.

Privacy: Requirements of Section 3 of the Manual: Policy on the Transparency of Privacy Policies, Procedures and Practices.

CCO provides information on its Privacy Program and its privacy policies, procedures and practices, to the organization, the public and other stakeholders, through a variety of means, including, through the CCO internal and public websites, updates and other privacy awareness initiatives.

The following documents outline CCO's compliance with this requirement:

1. *CCO's Privacy Policy*, LPO
2. *Privacy Inquiries and Complaints Procedure*, LPO
3. *Statement of Information Practices*, LPO
4. *Privacy FAQs*, LPO
5. *Annual Privacy Report,* LPO

In addition, the following document addresses additional compliance measures specific to CCO's role as a PP:

6. *CSP Privacy FAQs,* LPO

All requirements for this section have been met.

Privacy: Requirements of Section 4 of the Manual: Policy and Procedures for the Collection of PHI.

CCO policies and procedures articulate its commitment to limit the collection of PHI to only that which is permitted by PHIPA and only to that which is necessary. The policies and procedures identified below meet this commitment by setting out criteria for identifying the purposes for the collection of PHI, the review and approval processes for the collection of PHI and the conditions or restrictions that must be satisfied prior to the collection of PHI.

The following documents outline CCO's compliance with this requirement:

1. *CCO's Privacy Policy*, LPO
2. *Privacy Audit and Compliance Policy*, LPO
3. *Privacy Breach Management Policy,* LPO
4. *Privacy Breach Management Manual,* LPO
5. *Data Sharing Agreement Initiation Procedure*, LPO
6. *Data Sharing Agreement Template*, LPO
7. *IM/IT Stage – Gating Policy,* Gating Office

	**All requirements for this section have been met.**

Privacy: Requirements of Section 5 of the Manual: List of Data Holdings containing PHI.

CCO maintains a central, online repository which describes all CCO data holdings, both PHI and non-PHI. The Data Catalogue provides a single location for obtaining information about CCO data, including associated programs and subjects, data start and end dates.

The following document outlines CCO's compliance with this requirement:

1. *CCO's Privacy Policy*, LPO

✓	**All requirements for this section have been met.**

Privacy: Requirements of Section 6 of the Manual: Policy and Procedures for Statements of Purpose for Data Holdings containing PHI.

CCO has in place policies and procedures which require statements of purpose for data holdings containing PHI to be created, reviewed, amended and/or approved on an ongoing basis.

The following documents outline CCO's compliance with this requirement:

1. *CCO's Privacy Policy*, LPO
2. *Privacy Breach Management Policy*, LPO
3. *Privacy Breach Management Manual,* LPO
4. *Privacy Audit and Compliance Policy,* LPO

✓	**All requirements for this section have been met.**

Privacy: Requirements of Section 7 of the Manual: Statements of Purpose for Data Holdings Containing PHI.

CCO maintains a statement of purpose for each data holding containing PHI, identifying the purpose of the data holding, the PHI contained in the data holding, the source(s) of the PHI and the need for the PHI in relation to the identified purpose.

The following document outlines CCO's compliance with this requirement:

1. *CCO's Privacy Policy*, LPO

✓	**All requirements for this section have been met.**

Privacy: Requirements of Section 8 of the Manual: Policy and Procedures for Limiting Agent Access to and Use of PHI.

CCO ensures that access to PHI by its employees is strictly limited in accordance with the "need to know" principle, whereby employees access and use only the minimum

amount of identifiable information necessary for carrying out their job responsibilities. CCO's comprehensive access request and approval process must be followed before an individual is permitted access to data.

The following documents outline CCO's compliance with this requirement:

1. *CCO's Privacy Policy,* LPO
2. *Data Use and Disclosure Standard,* LPO and A&I
3. *Internal Data Access Policy,* LPO and A&I
4. *Internal Data Access Procedure*, LPO and A&I
5. *Internal Data Sharing Procedure,* LPO
6. *Digital Media Disposal Standard,* EISO
7. *Digital Media Disposal Procedure*, EISO
8. *Employee Exit Process,* Human Resources
9. *Exiting Employee Data Management,* Technology Services
10. *Privacy Audit and Compliance Policy,* LPO
11. *Privacy Breach Management Policy,* LPO
12. *Privacy Breach Management Manual,* LPO
13. *Log of Access Requests on the eCCO Data Access Request Tool* (*i.e.*, the log of agents granted approval to access and use PHI), A&I

	**All requirements for this section have been met.**

Privacy: Requirements of Section 9 of the Manual: Log of Agents Granted Approval to Access and Use PHI.

CCO maintains a log of users who are granted approval to access and use PHI to prevent against unauthorized access, use and disclosure of PHI. The Internal Data Access Request (**IDAR**) tool logs internal uses and access to PHI (non-research).

The following documents outline CCO's compliance with this requirement:

1. *CCO's Internal Direct Access Request on-line tool*, A&I

	**All requirements for this section have been met.**

Privacy: Requirements of Section 10 of the Manual: Policy and Procedures for the Use of PHI for Research.

All research, as defined in PHIPA, undertaken through CCO, per section 44 of PHIPA, is considered a disclosure of PHI to the researcher regardless of whether the researcher is a CCO employee or an external party (non-CCO employee) and is not considered by CCO to be a use of PHI for research purposes.

As such, this requirement is not applicable to CCO. Please see Requirement 13 - *Policies and Procedures for Disclosures of Personal Health Information for Research Purposes and the Execution of Research Agreements.*

All research requests for PHI must be accompanied by Research Ethics Board (**REB**) approval; a research plan; and an Application for Disclosure of Information from CCO for Research Purposes, which sets out the terms and conditions that a researcher must abide by when using the PHI disclosed by CCO for research purposes. The DDSC reviews all research requests for access to PHI. Requests are either approved or denied by the DDSC, which is co-chaired by the Group Manager, Privacy. The *Application for Disclosure of Information from CCO for Research Purposes*, along with the *CCO Non-Disclosure/Confidentiality Agreement* forms the agreement between CCO and a researcher.

This requirement is not applicable to CCO.

Privacy: Requirements of Section 11 of the Manual: Log of Approved Uses of PHI for Research.

CCO does not log all approved uses of PHI for research, as all research undertaken at CCO, per section 44 of PHIPA, is considered a disclosure of PHI to the researcher regardless of whether the researcher is a CCO employee or an external party (non-CCO employee) and is not considered by CCO to be a use of PHI for research purposes.

However, CCO does log all approved disclosures of PHI for research purposes. Please see Requirement 15 – *Log of Research Agreements*.

This requirement is not applicable to CCO.

Privacy: Requirements of Section 12 of the Manual: Policy/Procedure for Disclosure of PHI for Purposes other than Research.

CCO is committed to ensuring the data access processes and procedures related to disclosures of PHI for purposes other than research, are in accordance with PHIPA, its regulation and CCO's Privacy Policy. CCO has a comprehensive data request process in place to be utilized by all individuals requesting access to PHI for purposes other than

research. The documents listed below identify the process, including the documentation that must be completed, submitted, reviewed or executed by all responsible parties and committees.

The following documents outline CCO's compliance with this requirement:

1. *Data Use & Disclosure Standard,* LPO
2. *Business Process for Data Requests,* LPO
3. *De-Identification Guidelines*, LPO
4. *Data Sharing Agreement Template,* LPO
5. *Data Sharing Agreement Initiation Procedure,* LPO
6. *Data Sharing Agreement Initiation Form*, LPO
7. *Data Sharing Agreement Standard,* LPO
8. *Decision Criteria for Data Requests,* A&I
9. *Internal Data Sharing Procedure,* LPO
10. *Privacy Audit and Compliance Policy*, LPO
11. *Privacy Breach Management Policy*, LPO
12. *CCO's Privacy Policy,* LPO

	**All requirements for this section have been met.**

Privacy: Requirements of Section 13 of the Manual*:* Policy/Procedure for Disclosures of PHI for Research Purposes and the Execution of Research Agreements.

At CCO, all research requests for PHI must be accompanied by an REB approval, a research plan, and an Application for Disclosure for Information from CCO for Research Purposes, which sets out the terms and conditions that a researcher must abide by when using the PHI disclosed by CCO for research purposes. The DDSC reviews all research requests for access to PHI. Requests are either approved or denied by the DDSC, which is chaired by the Group Manager, Privacy. The Application for Disclosure for Information from CCO for Research Purposes, along with the CCO Non-Disclosure/Confidentiality Agreement, forms the agreement between CCO and a researcher.

The following documents outline CCO's compliance with this requirement:

1. *Data Use & Disclosure Standard,* LPO and A&I
2. *Business Process for Data Requests,* A&I
3. *Application for Disclosure of Information from CCO for Research Purposes,* A&I
4. *Research Data Disclosure Agreement,* LPO and A&I
5. *Decision Criteria for Data Requests,* A&I
6. *Data Disclosure Subcommittee Terms of Reference*, A&I
7. *Privacy Breach Management Policy*, LPO
8. *Privacy Breach Management Manual,* LPO
9. *Privacy Audit and Compliance Policy*, LPO
10. *De-Identification Guidelines,* LPO

All requirements for this section have been met.

Privacy: Requirements of Section 14 of the Manual: Template Research Agreements.

CCO has a comprehensive data request process in place to be utilized by all researchers requesting access to PHI, de-identified or aggregate information for research purposes. The research agreement sets out the responsibilities of the researcher and CCO when PHI is disclosed by CCO. This agreement demonstrates CCO's commitment towards preventing unauthorized disclosure of PHI.

The following documents outline CCO's compliance with this requirement:

1. *Application for Disclosure of Information from CCO for Research Purposes,* A&I
2. *Research Data Disclosure Agreement,* LPO and A&I
3. *Log of Research Agreements*, A&I
4. *Business Process for Data Requests,* A&I
5. *Secure Transfer of Personal Health Information Policy*, LPO
6. *Secure Transfer of Personal Health Information Standard*, LPO
7. *Data and Record Destruction Certificate*, EISO

8. *Privacy Audit and Compliance Policy*, LPO

✓	**All requirements for this section have been met.**

Privacy: Requirements of Section 15 of the Manual: Log of Research Agreements.

The Informatics & Analytics maintains a log of executed Research Agreements between CCO and all researchers on CCO's secure network drive.

The following document outlines CCO's compliance with this requirement:

1. *Log of Research Agreements*, A&I
2. *Business Process for Data Requests,* A&I

✓	**All requirements for this section have been met.**

Privacy: Requirements of Section 16 of the Manual: Policy and Procedures for the execution of DSAs.

Through its DSA processes, CCO demonstrates its commitment to ensuring that all data exchanges between CCO and another party are done so in accordance with PHIPA and privacy best practices.

The following documents outline CCO's compliance with this requirement:

1. *CCO's Privacy Policy*, LPO
2. *Data Sharing Agreement Initiation Procedure*, LPO
3. *Data Sharing Agreement Standard,* LPO
4. *Data Sharing Agreement Initiation Form*, LPO
5. *Privacy Audit and Compliance Policy*, LPO
6. *Privacy Breach Management Policy*, LPO
7. *Privacy Breach Management Manual,* LPO

All requirements for this section have been met.

Privacy: Requirements of Section 17 of the Manual: Template DSAs.

The CCO template DSAs specify the terms and conditions to be adhered to for each DSA executed by CCO when collecting or disclosing PHI for purposes other than research. These agreements demonstrate CCO's commitment towards preventing unauthorized collection, use or disclosure of PHI.

The following documents outline CCO's compliance with this requirement:

1. *CCO's Privacy Policy*, LPO
2. *Data Sharing Agreement Template*, LPO
3. *Data Sharing Agreement Standard,* LPO
4. *Data Sharing Agreement Initiation Procedure*, LPO
5. *Data Sharing Agreement Initiation Form,* LPO
6. *Secure Transfer of Personal Health Information Policy*, LPO
7. *Secure Transfer of Personal Health Information Standard*, LPO
8. *Privacy Audit and Compliance Policy*, LPO
9. *Privacy Breach Management Policy*, LPO
10. *Retention of Records Containing Personal Health Information*, LPO

All requirements for this section have been met.

Privacy: Requirements of Section 18 of the Manual: Log of DSAs.

CCO maintains a log of all DSAs in place with external parties.

The following documents outline CCO's compliance with this requirement:

1. *CCO's Privacy Policy*, LPO

2. *Data Sharing Agreement Initiation Procedure*, LPO
3. *Log of Data Sharing Agreements,* LPO

All requirements for this section have been met.

Privacy: Requirements of Section 19 of the Manual: Policy and Procedures for Executing Agreements with Third Party Service Providers in respect of PHI.

CCO requires that written agreements, with the appropriate privacy provisions, be entered into with third parties prior to permitting access to and use of PHI. These documents ensure that third parties access and use data in accordance with CCO privacy and security policies and that retention and disposal requirements are being met within the required time frame.

The following documents outline CCO's compliance with this requirement:

1. *CCO's Privacy Policy*, LPO
2. *Data Use and Disclosure Standard*, LPO and A&I
3. *Privacy Audit and Compliance Policy*, LPO
4. *Procurement Documentation and Records Management Procedure*, Strategic Sourcing
5. *CCO Procurement Policy*, Strategic Sourcing
6. *Procurement Guide for Good/Services Under 15K,* Strategic Sourcing
7. *Privacy Breach Management Policy*, LPO
8. *Privacy Breach Management Manual,* LPO
9. *Template Schedule for Third Party Agreements,* LPO
10. *Digital PHI Handling* Standard and Procedure, EISO

All requirements for this section have been met.

Privacy: Requirements of Section 20 of the Manual: Template Agreement for all Third Party Service Providers.

CCO is committed to respecting personal privacy, safeguarding confidential information and ensuring the security of PHI within its custody and within the custody of third parties

retained by CCO. It meets this commitment through the inclusion of the appropriate privacy provisions in its template agreement for all third party service providers, in addition to incorporating privacy and security related provisions and responsibilities as required on an ongoing basis.

The following documents outline CCO's compliance with this requirement:

1. *Services Agreement- Template Schedule for Third Party Agreements,* LPO
2. *Consulting Agreement – Template,* LPO

All requirements for this section have been met.

Privacy: Requirements of Section 21 of the Manual: Log of Agreements with Third Party Service Providers.

CCO maintains a log of all agreements with third party service providers through its Contract Management System.

The following documents outline CCO's compliance with this requirement:

1. *Contract Management System*, Strategic Sourcing
2. *Log of Third Party Service Providers with Access to PHI,* LPO

All requirements for this section have been met.

Privacy: Requirements of Section 22 of the Manual: Policy and Procedures for the Linkage of Records of PHI.

At CCO, all linkages of records of PHI are performed in accordance with PHIPA, CCO's privacy policies and the terms and conditions of agreements in place with data providers. CCO defines two types of data linkages, as follows:

Permanent/operational data linkages are linkages performed to set up data holdings, including both system based and manual linkages for ongoing operational and analytical purposes, and linkages across data holdings for purposes of ongoing routine reporting.

Ad hoc data linkages are linkages conducted to produce a deliverable such as a report in response to an ad-hoc analysis and/or an exploratory analysis request. Some of these deliverables can become permanent/operational linkages over time. Ad hoc linkages include linkages performed solely for troubleshooting or investigative purposes.

The following documents outline CCO's compliance with this requirement:

1. *Data Linkage Policy,* LPO and A&I
2. *Data Linkage Procedure,* LPO and A&I
3. *Privacy Breach Management Policy*, LPO
4. *Privacy Breach Management Manual,* LPO
5. *Privacy Audit and Compliance Policy*, LPO
6. *List of Data Linkages* (*i.e.*, the Log of approved linkages of records of PHI), A&I

	**All requirements for this section have been met.**

Privacy: Requirements of Section 23 of the Manual: Log of Approved Linkages of Records of PHI.

CCO maintains a List of Data Linkages which tracks the number of approved data linkages. The List includes the category of requestor, the date the linkage was approved and the nature of the records of PHI linked.

The following document outlines CCO's compliance with this requirement:

1. *List of Data Linkages,* A&I

	**All requirements for this section have been met.**

Privacy: Requirements of Section 24 of the Manual: Policy/Procedures with respect to De-Identification and Aggregation.

CCO is committed to providing de-identified and/or aggregate information, rather than PHI, to requesting parties if the de-identified and/or aggregate information serves the identified purpose. CCO meets this commitment by conducting a thorough review of all data requests and the purpose for which the data is to serve, in addition to reviewing the data that is to be disclosed to determine if it is reasonably foreseeable that the information could be utilized, either alone or with other information, to identify an individual.

CCO is in the process of acquiring a de-identification tool in order to facilitate the de-identification of PHI. A new policy suite and de-identification guidelines will accompany the implementation of the tool which is planned for fiscal year 2016/17.

The following documents outline CCO's compliance with this requirement:

1. *CCO's Privacy Policy*, LPO
2. *Data Use & Disclosure Standard,* LPO and A&I
3. *De-Identification Guidelines,* LPO
4. *Business Process for Data Requests,* A&I
5. *Privacy & Security Acknowledgment Form,* LPO
6. *Decision Criteria for Data Requests,* A&I
7. *Privacy Audit and Compliance Policy*, LPO
8. *Privacy Breach Management Policy*, LPO
9. *Privacy Breach Management Manual,* LPO
10. *PHI Handling Standard and Procedure,* EISO

All requirements for this section have been met.

Privacy: Requirements of Section 25 of the Manual: PIA Policy and Procedures.

CCO has policies in place to identify the circumstances in which PIAs are required. These policies provide clear direction on the scope of PIAs at CCO, the responsibility for conducting PIAs and the process for implementing recommendations arising from completed PIAs. All new initiatives and changes to existing projects are reviewed to determine if a PIA is required to identify the privacy risks and appropriate mitigating strategy.

The following documents outline CCO's compliance with this requirement:

1. *CCO's Privacy Policy*, LPO
2. *Privacy Impact Assessment Standard*, LPO
3. *Log of Privacy Impact Assessments*, LPO
4. *Privacy Audit and Compliance Policy*, LPO

5. *Privacy Breach Management Policy*, LPO
6. *Privacy Breach Management Manual,* LPO
7. *Privacy and Information Security Risk Management Procedure,* LPO & EISO

✓	**All requirements for this section have been met.**

Privacy: Requirements of Section 26 of the Manual: Log of PIAs.

CCO maintains a log of all PIAs which have been undertaken to ensure that identified privacy risks are tracked and mitigated in a timely manner.

The following document outlines CCO's compliance with this requirement:

1. *Log of Privacy Impact Assessments*, LPO

✓	**All requirements for this section have been met.**

Privacy: Requirements of Section 27 of the Manual: Policy and Procedures in respect of Privacy Audits.

Privacy audits are a key component of CCO's overall Privacy Program. In order for CCO to protect the privacy and confidentiality of the PHI it receives, privacy audits are conducted to ensure there is no unauthorized access, use or disclosure of PHI.

The following documents outline CCO's compliance with this requirement:

1. *CCO's Privacy Policy*, LPO
2. *Privacy Audit and Compliance Policy*, LPO
3. *Logging, Monitoring and Auditing Standard and Procedure,* EISO
4. *Privacy Risk Register* (*i.e.*, the Log of privacy audits), LPO

✓	**All requirements for this section have been met.**

Privacy: Requirements of Section 28 of the Manual: Log of Privacy Audits.

CCO maintains an up-to date and accurate log of all privacy audits conducted at the program and business unit and enterprise level.

The following document outlines CCO's compliance with this requirement:

1. *Privacy Risk Register*, LPO
2. *Privacy Audit and Compliance Policy*, LPO

	**All requirements for this section have been met.**

Privacy: Requirements of Section 29 of the Manual: Policy and Procedures for Privacy Breach Management.

CCO policies stipulate that it is mandatory to report all privacy breaches or suspected privacy breaches. CCO's *Privacy Breach Management Policy and Privacy Breach Management Manual* clearly defines the identification, reporting, containment, notification, investigation and remediation processes to be followed when a privacy breach or suspected privacy breach has occurred.

The following documents outline CCO's compliance with this requirement:

1. *CCO's Privacy Policy,* LPO
2. *Privacy Breach Management Policy*, LPO
3. *Privacy Breach Management Manual,* LPO
4. *Privacy Audit and Compliance Policy*, LPO
5. *Data Sharing Agreements Initiation Procedure*, LPO
6. *Privacy Breach Report Form*, LPO
7. *Log of Privacy Breaches*, LPO

	**All requirements for this section have been met.**

Privacy: Requirements of Section 30 of the Manual: Log of Privacy Breaches.

CCO maintains a comprehensive log of all privacy breaches, including suspected privacy breaches that occur.

The following documents outline CCO's compliance with this requirement:

1. *CCO's Privacy Policy*, LPO

2. *Privacy Breach Management Policy*, LPO
3. *Privacy Breach Management Manual,* LPO
4. *Log of Privacy Breaches*, LPO
5. *Privacy Breach Report Form*, LPO

Privacy: Requirements of Section 31 of the Manual: Policy and Procedures for Privacy Complaints.

CCO reviews and responds to all complaints from the public, on its information practices and/or its compliance with PHIPA. Through the use of its privacy complaints processes, the public is encouraged to contact CCO and have the appropriate measures taken when responding to the complaint.

The following documents outline CCO's compliance with this requirement:

1. *CCO's Privacy Policy*, LPO
2. *Privacy Inquiries and Complaints Procedure*, LPO
3. *Privacy Breach Management Policy*, LPO
4. *Privacy Breach Management Manual,* LPO
5. *Privacy Audit and Compliance Policy*, LPO
6. *Log of Privacy Inquiries and Complaints*, LPO
7. *Statement of Information Practices,* LPO

Privacy: Requirements of Section 32 of the Manual: Log of Privacy Complaints.

CCO maintains a log of all privacy complaints.

The following documents outline CCO's compliance with this requirement:

1. *CCO's Privacy Policy*, LPO
2. *Privacy Inquiries and Complaints Procedure*, LPO
3. *Log of Privacy Inquiries and Complaints*, LPO

	**All requirements for this section have been met.**

Privacy: Requirements of Section 33 of the Manual: Policy and Procedures for Privacy Inquiries.

CCO reviews and responds to all inquiries from the public, on its information practices and/or its compliance with PHIPA. Through the use of its privacy inquiries processes, the public is encouraged to contact CCO and have the appropriate measures taken when responding to the inquiry.

The following documents outline CCO's compliance with this requirement:

1. *CCO's Privacy Policy*, LPO
2. *Privacy Inquiries and Complaints Procedure*, LPO
3. *Privacy Breach Management Policy*, LPO
4. *Privacy Breach Management Manual,* LPO
5. *Privacy Audit and Compliance Policy*, LPO

	**All requirements for this section have been met.**

Part 2: CCO's Information Security Program

CCO operates digital services within a rapidly changing environment. This environment presents a number of risks, from both internal and external threat sources. CCO's Enterprise Information Security Program (**EISP**) provides a structured approach to managing these risks in a manner that delivers value to CCO's core business. This business value statement includes the protection of information and IT assets, reduction of risk event impact, support of compliance objectives, and enablement of new technologies.

The following are the drivers for the EISP implementation at CCO.

Business Enablement

Information security is a business enabler. A strong and robust information security program enables the effective management of technology related risks. The assurance derived from a sound information security program allows the business to take advantage of advances in technology, and other information sharing mechanisms, to grow the business through new business channels and partner interaction models.

Strategic Alignment

The information security program is driven by CCO's strategic objectives and business direction. This results in an enterprise security architecture based on a holistic approach to information protection, focused on business requirements. The business-based approach provides the context for the information security program implementation and assures that the resulting security architecture aligns with CCO's business strategy.

Risk Management

CCO follows a risk-based approach to information security. Any identified risks are weighed in relation to CCO's enterprise risk tolerance and managed in proportion to the assessed business impact and cost of mitigation. CCO's appetite and tolerances for information security risks are defined in consultation with CCO's ET.

Operational Effectiveness

CCO strives for effectiveness in the management of information security. This means security services are delivered that protect CCO's assets, reduce risk, and add business value in a meaningful and measurable way. CCO demonstrates capability in delivering on its security program and commitments, through effective management and governance.

Compliance with Legal and Regulatory Requirements

CCO's IM practices are subject to regulatory oversight through privacy and access legislation such as PHIPA and FIPPA.

All policy, standard, process, procedure, and guideline documents in support of information security must take into account the relevant legislative and regulatory frameworks, as well as the IPC guidelines, fact sheets, and good practices.

CCO also has compliance requirements stemming from financial audit obligations, obligations as a service provider, product certification processes, insurance requirements, and through various agreements and contracts with partners. Together these form a significant driver for the implementation and operation of the information security program.

CCO's Information Security Governance Framework

Information security governance ensures that CCO's information security program is aligned with, and meets the strategic needs of, CCO's business. This includes the establishment of processes that ensure reasonable actions are taken, in pursuit of business goals, to protect CCO's information resources in the most effective and efficient manner.

Implementation and management of the security program is accomplished through CCO's EISO. The EISO is responsible for working with CCO's various governance bodies and operational areas to ensure overall information protection is achieved in accordance with CCO's set objectives. The EISO works closely with partners within the LPO and CCO's A&I department.

Projects, operational teams, and program areas execute on the day-to-day security processes through a combination of cross functional roles throughout CCO.

The chart on the following page sets out how both privacy and security management is organized at CCO, followed by details about key aspects of the organizational structure.

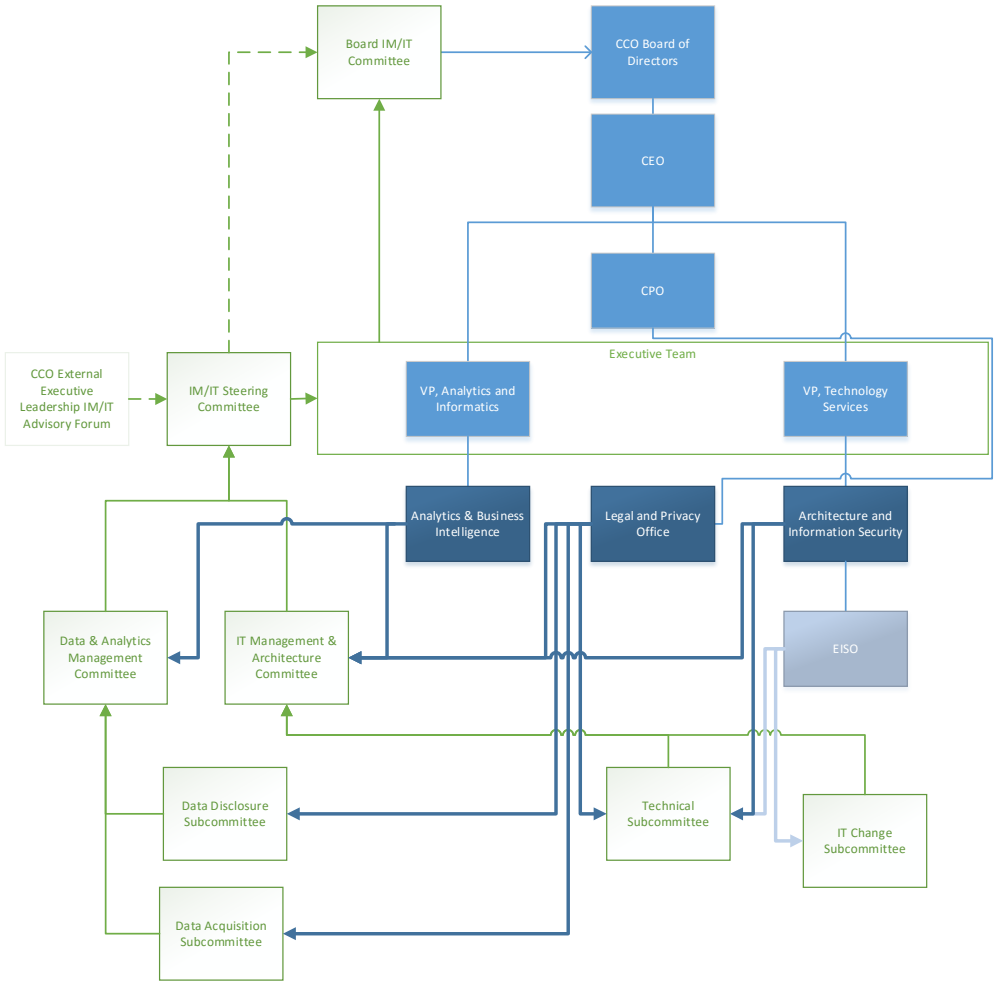


Figure 3 Privacy and Security Governance Structure

Board of Directors

CCO's Board of Directors holds accountability for security governance practices in support of CCO's mission. The complete Board of Directors receives a semi-annual cyber security briefing. The IM/IT Committee of the Board receives a scheduled report on cyber security matters at alternating meetings through a standing agenda item and on an as needed basis outside of the scheduled updates. These reports are delivered by the VP of Technology Services, supported by the EISO. This reporting structure ensures security is reported on regularly to the highest levels of the organization.

ET

The CCO ET supports and champions the security program at CCO, actively advocating a culture of privacy and information protection. The VP of Technology Services provides the ET with relevant information on matters of security compliance, breaches and material incidents, security audit reports, and industry developments of note. On a semi-annual basis, the VP of Technology Services also reports to the ET on technology and security risks, through the Enterprise Risk Management (**ERM**) report, which is also provided to the MOHLTC as part of CCO's Annual Business Plan.

VP of Technology Services

Accountability for security compliance, in support of privacy and other compliance regimes, resides with CCO's President and CEO. This function has been formally delegated to CCO's VP, Technology Services who is appointed by the CEO and reports directly to the CEO. The VP, Technology Services provides security representation on the most senior decision-making bodies within CCO. The VP, Technology Services delegates the strategic direction and operations of the EISP to the Director, Architecture and Information Security Services.

Director, Architecture and Information Security Services

The Director, Architecture and Information Security Services supports the VP, Technology Services and other executives by providing strategic advice and overseeing the development and implementation of the EISP. The Director ensures the EISP is staffed, funded, and functioning in accordance with the needs of CCO. The Director is supported by the Group Manager, Information Security who manages the day-to-day operation of the security program and services.

Group Manager, Information Security

The Group Manager for Information Security manages the EISO and reports to the Director, Architecture and Information Security Services. The Group Manager is specifically responsible for:

(i) Managing the operations of the information security program;

(ii) Working with the Business Unit Managers and Technology Services in establishing, implementing, monitoring and assessing security program controls on an ongoing basis;

(iii) Providing security advice and support to all business functions;

(iv) Ensuring that the suite of security policies is comprehensive, up-to-date and compliant with applicable law and standards;

(v) Providing security training;

(vi) Advocating for security within the organization;

(vii) Conducting security reviews, audits/compliance monitoring, and benchmarking, as appropriate;

(viii) Ensuring that appropriate security aspects of procurement and vendor management are implemented;

(ix) Overseeing the operational security team with the effective operation of security controls; and

(x) Monitoring the threat environment and other developments in the information security arena.

EISO

The EISO is led by the Group Manager, Information Security and supported by Security Architects, Senior (**Sr.**) Information Security Advisors, and Information Security Advisors.

The complete organizational structure for the EISO is provided within *Appendix "B".*

The EISO has developed over time from a technology focused group embedded within the technical operations team to an enterprise focused information assurance function. The EISO is structured to enable CCO business through the effective management of technology-related risks and facilitating the safe adoption of new technologies. The program is aligned to applicable standards and industry best practices allowing for eventual certification.

The EISO has the following objectives:

- The effective protection of CCO information and information assets from harm.
- Create and nurture a culture of Information Security in all organizational areas of CCO.
- Implement and operate an information security risk management program that takes into account CCO executive risk tolerances and ensures safeguards are selected based on appropriate criteria.
- Develop and maintain Information Security shared services and enterprise information security architecture for reuse and cost-effectiveness.
- Achieve compliance to legal and regulatory requirements a result of an effective information security program.
- Contribute to improving CCO's effectiveness and efficiency by maturing information security practices.

The EISO meets these objectives through integration with CCO's business processes and close relationships with business and corporate partners such as the LPO, A&I, and the Technology Services Operations team.

Network and Security Operations Team

Led by the Team Lead of Network and Security Operations, this group provides the front line technical expertise and services necessary to design, deploy, and operate various technical safeguards in support of CCO's secure environment. These technical safeguards operate at the network, computer, and application level – providing comprehensive coverage against modern threats. The Network and Security Operations team works closely with the EISO to ensure the overall effective security of CCO's information

Security Documentation

Security Documentation Matrix

CCO Security Matrix	Requirement 1	Requirement 2	Requirement 3	Requirement 4	Requirement 5	Requirement 6	Requirement 7	Requirement 8	Requirement 9	Requirement 10	Requirement 11	Requirement 12	Requirement 13	Requirement 14	Requirement 15	Requirement 16	Requirement 17	Requirement 18
Acceptable Use of Social Media Policy	**x**													**x**				
Access Card Procedure			**x**	**x**														
Access Data Centre Authorization - Contractor			**x**															
Access Data Centre Authorization - Employee			**x**															
Acquisition, Development, and Application Security Standard	**x**																	
Application for Disclosure of Information from CCO for Research Purposes					**x**													
Automated HCMS) process ~~System~~			**x**	**x**														
CCO's Privacy Policy					**x**										**x**			

CCO Security Matrix	Requirement 1	Requirement 2	Requirement 3	Requirement 4	Requirement 5	Requirement 6	Requirement 7	Requirement 8	Requirement 9	Requirement 10	Requirement 11	Requirement 12	Requirement 13	Requirement 14	Requirement 15	Requirement 16	Requirement 17	Requirement 18
CCO's Video Monitoring Policy			**x**															
Change Management Policy												**x**						
Change Subcommittee Terms of Reference												**x**						
Cryptography Standard						**x**	**x**											
Data Backup Policy	**x**				**x**								**x**					
Data Backup Procedure					**x**								**x**					
Data Centre Access and Usage Policy			**x**															
Data Sharing Agreement Initiation Procedure					**x**													
Data Sharing Agreement Standard					**x**													
Data Sharing Agreement Template					**x**													
Data Use & Disclosure Standard					**x**													
Digital Media Disposal Guideline					**x**			**x**										
Digital Media Disposal Procedure								**x**										

CCO Security Matrix	Requirement 1	Requirement 2	Requirement 3	Requirement 4	Requirement 5	Requirement 6	Requirement 7	Requirement 8	Requirement 9	Requirement 10	Requirement 11	Requirement 12	Requirement 13	Requirement 14	Requirement 15	Requirement 16	Requirement 17	Requirement 18
Digital Media Disposal Standard								x										
Digital PHI Handling Procedure					x	x	x											
Digital PHI Handling Standard					x	x	x											
Visitor Logging System			x	x														
Enterprise Information Security Policy	x	x	x		x	x	x	x	x	x	x	x	x	x	x	x	x	
Exchanging Personal Health Information Policy Suite							x											
Hard-Copy PHI Disposal Procedure								x										
HP Data Protectors Session Logs					x								x					
IM/IT Gating Process and Project Lifecycle Methodology	x																	
Incident Management Framework										x							x	
Information Classification and Handling Guideline					x		x	x										

CCO Security Matrix	Requirement 1	Requirement 2	Requirement 3	Requirement 4	Requirement 5	Requirement 6	Requirement 7	Requirement 8	Requirement 9	Requirement 10	Requirement 11	Requirement 12	Requirement 13	Requirement 14	Requirement 15	Requirement 16	Requirement 17	Requirement 18
Information Classification and Handling Standard					**x**		**x**											
Information Security Code of Conduct and Acceptable Use Policy	**x**	**x**	**x**		**x**	**x**			**x**	**x**	**x**			**x**				
Information Security Framework		**x**																
Information Security Incident and Breach Response Standard	**x**									**x**							**x**	**x**
Information Security Policy							**x**											
Information Security Program Framework	**x**	**x**													**x**			
Internal Data Access Requests (IDAR) Process			**x**															
Key Logging System			**x**	**x**														
Log of Security Audits															**x**	**x**		

CCO Security Matrix	Requirement 1	Requirement 2	Requirement 3	Requirement 4	Requirement 5	Requirement 6	Requirement 7	Requirement 8	Requirement 9	Requirement 10	Requirement 11	Requirement 12	Requirement 13	Requirement 14	Requirement 15	Requirement 16	Requirement 17	Requirement 18
Log of Third Party Service Providers with Access to Personal Health Information					**x**													
Logging, Monitoring, and Auditing Procedure	**x**						**x**		**x**	**x**				**x**	**x**			
Logging, Monitoring, and Auditing Standard	**x**						**x**		**x**	**x**				**x**	**x**			
Logical Access Control Standard	**x**		**x**			**x**	**x**		**x**									
Mobile Device and Pager ~~Procedure~~ Policy							**x**											
Open Media Logs					**x**								**x**					
Operational Security - Patch Management Standard											**x**							
Operational Security - Patching Procedure											**x**							
Operational Security Standard			**x**								**x**		**x**		**x**	**x**		
Photo ID Badge Request			**x**															

CCO Security Matrix	Requirement 1	Requirement 2	Requirement 3	Requirement 4	Requirement 5	Requirement 6	Requirement 7	Requirement 8	Requirement 9	Requirement 10	Requirement 11	Requirement 12	Requirement 13	Requirement 14	Requirement 15	Requirement 16	Requirement 17	Requirement 18
Photo Identification Request Form			**x**	**x**														
Policy on Retention of Records Containing PHI					**x**								~~**x**~~					
Privacy Audit and Compliance Policy			**x**	**x**	**x**		**x**											
Privacy Breach Management Policy			~~**x**~~		**x**			**x**										
Secure Transfer of Personal Health Information Policy					**x**		**x**						**x**					
Secure Transfer of Personal Health Information Standard					**x**		**x**						**x**					
Security Audit, Testing and Compliance Policy					**x**													
Security Audit, Testing~~,~~ and Compliance Standard										~~**x**~~				~~**x**~~	**x**			
Security Incident Log																	**x**	**x**

CCO Security Matrix	Requirement 1	Requirement 2	Requirement 3	Requirement 4	Requirement 5	Requirement 6	Requirement 7	Requirement 8	Requirement 9	Requirement 10	Requirement 11	Requirement 12	Requirement 13	Requirement 14	Requirement 15	Requirement 16	Requirement 17	Requirement 18
Security Risk Management Standard															**x**	**x**		
Services Agreement - Schedules for Third Party Agreements					**x**			**x**					**x**					
Visitor Access Policy			**x**															

IPC Requirements

Security: Requirements of Section 1 of the Manual: Information Security Policy.

CCO has implemented a broad overarching Enterprise Information Security Policy. This policy provides for a comprehensive information security program supporting administrative, technical, and physical controls consistent with established industry standards and practices. The program is risk based and includes a credible audit and assurance element. The program supports the identification, implementation, and effective operation of a robust information security infrastructure through the Technology Services department.

The following documents outline CCO's compliance with this requirement:

1. *Enterprise Information Security Policy*, EISO
2. *Information Security Program Framework*, EISO
3. *Information Security Code of Conduct and Acceptable Use Policy,* EISO
4. *Incident Management Framework*, EISO
5. *Logical Access Control Standard,* EISO
6. *Logging, Monitoring and Auditing Standard,* EISO
7. *Logging, Monitoring and Auditing Procedure*, EISO
8. *Information Management and Information Technology Stage - Gating Process and Project Lifecycle Methodology*
9. *Data Backup Policy,* Technology Services
10. *Acquisition Development and Application Security Standard*, EISO

	**All requirements for this section have been met.**

Security: Requirements of Section 2 of the Manual: Policy and Procedures for Ongoing Review of Security Policies, Procedures and Practices.

CCO has a process in place to review the entire body of the security policy framework. Updates are done according to CCO corporate practices, with policy documents kept in a controlled document library on eCCO. The implementation of the security program itself is an incremental and iterative process. Ongoing development allows CCO to maintain

an acceptable level of organizational risk that evolves with changes in technology, industry practices or standards, business environments, and information security threats. Monitoring, measurement and metrics help guide the program improvements towards maturity and ensure effective operation.

The following documents outline CCO's compliance with this requirement:

1. *Enterprise Information Security Policy*, EISO
2. *Information Security Code of Conduct and Acceptable Use Policy,* EISO
3. *Information Security Program Framework*, EISO
4. *Incident Management Framework*, EISO
5. *Logging, Monitoring and Auditing Standard,* EISO

All requirements for this section have been met.

Security: Requirements of Section 3 of the Manual: Policy and Procedures for Ensuring Physical Security of PHI.

This requirement is supported by certain other Facilities, Human Resources' and IT Services' policies that are designed to protect PHI from theft, loss, or unauthorized use or access. CCO is committed to protecting the physical security of all information within CCO, especially highly confidential information including PHI.

The following documents outline CCO's compliance with this requirement:

1. *Physical Security Policy,* Facilities
2. *Enterprise Information Security Policy*, EISO
3. *Information Security Code of Conduct and Acceptable Use Policy,* EISO
4. *Operational Security Standard,* Technology Services
5. *Statement of Confidentiality,* LPO and Human Resources
6. *Privacy Breach Management Policy,* LPO
7. *Logical Access Control Standard,* EISO

8. *Internal Data Access Procedure,* LPO and A&I
9. *Request for Service; Additional Badge,* Facilities
10. *Automated HCMS System,* Human Resources
11. *Photo Identification Request Form,* Facilities
12. *Data Center Access and Usage Policy,* Technology Services
13. *Data Centre Physical Security Standard*, Technology Services
14. *CCO Procurement Policy*, Strategic Sourcing
15. *Employee Exit Process,* Human Resources
16. *Visitor Access Procedure*, Facilities
17. *Video Monitoring Policy,* Facilities
18. *Privacy Audit and Compliance Policy*, LPO
19. *Access Card Procedure,* Facilities
20. *Physical Security Access Card Log,* Facilities
21. *Visitor Logging System,* Facilities
22. *Key Logging System,* Facilities

	**All requirements for this section have been met.**

Security: Requirements of Section 4 of the Manual: Log of Agents with Access to the Premises of CCO.

CCO maintains a comprehensive log of all access to its premises by visitors and CCO employees.

The following documents outline CCO's compliance with this requirement:

1. *Request for Service; Additional Badge*, Facilities and Technology Services.
2. *Photo Identification Request Form,* Facilities
3. *Automated HCMS System,* Human Resources

4. *Physical Security Access Card Log,* Facilities
5. *Access Card Procedure,* Facilities
6. *Visitor Logging System,* Facilities
7. *Key Logging System,* Facilities
8. *Privacy Audit and Compliance Policy,* LPO

	**All requirements for this section have been met.**

Security: Requirements of Section 5 of the Manual: Policy and Procedures for Secure Retention of Records of PHI.

The secure retention of PHI in either paper or electronic format is managed internally through the *Policy on Retention of Records Containing PHI*, the *Information Security Policy*, the *Information Security Code of Conduct*, the *PHI Handling Standard and Procedure*, and appropriate agreements. Where records of PHI will be accessible, retained, or disposed of by a third party, CCO's Services Agreement, which contains robust privacy provisions in its Schedule for Third Party Agreements, ensures that all third parties secure and dispose of PHI in accordance with CCO's applicable retention periods.

The following documents outline CCO's compliance with this requirement:

1. *Retention of Records Containing Personal Health Information*, LPO
2. *CCO's Privacy Policy*, LPO
3. *Enterprise Information Security Policy*, EISO
4. *Information Security Code of Conduct and Acceptable Use Policy*, EISO
5. *Secure Transfer of Personal Health Information Policy,* LPO
6. *Secure Transfer of Personal Health Information Standard*, LPO
7. *Research Data Disclosure Agreement,* LPO and A&I
8. *Application for Disclosure of Information from CCO for Research Purposes,* A&I
9. *Data Sharing Agreement Template,* LPO
10. *Data Sharing Agreement Initiation Procedure,* LPO
11. *Data Use and Disclosure Standard,* LPO and A&I

12. *Privacy Audit and Compliance Policy*, LPO
13. *Privacy Breach Management Policy,* LPO
14. *Data Back-up Policy*, Technology Services
15. *Data Back-up Procedure,* Technology Services
16. *Digital Personal Health Information Handling Standard,* EISO
17. *Digital Personal Health Information Handling Procedure*, EISO
18. *Open Media Logs*, Technology Services
19. *Session Logs*, Technology Services
20. *Services Agreement -Template Schedule for Third Party Agreements,* LPO
21. *Log of Third Party Service Providers with Access to PHI,* LPO
22. *Security Audit, Testing and Compliance Policy and Standard,* EISO

All requirements for this section have been met.

Security: Requirements of Section 6 of the Manual: Policy and Procedures for Secure Retention of Records of PHI on Mobile Devices.CCO has implemented a Digital PHI Handling Standard and Procedure that specifically includes the policy requirements, as defined in the Manual, for ensuring the protection of PHI records retained on mobile devices. The Standard and Procedure also address the retention of PHI on external storage media and use of PHI in non-production environments, ensuring consistency in application of the Manual's decision criteria regarding PHI use.

The following documents outline CCO's compliance with this requirement:

1. *Enterprise Information Security Policy,* EISO
2. *Information Security Code of Conduct and Acceptable Use Policy,* EISO
3. *Logical Access Control Standard,* EISO
4. *Cryptography Standard,* EISO
5. *Mobile Device Policy,* Technology Services
6. *Mobile Device and Pager Procedure,* Technology Services

7. *Digital Personal Health Information Handling Standard,* EISO
8. *Digital Personal Health Information Handling Procedure*, EISO
9. *De-Identification Guidelines,* LPO
10. *Data Back-up Policy*, Technology Services
11. *Digital Media Disposal Procedure*, EISO
12. *Digital Media Disposal Standard*, EISO

All requirements for this section have been met.

Security: Requirements of Section 7 of the Manual: Policy and Procedures for Secure Transfer of Records of PHI.

The security requirements for the secure transfer of PHI are set out in CCO's *Secure Transfer of PHI Standard*. CCO has documented standards for the use of cryptographic technologies and logical access controls. External parties' secure transfer obligations are managed through DSAs and other third party service provider agreements, all in accordance with *CCO's Secure Transfer of PHI Standard*. Collectively, these standards and agreements provide for a technical and administrative framework that supports the secure transfer of confidential information, including PHI.

The following documents outline CCO's compliance with this requirement:

1. *Secure Transfer of Personal Health Information Policy,* LPO
2. *Secure Transfer of Personal Health Information Standard*, LPO
3. *Courier Transfer of Personal Health Information Procedure*, LPO and Technology Services
4. *Exchanging Personal Health Information via Application Services Procedure,* LPO and Technology Services
5. *Exchanging Encrypted Personal Health Information on Digital Media,* LPO and Technology Services
6. *Exchanging Personal Health Information via Secure Managed File Transfer Procedure,* LPO and Technology Services
7. *Fax Transmission of Personal Health Information Procedure*, LPO and Technology Services

8. *In Person Transfer of Personal Health Information Procedure*, LPO and Technology Services
9. *Transfer of Personal Health Information by Regular Mail Procedure*, LPO and Technology Services
10. *Statement of Confidentiality,* LPO and Human Resources
11. *Privacy Audit and Compliance Policy,* LPO
12. *Enterprise Information Security Policy*, EISO
13. *Cryptography Standard,* EISO
14. *Logical Access Control Standard,* EISO
15. *Logging, Monitoring and Auditing Standard,* EISO
16. *Logging, Monitoring and Auditing Procedure,* EISO
17. *Digital Personal Health Information Handling Standard,* EISO
18. *Digital Personal Health Information Handling* Procedure, EISO
19. *Information Security Code of Conduct and Acceptable Use Policy*, EISO
20. *Security Audit, Testing and Compliance Standard,* EISO
21. *Information Security Program Framework*, EISO

	**All requirements for this section have been met.**

Security: Requirements of Section 8 of the Manual: Policy and Procedures for Secure Disposal of Records of PHI.

CCO has in place policies and practices to ensure the secure disposal of paper and electronic copies of records containing PHI. Where records of PHI will be disposed of by a third party service provider, CCO's Services Agreement, which contains robust privacy provisions in its Schedule for Third Party Agreements, ensures that all third parties are required to secure and dispose of PHI in accordance with CCO's security standards.

The following documents outline CCO's compliance with this requirement:

1. *Physical Security Policy,* Facilities
2. *Hard Copy Personal Health Information Disposal Procedure*, Facilities

3. *Enterprise Information Security Policy*, EISO
4. *Digital Media Disposal Standard,* EISO
5. *Digital Media Disposal Procedure,* EISO
6. *Services Agreement - Template Schedule for Third Party Agreements,* LPO
7. *Operational Security Standard,* EISO
8. *Security Audit, Testing and Compliance Standard,* EISO
9. *Information Security Code of Conduct and Acceptable Use Policy*, EISO

All requirements for this section have been met.

Security: Requirements of Section 9 of the Manual: Policy and Procedures Relating to Passwords.

CCO has implemented policies and procedures with respect to supporting passwords for authentication to information systems, equipment, resources, applications and programs. These policies and procedures represent a foundation from which technical controls are implemented, including controls to identify, authenticate, and authorize users and systems accessing CCO information resources. The policies also include the requirement to include risk based decisions regarding the context of any given authentication approach.

The following documents outline CCO's compliance with this requirement:

1. *Enterprise Information Security Policy*, EISO
2. *Logical Access Control Standard,* EISO
3. *Information Security Code of Conduct and Acceptable Use Policy,* EISO
4. *Logging, Monitoring and Auditing Standard,* EISO
5. *Logging, Monitoring and Auditing Procedure,* EISO

All requirements for this section have been met.

Security: Requirements of Section 10 of the Manual: Policy and Procedure for Maintaining and Reviewing System Control and Audit Logs.

CCO has implemented a system for the creation, maintenance and ongoing review of system control and audit logs that are consistent with evolving industry standards and that are commensurate with the amount and sensitivity of the PHI maintained, with the number and nature of agents with access to PHI and with the threats and risks associated with the PHI.

The following documents outline CCO's compliance with this requirement:

1. *Enterprise Information Security Policy*, EISO
2. *Information Security Code of Conduct and Acceptable Use Policy,* EISO
3. *Logging, Monitoring and Auditing Standard,* EISO
4. *Logging, Monitoring and Auditing Procedure,* EISO
5. *Information Security Incident & Breach Response Standard*, EISO
6. *Incident Management Framework*, EISO
7. *Security Audit, Testing, and Compliance Standard*, EISO

	**All requirements for this section have been met.**

Security: Requirements of Section 11 of the Manual: Policy and Procedure for Patch Management.

CCO's Operational Security Standard and Operational Security Patching Procedure set out CCO's standard operating practices for patch management. These practices provide baseline patching of operating systems and applications designed to support the security accessibility and reliability of CCO data holdings. Technology and process enhancements to patching are implemented on a regular basis.

The following documents outline CCO's compliance with this requirement:

1. *Enterprise Information Security Policy*, EISO
2. *Operational Security Standard,* Technology Services
3. *Information Security Code of Conduct and Acceptable Use Policy,* EISO
4. *Operational Security – Patching Procedure*, Technology Services
5. *Operational Security – Patch Management Standard,* Technology Services
6. *Security Audit, Testing, and Compliance Standard*, EISO

f

All requirements for this section have been met.

Security: Requirements of Section 12 of the Manual*:* Policy and Procedures Related to Change Management.

CCO has implemented change management practices based on alignment to the Information Technology Infrastructure Library (**ITIL**) standards for service management. In early 2016, CCO revised and supplemented its change management practices to clarify roles, improve testing requirements, among other improvements and has initiated a post implementation review (**PIR**) process, with mandatory presentations on all emergency changes.

The following documents outline CCO's compliance with this requirement:

1. *Enterprise Information Security Policy*, EISO
2. *Information Technology Change Management Policy*, Technology Services
3. Information Technology Change Subcommittee, Technology Services

All requirements for this section have been met.

Security: Requirements of Section13 of the Manual: Policy and Procedures for Backup and Recovery of Records of PHI.

CCO has implemented operational policies and procedures for the back-up and recovery of records of PHI. These documents, in conjunction with the third party service provider agreements, address administrative processes, technical practices for backups and data recovery, and the controls relevant to the storage of backup media.

The following documents outline CCO's compliance with this requirement:

1. *Enterprise Information Security Policy*, EISO
2. *Data Backup Policy,* Technology Services
3. *Data Backup Procedure,* Technology Services
4. *Disaster Recovery Plan,* Technology Services
5. *Services Agreement - Template Schedule for Third Party Agreements,* LPO
6. *Secure Transfer of Personal Health Information Policy,* LPO

7. *Secure Transfer of Personal Health Information Standard*, LPO
8. *Retention of Records Containing Personal Health Information*, LPO
9. *Operational Security Standard,* Technology Services
10. *Session Logs,* Technology Services
11. *Media Logs*, Technology Services and Third Party Service Provider

	**All requirements for this section have been met.**

Security: Requirements of Section 14 of the Manual*:* Policy and Procedures on the Acceptable Use of Technology.

CCO has implemented policies and practices outlining the acceptable use of information systems, technologies, equipment, resources, applications and programs. These policies are complemented by both online and in person training sessions to ensure CCO employees understand the acceptable use of technology in their job role.

The following documents outline CCO's compliance with this requirement:

1. *Enterprise Information Security Policy*, EISO
2. *Information Security Code of Conduct and Acceptable Use Policy,* EISO
3. *Logging, Monitoring and Auditing Standard,* EISO
4. *Logging, Monitoring and Auditing Procedure,* EISO
5. *Security Audit, Testing, and Compliance Standard*, EISO
6. *Acceptable Use of Social Media Policy*, HR

	**All requirements for this section have been met.**

Security: Requirements of Section 15 of the Manual: Policy and Procedures in Respect of Security Audits.

CCO has put in place standards and practices that outline the types of security audits that are required to be conducted. These practices include review of compliance with the security policies, procedures and practices; threat risk assessments (**TRAs**); security reviews or assessments; and technical vulnerability assessments (**VAs**); penetration testing and ethical hacks (when required) and reviews of system control and audit logs.

The following documents outline CCO's compliance with this requirement:

1. *Enterprise Information Security Policy*, EISO
2. *Security Risk Management Standard*, EISO
3. *Information Security Program Framework,* EISO
4. *Operational Security Standard*, Technology Services
5. *CCO's Privacy Policy*, LPO
6. *Logging, Monitoring, and Auditing Standard,* EISO
7. *Logging, Monitoring, and Auditing Procedure,* EISO
8. *Threat Risk Assessment Template,* EISO
9. *Security Audit, Testing, and Compliance Standard,* EISO
10. *Log of Security Audits*, EISO

	**All requirements for this section have been met.**

Security: Requirements of Section 16 of the Manual: Log of Security Audits.

CCO maintains a log of security audits that have been completed. This log is inclusive of the nature and type of the security audit conducted; the date that the security audit was completed; the agent(s) responsible for completing the security audit; the recommendations arising from the security audit; the agent(s) responsible for addressing each recommendation; the date that each recommendation was or is expected to be addressed; and the manner in which each recommendation was or is expected to be addressed

The following documents outline CCO's compliance with this requirement:

1. *Security Risk Management Standard,* EISO
2. *Operational Security Standard*, Technology Services
3. *Enterprise Information Security Framework*, EISO
4. *Log of Security Audits,* EISO

	**All requirements for this section have been met.**

Security: Requirements of Section 17 of the Manual: Policy and Procedures for Information Security Breach Management.

EISO has implemented practices for the identification, reporting, containment, notification, investigation and remediation of information security incidents. This work has synergy with the privacy breach management processes and leverages the security and privacy auditing and logging technologies.

The following documents outline CCO's compliance with this requirement:

1. *Enterprise Information Security Policy*, EISO
2. *Information Security Incident and Breach Response Standard*, EISO
3. *Incident Management Framework*, EISO
4. *Log of Security Incidents,* EISO
5. *Information Security Code of Conduct and Acceptable Use Policy,* EISO
6. *Privacy Breach Management Policy*, LPO
7. *Security Audit, Testing, and Compliance Standard,* EISO

	**All requirements for this section have been met.**

Security: Requirements of Section 18 of the Manual: Log of Information Security Breaches.

CCO has implemented practices for the identification, reporting, containment, notification, investigation and remediation of information security incidents.

The following documents outline CCO's compliance with this requirement:

1. *Log of Security Incidents,* EISO
2. *Information Security Incident and Breach Response Standard*, EISO

	**All requirements for this section have been met.**

Part 3: Human Resources Documentation

Human Resources Documentation Matrix

CCO Human Resources Matrix	Requirement 1	Requirement 2	Requirement 3	Requirement 4	Requirement 5	Requirement 6	Requirement 7	Requirement 8	Requirement 9	Requirement 10	Requirement 11
CCO Procurement Policy					x						
CCO's Privacy Policy	x	x	x								
Code of Conduct											x
Confidentiality Policy					x						
Consulting Agreement					x	x					
Contract Management System					x		x				
Core Privacy and Security Training eLearning Curriculum	x					x	x				
Employee Exit Process										x	
Enterprise Information Security Policy			x	x							
Information Security Code of Conduct and Acceptable Use Policy			x	x						x	
Information Security Policy			x	x							
Job Descriptions for the Position(s) Delegated Day-to-Day Authority to Manage the Privacy Program								x			
Log of Privacy and Security Training Completion	x	x	x	x							
Privacy and Security Training and Awareness Procedure	x	x	x	x	x						

CCO Human Resources Matrix	Requirement 1	Requirement 2	Requirement 3	Requirement 4	Requirement 5	Requirement 6	Requirement 7	Requirement 8	Requirement 9	Requirement 10	Requirement 11
Privacy Audit and Compliance Policy	**x**		**x**							**x**	
Privacy Breach Management Policy	**x**										
CCO Procurement Policy					**x**						
Record Series on "Employee Management: Individual Employee Files"											**x**
Statement of Confidentiality	**x**					**x**				**x**	
Termination of Employment Policy										**x**	
Payroll System					**x**		**x**				
HCMS System					**x**					**x**	

IPC Requirements

Human Resources: Requirements of Section 1 of the Manual: Policy and Procedures for Privacy Training and Awareness.

CCO has a comprehensive privacy training and awareness program in place to ensure that its individual agents (*e.g.*, employees) are aware of CCO privacy policies, procedures and best practices, as described herein. The mandatory new employee privacy and security training program and the mandatory annual privacy and security refresher training program, ensure that all CCO employees and all other agents of CCO that will have access to CCO's systems or PHI are informed of their privacy and security responsibilities, in addition to CCO's legislative compliance obligations. All of these individuals, upon completion of the training, must electronically accept a Privacy and Security Acknowledgment form that confirms their understanding of the training and acceptance of their obligations and responsibilities. This ensures that all users of CCO systems, including systems containing PHI, have received the requisite privacy and security training. CCO's extensive training and awareness program plays a key role in fostering a culture of privacy and security within the organization.

The following documents outline CCO's compliance with this requirement:

1. *CCO's Privacy Policy*, LPO
2. *Privacy and Security Training and Awareness Procedure*, LPO
3. *Core Privacy & Security Training eLearning Curriculum*, LPO
4. *Privacy Audit and Compliance Policy*, LPO
5. *Privacy Breach Management Policy*, LPO
6. *Privacy Breach Management Manual,* LPO
7. *Statement of Confidentiality*, LPO and Human Resources
8. *Log of Privacy and Security Training Completion*, LPO
9. *Privacy Governance Framework*, LPO

All requirements for this section have been met.

Human Resources: Requirements of the Manual 2 of the Manual: Log of Attendance at initial privacy orientation and Ongoing Privacy Training.

CCO tracks completion of its privacy training program through the electronic acceptance of a Privacy and Security Acknowledgement Form. CCO's IT solution for privacy & security training ensures that an individual cannot electronically accept this form without first reviewing the applicable privacy & security training.

The following documents outline compliance with this requirement:

1. *CCO's Privacy Policy*, LPO
2. *Privacy and Security Training and Awareness Procedure*, LPO
3. *Log of Privacy and Security Training Completion*, LPO

	**All requirements for this section have been met.**

Human Resources: Requirements of Section 3 of the Manual: Policy and Procedures for Security Training and Awareness.

CCO has a comprehensive security training and awareness program in place to ensure that its individual agents are aware of CCO security policies, procedures and best practices as described herein. Through the employee privacy and security training program and the annual privacy and security refresher training program, all CCO employees and all other agents of CCO that will have access to CCO's systems or PHI are informed of their security responsibilities and obligations. This ensures that all users of CCO systems, including systems containing PHI, have received the requisite security training. CCO's extensive training and awareness program plays a key role in fostering a culture of privacy and security in the organization.

The following documents outline compliance with this requirement:

1. *CCO's Privacy Policy*, LPO
2. *Enterprise Information Security Policy*, EISO
3. *Information Security Code of Conduct and Acceptable Use Policy,* EISO
4. *Privacy and Security Training and Awareness Procedure,* LPO
5. *Core Privacy & Security Training eLearning Curriculum*, LPO
6. *Privacy Audit and Compliance Policy*, LPO
7. *Log of Privacy and Security Training Completion*, LPO

	**All requirements for this section have been met.**

Human Resources: Requirements of Section 4 of the Manual: Log of Attendance at Initial Security Orientation and Ongoing Security Training.

CCO tracks completion of its security training program through the electronic acceptance of a *Privacy and Security Acknowledgement Form*. CCO's IT solution for privacy & security training ensures that an individual cannot electronically accept this form without first reviewing the applicable privacy & security training.

The following documents outline compliance with this requirement:

1. *Enterprise Information Security Policy,* EISO
2. *Information Security Code of Conduct and Acceptable Use Policy,* EISO
3. *Privacy and Security Training and Awareness Procedure,* LPO
4. *Log of Privacy and Security Training Completion,* LPO

	**All requirements for this section have been met.**

Human Resources: Requirements of Section 5 of the Manual: Policy and Procedure for the Execution of Confidentiality Agreement with Agents.

CCO ensures that the confidentiality obligations are clearly articulated at the outset of engagement with the organization. Agreements are in place for all individual agents working for or under contract with CCO, which clearly outline the importance of preserving the confidentiality of all information of a private or sensitive nature, including all PHI.

The following documents outline CCO's compliance with this requirement:

1. *Confidentiality Policy*, LPO and Human Resources
2. *Privacy and Security Training and Awareness Procedure,* LPO
3. *Automated HCMS System*, Human Resources
4. *CCO Procurement Policy*, Strategic Sourcing
5. *Consulting Agreement – Template*, LPO

6. *Services Agreement - Template Schedule for Third Party Agreements,* LPO
7. *Contract Management System*, Strategic Sourcing
8. *Payroll System*, Human Resources

✓	**All requirements for this section have been met.**

Human Resources: Requirements of Section 6 of the Manual: Template Confidentiality Agreement with Agents.

CCO has put in place administrative safeguards to ensure that CCO employees and all other agents of CCO that will have access to CCO's systems or PHI will meet their obligations to protect confidential information, including PHI, to which they may have access in the course of performing their job duties.

The following documents outline CCO's compliance with this requirement:

1. *Statement of Confidentiality*, LPO and Human Resources
2. *Confidentiality Agreement, Board and Board Committees,* LPO
3. *Services Agreement - Template Schedule for Third Party Agreements,* LPO
4. *Consulting Agreement – Template*, LPO
5. *Core Privacy & Security Training eLearning Curriculum,* LPO

✓	**All requirements for this section have been met.**

Human Resources: Requirements of Section 7 of the Manual: Log of Executed Confidentiality Agreements with Agents.

CCO's Human Resources Department maintains a log of confidentiality agreements executed by employees of CCO. LPO maintains a log of confidentiality agreements executed by CCO Board and Board Committee members. Agreements executed by third parties retained by CCO, with access to PHI, include specific terms outlining the third party's confidentiality obligations in respect of the PHI. A log of such agreements is maintained by CCO's Strategic Sourcing Office through its Contract Management System.

The following documents outline CCO's compliance with this requirement:

1. *Contract Management System*, Strategic Sourcing
2. *Payroll System*, Human Resources
3. *Core Privacy & Security Training eLearning Curriculum,* LPO

	**All requirements for this section have been met.**

Human Resources: Requirements of Section 8 of the Manual: Job Descriptions for the Position(s) Delegated Day-to-Day Authority to Manage the Privacy Program.

CCO has in place an effective governance structure including delegated roles to carry out the Privacy Program at CCO.

The following documents outline compliance with this requirement:

1. *Assistant General Counsel & Director Privacy Job Description,* LPO
2. *Privacy Specialist Job Description,* LPO
3. *Senior Privacy Specialist Job Description*, LPO
4. *Group Manager, Privacy Job Description,* LPO

	**All requirements for this section have been met.**

Human Resources: Requirements of Section 9 of the Manual: Job Descriptions for the Position(s) Delegated Day-to-Day Authority to Manage the Security Program.

CCO has in place an effective governance structure including delegated roles to carry out the Security Program at CCO.

The following documents outline CCO's compliance with this requirement:

1. *Group Manager, Information Security Job Description ,* EISO
2. *Senior Information Security Advisor, Job Description*, EISO
3. *Information Security Advisor, Job Description,* EISO

	**All requirements for this section have been met.**

Human Resources: Requirements of Section 10 of the Manual: Policy and Procedures for Termination or Cessation of the Employment or Contractual Relationship.

The process that is followed at CCO upon termination or cessation of the individual agent (*e.g.*, employment or under contract) relationship, is primarily outlined in the Employee Exit Process. In addition, the policies and procedures listed below ensure that when an individual agent relationship with CCO ends, all access privileges to CCO's systems and premises are terminated, and all property including records of PHI, access cards and keys are returned in a timely fashion.

The following documents outline compliance with this requirement:

1. *Employee Exit Process*, Human Resources
2. *Automated HCMS System*, Human Resources
3. *Statement of Confidentiality*, LPO and Human Resources
4. *Termination of Employment Policy,* Human Resources
5. *Information Security Code of Conduct and Acceptable Use Policy,* EISO
6. *Exiting Employee Data Management Policy,* Technology Services
7. *Privacy Audit and Compliance Policy*, LPO

	**All requirements for this section have been met.**

Human Resources: Requirements of Section 11 of the Manual: Policy and Procedures for Discipline and Corrective Action.

CCO has a formal progressive discipline policy that is invoked as appropriate whenever an employee fails to comply with any of CCO's privacy and security and related policies. The *Progressive Discipline Policy* includes requirements relating to the investigation, documentation, and follow-up in respect of any reported non-compliance. The privacy and security-related policy owners are responsible for the enforcement of their policies, and are supported by Human Resources and the LPO.

The following documents outline compliance with this requirement:

1. *Code of Conduct*, Human Resources
2. *Statement of Confidentiality*, LPO and Human Resources
3. *Privacy & Security Acknowledgment Form,* LPO
4. *Progressive Discipline Policy*, Human Resources
5. *Privacy Breach Management Policy*, LPO
6. *Privacy Breach Management Manual,* LPO
7. *Information Security Code of Conduct & Acceptable Use Policy*, EISO

	**All requirements for this section have been met.**

Part 4: Organizational and Other Documentation

Organizational and Other Documentation Matrix

CCO Organizational and Other Documentation Matrix	Requirement 1	Requirement 2	Requirement 3	Requirement 4	Requirement 5	Requirement 6	Requirement 7	Requirement 8
Annual Privacy Report	x							
Business Continuity Framework								x
Business Continuity Plan								x
CCO Board of Directors Orientation Handbook		x						
CCO's Privacy Policy	x					x	x	
Charter - CCO Board of Directors	x	x						
Charter - Information Management and Information Technology Committee of the Board of Directors	x	x						
Data Analytics Management Committee Terms of Reference			x					
Data Disclosure Working Group Terms of Reference			x					
Disaster Recovery Plan								x

CCO Organizational and Other Documentation Matrix	Requirement 1	Requirement 2	Requirement 3	Requirement 4	Requirement 5	Requirement 6	Requirement 7	Requirement 8
Enterprise Information Security Policy		**x**						
ERM Framework				**x**				
Enterprise Risk Register				**x**	**x**			
Data Disclosure Subcommittee Terms of Reference			**x**					
Information Management and Information Technology Steering Committee Terms of Reference			**x**					
Information Security Program Framework		**x**						
Information Technology Management and Architecture Committee Terms of Reference			**x**					
Log of IPC Recommendations						**x**		
Log of Privacy Breaches						**x**		
Log of Privacy Impact Assessments						**x**		
Log of Privacy Inquiries and Complaints						**x**		
Log of Security Audits						**x**		
Log of Security Incidents						**x**		

CCO Organizational and Other Documentation Matrix	Requirement 1	Requirement 2	Requirement 3	Requirement 4	Requirement 5	Requirement 6	Requirement 7	Requirement 8
Privacy and Information Security Risk Management Procedure				**x**		**x**		
Privacy Audit and Review Standard						**x**		
Privacy Breach Management Manual						**x**		
Privacy Breach Management Policy						**x**		
Privacy Governance Framework	**x**							
Privacy Risk Register						**x**	**x**	
Security Risk Management Standard				**x**				

IPC Requirements

Organizational and Other: Requirements of Section 1 of the Manual*:* Privacy Governance and Accountability Framework.

CCO's Privacy Governance Framework identifies the Chief Executive Officer as ultimately accountable for CCO's compliance with PHIPA and its Regulation as well as with all privacy policies, procedures and practices at CCO. The CPO has been delegated authority to manage the Privacy Program and is supported by the LPO in carrying out the day-to-day duties. Significant Privacy Program initiatives and changes to the Privacy Program are presented to the CCO Board of Directors. The IM/IT Committee of the Board of Directors oversees the CCO Privacy Program.

CCO's privacy governance structure informs its overall privacy management practices, including leadership, strategy, priorities and risk management. The privacy governance structure provides assurance that the strategies, policies, standards, processes and resources to manage privacy risk are aligned with CCO's objectives and are consistent with applicable laws, standards and best practices.

The following documents outline compliance with this requirement:

1. *CCO's Privacy Policy*, LPO
2. *Privacy Governance Framework,* LPO
3. *Statement of Information Practices*, LPO
4. *Annual Privacy Report,* LPO
5. *Charter – Information Management and Information Technology Committee of the Board of Directors,* LPO
6. *Charter – CCO Board of Directors,* LPO

✓	**All requirements for this section have been met.**

Organizational and Other: Requirements of Section 2 of the Manual*:* Security Governance and Accountability Framework.

CCO's security policy outlines the CEO's accountability for ensuring the security of PHI as well as the appropriate delegation of day-to-day authority to manage the security program. The CCO Board of Directors Orientation Handbook includes briefing elements of both the Privacy and Security program. CCO's ET and Board are apprised of the security program updates through the Vice President of Technology Services and CPO

briefing updates bi-annually. Quarterly cyber risk updates are provided to the IM/IT Committee of the Board of Directors.

The following documents outline CCO's compliance with this requirement:

1. *Enterprise Information Security Policy*, EISO
2. *Information Security Program Framework,* EISO
3. *CCO Board of Directors Orientation Handbook,* LPO
4. *Charter – Information Management and Information Technology Committee of the Board of Directors*, LPO
5. *Charter – CCO Board of Directors,* LPO

All requirements for this section have been met.

Organizational and Other: Requirements of Section 3 of the Manual*:* Terms of Reference for Committees with Roles with respect to the Privacy Program and/or Security Program.

CCO has terms of reference for every committee that has a role in the Privacy and Security Programs. In addition, the LPO, EISO, CPO, and VP Technology Services are supported by the ET when addressing significant privacy and security issues.

The following documents outline compliance with this requirement:

1. *Information Management and Information Technology Steering Committee Terms of Reference,* Enterprise Services Council
2. *Data Analytics Management Committee Terms of Reference,* A&I
3. *Data Disclosure Subcommittee Terms of Reference,* A&I
4. *Data Disclosure Working Group Terms of Reference,* A&I
5. *Information Technology Management and Architecture Committee Terms of Reference,* Technology Services
6. *Technical Subcommittee Terms of Reference,* Technology Services
7. *Information Management and Information Technology Subcommittee of the Board of Directors Terms of Reference*, LPO

	**All requirements for this section have been met.**

Organizational and Other: Requirements of Section 4 of the Manual: Corporate Risk Management Framework.

CCO has an ERM Framework (which establishes CCO's Risk Tolerance Levels) which is designed to ensure compliance with CCO's ERM requirements under Management Board of Cabinet's Agencies and Appointments Directive and CCO's MOU with the MOHLTC. This enterprise-wide document is complemented by CCO's Security Risk Management standard and the *Privacy and Information Security Risk Management Procedure.* Together, these documents comprehensively address all roles and responsibilities associated with the identification, assessment, management and monitoring of privacy and security risks throughout CCO.

The following documents outline compliance with this requirement:

1. *Privacy and Information Security Risk Management Procedure,* LPO & EISO
2. *Privacy Risk Register,* LPO
3. *Security Risk Management Standard,* EISO
4. *ERM Framework*, LPO
5. *Enterprise Risk Register,* LPO

	**All requirements for this section have been met.**

Organizational and Other: Requirements of Section 5 of the Manual: Corporate Risk Register.

CCO has implemented an enterprise wide risk inventory process, which captures enterprise-wide risks. CCO has also expanded this process to establish risk registers at the program, portfolio, and project level. In terms of its Privacy, CCO developed a comprehensive Register logs which reflects all privacy risks respectively throughout CCO. CCO's Privacy Risk Register logs both privacy risks as well as recommendations to mitigate and manage those risks for any risk identified during the course of a privacy review.

The following documents outline CCO's compliance with this requirement:

1. *Privacy Risk Register*, LPO
2. *Enterprise Risk Register,* LPO

All requirements for this section have been met.

Organizational and Other: Requirements of Section 6 of the Manual*:* Policy and Procedures for Maintaining a Consolidated Log of Recommendations.

CCO's Privacy and Information Security Risk Management Procedure requires the maintenance of a Privacy Risk Register which logs both privacy risk as well as recommendations to mitigate and manage those risks. The log includes risks or recommendations identified through PIAs, privacy audits, privacy reviews, complaint investigations, breach reports and IPC reviews.

Likewise, CCO's Privacy and Information Security Risk Management Procedure and Security Risk Management Standard require the maintenance of the Security Risk Register which logs security risks and the corresponding asset, vulnerability, and impact information. The log aggregates risks identified through TRAs, security audits, security reviews, incidents and operational security activities.

The following documents outline compliance with this requirement:

1. *CCO's Privacy Policy*, LPO
2. *Privacy Breach Management Policy*, LPO
3. *Privacy Breach Management Manual,* LPO
4. *Privacy Impact Assessment Standard,* LPO
5. *Privacy Audit and Compliance Policy*, LPO
6. *Privacy and Information Security Risk Management Procedure,* LPO & EISO
7. *Security Risk Management Standard,* EISO
8. *Security Audit, Testing, and Compliance Standard,* EISO
9. *Information Security Incident & Breach Response Standard,* EISO
10. *Privacy Risk Register*, LPO
11. *Log of Privacy Impact Assessments*, LPO
12. *Log of Privacy Breaches*, LPO
13. *Log of Privacy Inquiries and Complaints*, LPO
14. *Log of IPC Recommendations*, LPO
15. *Log of Security Audits*, EISO

16. *Log of Security Incidents*, EISO

	**All requirements for this section have been met.**

Organizational and Other: Requirements of Section 7 of the Manual*:* Consolidated Log of Recommendations.

Currently, CCO consolidates recommendations through the use of several logs (i.e. breach log, PIA log, Inquiries and complaints log, Procurement PIA log, IPC recommendations log). CCO has developed central Privacy Risk Register which logs both privacy risks as well as recommendations to mitigate and manage those risks for any risk identified during the course of a privacy review. The log will include risks or recommendations identified through PIAs, privacy audits, privacy reviews, complaint investigations, and IPC reviews.

CCO also maintains a Security Risk Register which is a consolidated log of risks and recommendations identified through TRAs, security audits, security reviews, incidents and operational security activities.

The following documents outline CCO's compliance with this requirement:

1. *CCO's Privacy Policy*, LPO
2. *Privacy Risk Register,* LPO
3. *Log of Privacy Impact Assessments,* LPO
4. *Log of Privacy Breaches,* LPO
5. *Log of Privacy Inquiries and Complaints,* LPO
6. *Log of IPC Recommendations,* LPO
7. *Log of Security Audits,* EISO
8. *Log of Security Incidents,* EISO

	**All requirements for this section have been met.**

Organizational and Other: Requirements of Section 8 of the Manual*:* Business Continuity and Disaster Recovery Plan.

In 2013, CCO improved its Business Continuity and Disaster Recovery strategies with the re-drafting and implementation of a robust Business Continuity Plan and separate Disaster Recovery Plan. The Business Continuity Plan is also supported by the Business Continuity Framework. These documents comprehensively address identification, notification, documentation, and assessment of an interruption or threat. They further address the activation of the Disaster Recovery Plan and/or Business Continuity Plan, as applicable, including roles and responsibilities, decision-making, documentation, and resumption activities.

1. *Business Continuity Plan,* Technology Services
2. *Business Continuity Framework*, Technology Services
3. *Business Continuity Worksheet,* Technology Services
4. *Disaster Recovery Plan*, Technology Services

All requirements for this section have been met.

Privacy, Security and Other Indicators

Part 1 – Privacy Indicators

(All indicators are for the period of November1, 2013 to October 31, 2016)

General Privacy Policies, Procedures and Practices

IPC Key Indicator Required		CCO's Response
1	Record of dates for review of policies and procedures since the prior review of the IPC.	A number of policies and procedures were reviewed since the last review of the IPC. Please refer to *Appendix "C"* for a log and brief description of the policies and procedures reviewed and amended within the time periods November 1, 2013 – October 31, 2016.
2	Log of amendments, date of amendment and description of amendment, as a result of the prior review of the IPC.	A number of policies and procedures were reviewed since the last review of the IPC. Please refer to *Appendix "C"* for a log and brief description of the policies and procedures that were reviewed and amended within the time periods November 1, 2013 – October 31, 2016.
3	Record of new policies and procedures developed as a result of the prior review of the IPC.	There were no new policies and procedures developed as a result of the prior review of the IPC.
4	Record of dates and nature of communication regarding amendments.	All privacy policies and/or procedures which were amended and approved have been communicated through CCO's Intranet, public-facing website, and/or targeted emails. Please refer to *Appendix "C*" for a log and brief description of amendments as well as the date and nature of communication regarding amendments to the policies.
5	Record of changes to public communication materials, as a result of the prior review of the IPC.	There were no changes related to public communication materials as a result of the prior IPC review. Any changes that were made were due to regular updates to policies and procedures.

Collection

IPC Key Indicator Required		CCO's Response
1	The number of data holdings containing PHI	CCO has 42 data holdings which are operating under the PHIPA authority of a PE CCO has 19 data holdings which are operating under the PHIPA authority of a PP.
2	The number of statements of purpose developed for data holdings containing PHI.	CCO has 42 statements of purpose developed for CCO's data holdings for programs operating under the PHIPA authority of a PE CCO has 19 statements of purpose developed for CCO's data holdings for programs operating under the PHIPA authority of a PP
3	The number and list of the statements of purpose for data holdings containing PHI that were reviewed since the prior review of the IPC.	CCO has reviewed all 42 statement of purposes for CCO's data holdings for programs operating under the PHIPA authority of a PE CCO has reviewed all 19 statements of purpose for CCO's data holdings for programs operating under the PHIPA authority of a PP CCO's statements of purpose are reviewed annually during the review of CCO's Privacy Policy, and also on an ongoing basis by the CCO Business Unit responsible for ensuring that the statement of purpose is up to date, as set out in CCO's Privacy Policy. CCO's statements of purpose have been reviewed in accordance with this frequency. Please see *Appendix "J"* for the complete list of data holdings for programs operating as a PE and PP along with the statement of purpose for each data holding.
4	Log of amendments, date of amendment and description of amendment made to statements of purpose as a	CCO has amended 1 statement of purpose and added 15 new data holdings to the log of data holdings.

	result of the prior review of the IPC.	The following was amended: • *OBSP* – the name was changed to Integrated Cancer Management System (**ICMS**) to reflect the operation of the OBSP as a PP. The following data holdings were added to the list: • *DSP-RFNS* • *Cancer Level Reporting* • *Canadian Community Health Survey* • *Complex Continuing Care Reporting* • *Diagnostic Assessment Program (**DAP**) – Diagnostic Data Upload Tool (**DDUT**)* • *Specialized Service Oversight Information System* • *Incident case level stage data* • *Health based application model innovation group* • *National rehabilitation reporting system* • *Ontario Association of Community Care Access Centres (**OACCAC**)* • *Ontario Drug Benefit (**ODB**)* • *Ontario Mental Health Reporting system* • *OOC* • *Systemic treatment quality-based procedures* • *Hub-Fulfillment house* Statements of purpose were developed for the 15 new data holdings added since the previous review by the IPC. Please see *Appendix "J"* for the complete list of data holding for programs operating as PE and PP along with the statement of purpose for each data holding.

Use

IPC Key Indicator Required	**CCO's Response**

1	The number of agents granted approval to access and use PHI for purposes other than research.	Through the IDAR process, CCO has granted approval to 665 agents between the period of November 1, 2013 and October 31, 2016.
2	The number of requests received for the use of PHI for research, since the prior review of the IPC.	N/A.
3	The number of requests for the use of PHI for research purposes that were granted and that were denied, since the prior review of the IPC.	N/A.

Disclosure

IPC Key Indicator Required		**CCO's Response**
1	The number of requests received for the disclosure of PHI for purposes other than research, since the prior review of the IPC.	CCO in respect of the PP received zero request for PHI for purposes other than research. CCO in respect of the PE received 42 requests for PHI for purposes other than research.
2	The number of requests for the disclosure of PHI for purposes other than research that were granted and that were denied,	Of the 42 requests received for PHI in respect of the PE for purposes other than research, since the IPC's last review, 26 were approved.

	since the prior review of the IPC.	
3	The number of requests received for the disclosure of PHI for research purposes, since the prior review of the IPC.	There were 21 research requests received by CCO in respect to PP for PHI. There were 74 research requests received by CCO in respect of the PE for PHI. Note: The number of requests submitted between Nov. 1, 2013 to Oct 31, 2016 (Indicator 3) and the number of requests for which data was disclosed between Nov. 1, 2013 to Oct 31, 2016 (Indicator 4) have been included in these indicators. However, there may be a variance across the two indicators as they include requests which were submitted prior to Nov. 1, 2013 but data disclosed only in this review period and likewise these numbers may also include requests that were submitted by Oct 31, 2016 but data disclosed only later in the year upon the completion of the routine data disclosure process.
4	The number of requests for the disclosure of PHI for research purposes that were granted and that were denied, since the prior review of the IPC.	There were 14 research requests approved, and 2 denied, for the disclosure of PHI by CCO in respect of the PP There were 48 research requests approved, and 1 denied, for the disclosure of PHI by CCO in respect of the PE. Note: The number of requests submitted between Nov. 1, 2013 to Oct. 31, 2016 (Indicator 3) and the number of requests for which data was disclosed between Nov. 1, 2013 to Oct 31, 2016 (Indicator 4) have been included in these indicators. However, there may be a variance across the two indicators as they include requests which were submitted prior to Nov. 1, 2013 but data disclosed only in this review period and likewise these numbers may also include requests that were submitted by Oct 31, 2016 but data disclosed only later in the year upon the completion of the routine data disclosure process.
5	The number of Research Agreements executed with researchers to whom PHI was disclosed, since	There were 14 research agreements executed with researchers in respect of the PP. There were 47 research agreements executed with researchers in respect of the PE.

	the prior review of the IPC.	
6	The number of requests received for the disclosure of de-identified and/or aggregate information for both research and other purposes, since the prior review of the IPC.	There were 89 requests received for de-identified and/or aggregate information for both research and other purposes, in respect of the PP. There were 136 requests received for de-identified and/or aggregate information for both research and other purposes, in respect of the PE.
7	The number of acknowledgements or agreements executed by persons to whom de-identified and/or aggregate information was disclosed for both research and other purposes, since the prior review of the IPC.	70 agreements were signed for Surveillance, Epidemiology, and End Results Statistical (**SEER*Stat**).

DSAs

IPC Key Indicator Required		**CCO's Response**
1	The number of DSAs executed for the collection of personal health information by the PP or PE, since the prior review of the IPC.	From November 1, 2013 to October 31, 2016, there have been **21** DSAs executed or amended for the collection of PHI by CCO, under its PHIPA authority of a PE and a PP: • 10 DSAs were executed for the collection of PHI by CCO • **11** were amending agreements, including 3 amending agreements for the collection and disclosure of PHI between PE and PP programs within CCO.

		Of the 21, 19 are collections as a PE, and 2 are collections as PP. This includes 4 that were a collection as both a PE and a PP. CCO has also executed 177 master data sharing agreements (**MDSAs**) with HICs for the collection, use and disclosure of PHI as a PE or a PP. This is a one-time executed agreement with health information custodians, noting both parties' roles, responsibilities and obligations concerning the collection, use and disclosure of PHI. The MDSA is referenced in other subsequent agreements that CCO has with HICs, such as annual funding agreements and license agreements. MDSAs are executed in CCO's capacity as both a PE and PP.
2	The number of DSAs executed for the disclosure of PHI by the PP or PE, since the prior review of the IPC.	From November 1, 2013 to October 31, 2016, there have been **23** DSAs executed or amended for the disclosure of PHI by CCO, under the PHIPA authority of a PE and/or a PP: • **8** DSAs were executed for the disclosure of PHI by CCO • **15** were amending agreements Of the 23, 15 are disclosures as a PE, and 4 are disclosures as PP, and 4 are disclosures as both PE and PP.

Agreement with Third Party Service Providers

IPC Key Indicator Required		**CCO's Response**
1	The number of agreements executed with third party service providers with access to PHI, since the prior review of the IPC.	CCO has conducted a manual review of the number of agreements executed with third party service providers with access to PHI in the PE. From November 1, 2013 to October 31, 2016, there have been **six** agreements executed with third party service providers with access to personal health information in the PP and **six** agreements executed with third party service providers with access to PHI in the PE capacity.

		Note: CCO has controls in place to ensure third parties who are provided with access to PHI on CCO's systems receive privacy and security training and sign agreements that include confidentiality terms, within their third party agreements. CCO also ensures that access privileges to CCO's data holdings are renewed on an annual basis through the IDAR system.

Data Linkage

IPC Key Indicator Required		CCO's Response
1	The number and a list of data linkages approved, since the prior review of the IPC.	There have been 14 permanent/operational and 29 ad hoc data linkages approved since the prior review of the IPC. Please refer to *Appendix "D": Indicators – List of Data Linkages* Permanent/operational data linkages are linkages performed to set up data holdings, including both system based and manual linkages for ongoing operational and analytical purposes, and linkages across data holdings for purposes of ongoing routine reporting. Ad hoc data linkages are linkages conducted to produce a deliverable such as a report in response to an ad-hoc analysis and/or an exploratory analysis request. Some of these deliverables can become permanent/operational linkages over time. Ad hoc linkages include linkages performed solely for troubleshooting or investigative purposes.

PIAs

IPC Key Indicator Required	CCO's Response

1	The number and a list of PIAs completed since the prior review by the IPC and for each privacy impact assessment: • The data holding, information system, technology or program, • The date of completion of the PIA, • A brief description of each recommendation, • The date each recommendation was addressed or is proposed to be addressed, and • The manner in which each recommendation was addressed or is proposed to be addressed.	CCO has completed **15** PIAs since the IPC's last review of CCO in October 2013 for programs operating under the PHIPA authority of a PE and 5 PIAs under the PHIPA authority of PP. Please refer to *Appendix "E": Indicators – Summary from the Log of Privacy Impact Assessments*, for a list of PIAs completed by CCO from November 1, 2013 to October 31, 2016.
2	The number and a list of PIAs undertaken but not completed, since the prior review of the IPC and the proposed date of completion.	CCO has undertaken but not completed 3 PIAs since the IPC's last review of CCO in October 2014 for programs operating under the PHIPA authority of a PE. These are as follows: • GI Endoscopy PIA – Expected to be complete by August 31, 2017 • Integrate PIA Addendum – On hold • Real Time Measures/Electronic Patient Reported Experience Measure (**ePREM**) PIA – Expected to be complete by August 31, 2017 For programs operating under the PHIPA authority of a PP, there have not been any PIAs undertaken but not

		completed since the IPC's last review of CCO in October 2014.
3	The number and list of privacy impact assessments that were not undertaken but will be completed and the proposed date of completion.	**1** Planned PIA is scheduled to be completed for programs operating under the PHIPA authority of a PP. The following PIA is expected to complete by March 2017. • High Risk Lung Cancer There are not any PIAs scheduled to be completed by programs operating under the PHIPA authority of a PE.
4	The number of determinations made, since the prior review of the IPC, that a PIA is not required and, for each determination, the data holding, information system, technology or program at issue and a brief description of the reasons for the determination.	The LPO used two different types of assessment tools to determine if a PIA is required for each engagement. The Privacy Services Engagement Request (**PSER**) along with the Privacy Needs Assessment and Work plan (**PNAW**) was used until August 2014. In August 2014, PSER was replaced by the Legal & Privacy Engagement Request (**LPER**) Form. LPER completed in the initiating phase of a project, to determine whether a PIA or Addendum to a PIA is required for a project based on the collection, use or disclosure of PI/PHI which is in scope for that project. • Nov 1, 2013 – Dec 31, 2013 - there was 7 determinations made that a PIA is not required. • Jan 1, 2014 – Dec 31, 2014 - there was 40 determinations made that a PIA is not required. • Jan 1, 2015 – Dec 31, 2015 - there was 35 determinations made that a PIA is not required • Jan 1, 2016 – October 31, 2016 - there was 18 determinations made that a PIA is not required Please refer to *Appendix "F": Indicators – Summary from the Log of LPERs/PSERs*, for the data holding, information system/technology/program at issue, and a brief description of the reasons for the determination.
5	The number, list and a brief description of PIAs reviewed, since	9 PIAs for programs operating under the PHIPA authority of a PE have been reviewed since the IPC's last review of CCO in October 2014:

	the prior review of the IPC.	• Stem Cell Transplant (**SCT**) Program PIA Addendum no. 1–- November 2013 – Reviews a new method of data collection and an amended list of data elements collected for the SCT program. • DAP-EPS Phase II PIA Addendum no. 2 – November 2013 – Reviews new functionalities of the DAP-EPS including a messaging system, calendar tool, discussion board and blog feature. • Pediatric Positron Emission Tomography (**PET**) Registry PIA Addendum no. 1 – November 2013 – Reviews CCO's collection of PET PHI from PET centres and referring physicians, as well as the transfer of PHI to the Pediatric Oncology Group of Ontario (POGO). • Magnetic Resonance Imaging (**MRI**) Process Improvement Project (PIP) Phase III PIA Addendum no. 1 – January 2014 – Reviews CCO's collection of medical record number and general anesthetic case information from participating hospitals. • ORN Acquisition of Ontario Laboratories Information System (**OLIS**) Data Phase I PIA Addendum no. 2 – May 2014 – To review eHealth Ontario's provision of OLIS data to CCO for use by the ORN to assess the quality and usability of such data for the ORN's purposes. • Ontario Renal Reporting System (**ORRS**) (partial) Release 4.0 PIA Addendum no. 2 – September 2014 – Reviews privacy risks related to one component of ORRS Release 4.0 – the creation and distribution of a new "Bundle Report". • WTIS Release 17 and 18 PIA Addendum no. 1 – October 2014 – Reviews the collection, use and disclosure of PHI in release 17 and 18 of CCO's Wait Times Information System (WTIS), which automates the collection of diagnostic imaging (DI) and scanner data, and offers near-real time reporting of all DO procedures. • Interactive Symptom Assessment and Collection (**ISAAC**) Admission Discharge and Transfer (**ADT**) Integration PIA Addendum no. 2 – November 2014 – Reviews the extension of the HL7 integration to include unidirectional data transfer of patient admission discharge transfer information to ISAAC.

		• ORN Community Care Access Centre (**CCAC**) Long-Term Care (**LTC**) Funding Model PIA Addendum no. 2 – November 2014 – Reviews the role of CCO in the development of the Community Care Access Centre/Long Term Care Funding Model. Three PIAs for programs operating under the PHIPA authority of a PP have been reviewed since the IPC's last review of CCO in October 2014: • OCSP Correspondence Phase II PIA Addendum no. 1- March 2014 – Reviews the privacy risks associated with sending the following types of cervical cancer screening correspondence – invitations, invitations-reminders, recalls and recall-reminders, and follow-up reminders. • eReports (Secure Messaging Solution) Primary Care Screening Activity Report (**PC SAR**) Release 1 PIA Addendum no. 1- March 2014 – Reviews the expansion of the ColonCancerCheck Screening Activity Report (SAR) to include data from CCO's Ontario Cervical Screening Program (OCSP) and Ontario Breast Screening Program (OBSP). • OBSP Correspondence Phase II PIA Addendum no. 1- January 2015 – Reviews privacy risks associated with sending the following types of breast screening correspondence – invitation-reminders, recalls, recall-reminders and normal results.

Privacy Audit Program

IPC Key Indicator Required		**CCO's Response**
1	The dates of audits of agents granted approval to access and use PHI since the prior review of the IPC, and for	Per CCO's Privacy Audit and Compliance Policy, the following audits of users granted approval, through CCO's IDAR system, to access and use PHI, were conducted since the IPC's last review of CCO in November 2014:

	each audit conducted: • A brief description of each recommendation made, • The date each recommendation was addressed or is proposed to be addressed, and • The manner in which each recommendation was addressed or is proposed to be addressed.	• January 2014 – Audit of all data holdings in IDAR system • December 2015 – Audit of all data holdings in IDAR system • May, July and October 2016 – Audit of all data holdings in IDAR system Please refer to *Appendix "G": Indicators – Audit Report & Recommendations.*
2	The number and a list of all other privacy audits completed, since the prior review of the IPC, and for each audit: • A description of the nature and type of audit conducted, • The date of completion of the audit, • A brief description of each recommendation made, • The date each recommendation was addressed or is proposed to be addressed, and	Per CCO's *Audit and Compliance Procedure*, the following types of privacy audits were completed since the IPC's last review of CCO in November 2011: • An audit was done at the request of a contractual counterparty. Due to the confidential nature of some of the information provided in response to this indicator, CCO has excluded some of the details from the public version of this report, however this information has been provided to the IPC. • August 2016 – CCO conducted an audit of privacy policies and procedures. The following policy and procedures were audited: o *CCO Privacy Policy* o *Retention of Records Containing Personal Health Information* o *Privacy Impact Assessment Standard* o *Privacy and Information Security Risk Management Procedure* o *Data Sharing Agreement Initiation procedure* o *Internal Data Access Request Procedure*

	• The manner in which each recommendation was addressed or is proposed to be addressed.	

Privacy Breaches

IPC Key Indicator Required		CCO's Response
1	The number of notifications of privacy breaches or suspected privacy breaches received, since the prior review of the IPC.	For the PE programs there was a total of 236 privacy incidents from November 1, 2013 – October 31, 2016: · In 2013, 9 confirmed PE breaches occurred · In 2014, 24 confirmed PE breaches occurred. · In 2015, 111 confirmed PE breaches occurred. · In 2016, 91 confirmed PE breaches and 1 suspected PE breach occurred For the PP programs there was a total of 1323 privacy incidents from November 1, 2013 – October 31, including both Cancer Screening Program Contact Centre (CC) and non-CC related incidents: · In 2013, 77 confirmed PP breach occurred. · In 2014, 540 confirmed PP breaches occurred. · In 2015, 415 confirmed PP breaches occurred. · In 2016, 290 confirmed PP breaches occurred. In addition, 1 confirmed PP breach was missing year information (based on date the breach was identified or suspected). Note: The above counts of "privacy breaches" also include policy breaches.
2	With respect to each privacy breach or suspected privacy breach:	CCO's Remediation Program maintains a comprehensive log of all reported privacy breaches and incidents. The root cause of privacy breaches is noted as follows: 2013: PE – 0 policy breaches, 9 privacy breaches

	• The date that the notification was received, • The extent of the privacy breach or suspected privacy breach, • Whether it was internal or external, • The nature and extent of PHI at issue, • The date that senior management was notified, • The containment measures implemented, • The date(s) that the containment measures were implemented, • The date(s) that notification was provided to the HICs or any other organizations, • The date that the investigation was commenced, • The date that the investigation was completed, • A brief description of each recommendation made, • The date each recommendation	PP – 3 policy breaches, 74 privacy breach 2014: PE – 16 policy breaches, 8 privacy breaches PP – 17 policy breaches, 523 privacy breaches 2015: PE – 73 policy breaches, 37 privacy breaches; there was also 1 incident where it was unclear whether it was a policy breach or privacy breach PP – 18 policy breaches, 397 privacy breaches 2016: PE – 48 policy breaches, 42 privacy breaches; there was also 1 incident where it was unclear whether it was a policy breach or privacy breach, and 1 suspected breach. PP – 49 policy breaches, 241 privacy breaches Note: · 1 confirmed PP breach was missing year information and were not counted above. (This was a privacy breach.) Please refer to *Appendix "H": Indicators – Summary from the Log of Privacy Breaches* for a list of privacy breaches.

	was addressed or is proposed to be addressed, and • The manner in which each recommendation was addressed or is proposed to be addressed.	

Privacy Complaints

IPC Key Indicator Required		CCO's Response
1	The number of privacy complaints received, since the prior review of the IPC.	No privacy complaints received for the PE. 379 complaints received for the PP. CCO's CSPs, operating under a PP authority, involve direct contact with the public through several different types of correspondence. This correspondence includes invitation letters, result letters and reminder letters to remind participants to get screened. The public facing nature of these programs and direct contact with the public tend to promote more awareness among members of the public of CCO's collection of PI and PHI. In contrast, CCO's PE programs are not public facing and do not involve direct contact with the public using PI and PHI.
2	Of the privacy complaints received, the number of privacy complaints investigated, since the prior review of the IPC, and with respect to each privacy complaint investigated: • The date that the privacy	Of the 379 complaints received for the PP, all have been investigated and closed as per CCO's *Privacy Inquiries and Complaints Procedure*. As part of an ongoing effort to address complaints and inquiries, the LPO develops FAQs that respond to common questions and complaints. Most complaints that are received by telephone are resolved using FAQs. All relevant details of each resolution are logged. Complaints that cannot be addressed using FAQs are investigated further by the Privacy Specialist assigned to the CSPs in accordance with CCO's *Privacy Inquiries and Complaints Procedure.* Please see *Appendix "K": Log of Privacy Complaints*.

	complaint was received, • The nature of the privacy complaint, • The date that the investigation was commenced, • The date of the letter to the individual who made the privacy complaint in relation to the commencement of the investigation, • The date that the investigation was completed, • A brief description of each recommendation made, • The date each recommendation was addressed or is proposed to be addressed, • The manner in which each recommendation was addressed or is proposed to be addressed, and • The date of the letter to the individual who made the privacy complaint	

	describing the nature and findings of the investigation and the measures taken in response to the complaint.	
3	Of the privacy complaints received, the number of privacy complaints not investigated, since the prior review of the IPC, and with respect to each privacy complaint not investigated: • The date that the privacy complaint was received, • The nature of the privacy complaint, and • The date of the letter to the individual who made the privacy complaint and a brief description of the content of the letter.	All privacy complaints are investigated.

Part 2 – Security Indicators

(All indicators are for the period of November 1, 2013 to October 31, 2016)

General Security Policies and Procedures

IPC Key Indicator Required		CCO's Response
1	The dates that the security policies and procedures were reviewed by the PP or PE since the prior review of the IPC.	CCO reviewed and revised a number of security policies and procedures in 2013, 2014, 2015 and 2016. A list of policy/procedures reviewed and changes made to them are noted in *Appendix "C"* of the report.
2	Whether amendments were made to existing security policies and procedures as a result of the review and, if so, a list of the amended security policies and procedures and, for each policy and procedure amended, a brief description of the amendments made.	The following policy/procedures were amended as result of the review: The 2013 review of CCO's security policy suite resulted in amendments to the following documents: • *Digital Personal Health Information Handling Standard* • *Enterprise Information Security Policy* • *Information Security Code of Conduct and Acceptable Use Policy* • *Mobile Device Policy Data Centre Physical Security Standard* All amendments made were to ensure technical currency. For a description of amendments made as a result of the review, please see *Appendix "C"*.
3	Whether new security policies and procedures were developed and implemented as a result of the review, and if so, a brief description of each of the policies and procedures developed and implemented.	There were no new policies and procedures developed as a result of the prior review of the IPC.
4	The dates that each amended	All of the new security policies, standards and/or procedures which were developed and approved have been

	and newly developed security policy and procedure was communicated to agents and, for each amended and newly developed security policy and procedure communicated to agents, the nature of the communication.	communicated through CCO's Intranet. The date of communication for each policy/procedure is noted in *Appendix "C"*.
5	Whether communication materials available to the public and other stakeholders were amended as a result of the review, and if so, a brief description of the amendments.	No externally available communication materials were amended as a result of the IPC's last review of CCO in October 2014.

Physical Security

IPC Key Indicator Required		**CCO's Response**
1	The dates of audits of agents granted approval to access the premises and locations within the premises where records of	CCO practice is to conduct audits when an incident or suspected physical security incident has occurred or is notified by an employee. This type of audit occurs at least once per year. There have been three physical security breaches since the previous IPC review in 2014. Feb 3rd, 2014 – Theft of personal belongings at 620 University

	PHI are retained since the prior review by the IPC and for each audit: A brief description of each recommendation made, – The date each recommendation was addressed or is proposed to be addressed, and – The manner in which each recommendation was addressed or is proposed to be addressed.	Report filed to security. CCTV system reviewed and photo provided to all admins in the building. Communication sent to organization to be vigilant and challenge individuals without photo identification (**ID**). Police report not filed due to negligible loss. <u>July 22, 2015 – Unruly visitor at 505 University</u> Visitor left on their own. CCTV system reviewed and photo provided to security. Police report not deemed necessary. August 22, 2016 – Theft of laptop at 620 University It was suspected that a terminated employee took their laptop with them when leaving the premises. The video system was reviewed to confirm that this was the case. Human Resources retrieved the laptop from the former employee. In addition to the above, Facilities conducts regular spot audits of the video system..Due to the sensitive nature of CCO's security practices, CCO has excluded some of the details of these practices from the public version of this report, however, these have been provided to the IPC

<u>Security Audit Program</u>

IPC Key Indicator Required		**CCO's Response**
1	The dates of the review of system control and audit logs since the prior review by the IPC and a general description of the findings, if any, arising from the review of system control and audit logs.	CCO continually monitors our system control and audit logs using a number of automated systems. These systems monitor for errors in applications, availability of system components, and security events. These logs are reviewed both through automated means, as well as by CCO operations staff. For example: • Security events at both an infrastructure level and application level are logged to CCO's Logging, Monitoring, and Auditing System (**LMAS**). This system uses a collection of rules to generate alerts based on

		certain detected patterns. An example of this would be excessive file system activity on our PHI file shares. • Operational events from our Windows servers are centrally logged and monitored through the Microsoft System Centre Suite. This monitoring detects failed applications and other error states, allowing operations staff to ensure normal operation of systems • Network devices use Syslog and Simple Network Management Protocol (**SNMP**) to generate logging and event data for both real time and ad-hoc analysis. These typically discover excessive network patterns or configuration errors, allowing for operational staff to investigate. Events that require action trigger some combination of CCO's ITIL-based incident process, security response process, and privacy breach process. Examples of typical responses include: • Reviewing and analyzing unusual log entries that are indicative of a misconfiguration or software flaw. These are then escalated to a product team to isolate the cause. In some cases, vendors are notified and a software patch is applied. • Excessive security events trigger follow up from CCO's EISO. For example, failed login attempts are analyzed to determine whether a system is being attacked or whether a user simply forgot their password. • Alerts from operational systems result in more immediate responses from both operational teams and the EISO when the source of the alert is deemed to be security related. For example, a server that goes offline is investigated immediately based on alerts triggered within the monitoring systems.
2	The number and a list of security audits completed since the prior review by the IPC	**46** security audits have been completed since the IPC's last review of CCO in November 2014, as noted in CCO's log of security assessments. CCO's security audits include:

	and for each audit: – A description of the nature and type of audit conducted, – The date of completion of the audit, – A brief description of each recommendation made, – The date that each recommendation was addressed or is proposed to be addressed, and – The manner in which each recommendation was addressed or is expected to be addressed.	• TRAs; and • Vulnerability and other assessments. Please refer to *Appendix "I": Indicators – Summary from the Log of Security Audits*, for a list of security audits completed since the IPC's last review of CCO.

Information Security Breaches

IPC Key Indicator Required		CCO's Response
1	The number of notifications of information security breaches or suspected information security breaches received by the PP or PE since the prior review by the IPC.	CCO does not distinguish between Prescribed Entity and Prescribed Person incidents hence the number below includes incidents and breaches for both Prescribed Entity and Prescribed Person: • Jan – Dec 2014: 7 Incidents, 1 of which was determined to be a breach • Jan – Dec 2015: 22 Incidents. • Jan – Oct 2016: 34 Incidents, 1 of which was determined to be a breach **Note:** CCO's EISO definitions of information security incident and security breach as follows: **Information Security Incident:** An information security incident is a security event that may compromise business operations or threaten CCO security. Incidents require action on the part of CCO resources to contain and prevent further harm to CCO infrastructure and/or information assets. A *Near Miss* is an incident that did not result in a breach – but had the potential to do so. **Information Security Breach:** A security breach occurs when there is a loss of confidentiality, integrity, or availability of sensitive information and information assets, resulting from a breach of CCO's security safeguards or from failure to establish reasonable safeguards. Security breaches include contravention of policies, procedures, or practices that result in material security risk to CCO.
2	With respect to each information security breach or suspected information security breach:	Descriptions of all suspected information security breaches are captured in Appendix I: Summary from the Log of Security Audits & Information Security Breaches.

	– A description of the nature and type of audit conducted, – The date that the notification was received, – The extent of the information security breach or suspected information security breach, – The nature and extent of PHI at issue, – The date that senior management was notified, – The containment measures implemented, – The date(s) that the containment measures were implemented, – The date(s) that notification was provided to the HICs or any other organizations, – The date that the investigation was commenced, – The date that the investigation was completed, – A brief description of each recommendation made,	

	– The date each recommendation was addressed or is proposed to be addressed, and – The manner in which each recommendation was addressed or is proposed to be addressed.	

Part 3 – Human Resources Indicators

(All indicators are for the period of November 1, 2013 to October 31, 2016)

Privacy Training and Awareness

IPC Key Indicator Required		CCO's Response
1	The number of agents who have received and who have not received initial privacy orientation, since the prior review of the IPC.	As of October 31, 2016 all CCO employees (includes PE and PP) have received initial privacy orientation since October 2013. • **Nov 1, 2013 – Dec 31st, 2013:** 28 employees received initial privacy orientation at the start of their employment • **Jan 1st 2014 – Dec 31st 2014:** 378 employees received initial privacy orientation at the start of their employment • **Jan 1st 2015 – Dec 31st 2015:** 69 employees received initial privacy orientation at the start of their employment • **Jan 1st 2016 – October 31, 2016:** 255 employees received initial privacy orientation at the start of their employment The completion of initial privacy orientation is mandatory for all employees within 30 days of their start date, per the

		Privacy and Security Training and Awareness Procedure and as a condition of employment with CCO
2	The date of commencement of the employment, contractual or other relationship for agents that have yet to receive initial privacy orientation and the scheduled date of the initial privacy orientation.	The completion of initial privacy orientation is mandatory for all employees within 30 days of their start date, per the Privacy and Security, Training and Awareness Procedure and as a condition of employment with CCO. There are not any employees who did not receive initial privacy and security training. CCO system access for employees who do not complete their initial privacy orientation within 30 days of their start date will be disabled.
3	Record of agents who have attended and who have not attended ongoing privacy training each year, since the prior review of the IPC.	As of October 31, 2016, the number of CCO employees who completed ongoing privacy training each year since the IPC's last review of CCO in October 2014 are as follows: **2013**: 956 completed the Annual Privacy Refresher Training **2014**: 1111 completed the Annual Privacy Refresher Training **2015**: 1071 completed Annual Privacy Refresher Training **2016:** The Annual Privacy Refresher is scheduled for December 2016 Per the Privacy and Security Training and Awareness Procedure, all CCO employees are required to complete privacy training on an annual basis. Since the implementation of CCO's eLearning tool in 2009, there have been 10 or fewer employees each year who have not completed the Annual Privacy Refresher Training curriculum, for reasons such as long-term leave. The exact numbers are as follows: 2013: 4 2014: 10 2015: 3 Note: CCO electronically tracks completion of the Annual Privacy Refresher Training curriculum through its eLearning tool. This record is contained in CCO's Log of Refresher Privacy and Security Training Completion.
4	Record of dates and number of communications	There have been a number of communications to CCO employees since October 2013. These are as follows:

	to agents by CCO in relation to privacy and a brief description of each communication, since the prior review of the IPC.	• December 2014 – Info Fair • Spring 2015 – Privacy Awareness Training to Directors • Spring 2015 – LPO Open House Winter – Summer 2016 – Privacy Awareness training for the following business units: • CC • Aboriginal Cancer Control Unit (**ACCU**) • Regional Programs • A&I • CQCO • CRO • Legal Team Fall 2015 and Summer 2016 – Privacy Awareness Training for the PFAC Program March 2016 – Cloud and privacy implication presentation to the Chief Technology Office (**CTO**) Town Hall March 2016 – Lunch and Learn on Cloud and privacy implications

Security Training and Awareness

IPC Key Indicator Required		**CCO's Response**
1	The number of agents who have received and who have not received initial security orientation, since the prior review of the IPC.	As of October 31, 2016 all CCO employees (includes PE and PP) have received initial security orientation since October 2013. • **Nov 1, 2013 – Dec 31st, 2013:** 28 employees received initial security orientation at the start of their employment • **Jan 1st 2014 – Dec 31st 2014:** 378 employees received initial security orientation at the start of their employment • **Jan 1st 2015 – Dec 31st 2015:** 69 employees received initial security orientation at the start of their employment • **Jan 1st 2016 – October 31, 2016:** 255 employees received initial security orientation at the start of their employment

		The completion of initial security orientation is mandatory for all employees within 30 days of their start date, per the Privacy and Security Training and Awareness Procedure and as a condition of employment with CCO
2	The date of commencement of the employment, contractual or other relationship for agents that have yet to receive initial security orientation and the scheduled date of the initial security orientation.	The completion of initial privacy and security orientation is mandatory for all employees within 30 days of their start date, per the *Privacy and Security, Training and Awareness Procedure* and as a condition of employment with CCO. There are not any employees who did not receive initial privacy and security training. CCO system access for employees who do not complete their initial security orientation within 30 days of their start date will be disabled.
3	Record of agents who have attended and who have not attended ongoing security training each year, since the prior review of the IPC.	As of October 31, 2016, the number of CCO employees who completed ongoing security training each year since the IPC's last review of CCO in October 2014 are as follows: **2013**: 956 completed the Annual Security Refresher Training **2014**: 1111 completed the Annual Security Refresher Training **2015**: 1071 completed Annual Security Refresher Training **2016:** The Annual Security Refresher is scheduled for December 2016 Per the Privacy and Security Training and Awareness Procedure, all CCO employees are required to complete security training on an annual basis. Since the implementation of CCO's eLearning tool in 2009, there have been 10 or fewer employees each year who have not completed the Annual Privacy Refresher Training curriculum, for reasons such as long-term leave. The exact numbers are as follows: 2013: 4 2014: 10 2015: 3

		Note: CCO electronically tracks completion of the Annual Security Refresher Training curriculum through its eLearning tool. This record is contained in CCO's Log of Refresher Privacy and Security Training Completion.
4	Record of dates and number of communications to agents by CCO in relation to information security and a brief description of each communication, since the prior review of the IPC.	There have been a number of security communications to CCO employees since November 2011. These are as follows: **2014:** • Monthly Security Bulletins (once a month) • Privacy and Security Annual Refresher Training 2014 (Nov- Dec, 2014) **2015:** • Privacy and Security Annual Refresher Training 2015. (Nov – Dec, 2015) **2016:** • Anti-Phishing Awareness Program (Sept 2016 – ongoing)

Confidentiality Agreements

IPC Key Indicator Required		**CCO's Response**
1	The number of agents who have executed Confidentiality Agreements each year since the prior review by the IPC.	For the period between November 1st, 2013 and October 31st, 2016, the number of Confidentiality Agreements executed are as follows: • Nov 1, 2013 to Dec 31 2013 - 23 Confidentiality Agreements executed • Jan 1, 2014 to Dec 31, 2014 - 201 Confidentiality Agreements executed • Jan 1, 2015 to Dec 31, 2015 - 211 Confidentiality Agreements executed • Jan 1, 2016 to Oct 31, 2016 - 249 Confidentiality Agreements executed

2	The date of commencement of the employment, contractual or other relationship for agents that have yet to executed the Confidentiality agreements and the date by which the Confidentiality Agreement must be executed.	All CCO employees and contractors are required to sign a Confidentiality Agreement with CCO. There are zero agents who have not executed confidentiality agreements each year since the prior review. An employee will not be set up in the HCMS System until all of the mandatory paperwork has been received, which includes the confidentiality agreements. All agreements with third party service providers contain confidentiality terms.

Termination or Cessation

IPC Key Indicator Required		CCO's Response
1	The number of notifications received from agents since the prior review by the IPC related to termination of their employment, contractual or other relationship with the PP or PE.	From November 1st, 2013 to October 31 2016, there have been **743** terminations and cessations. The number of Terminations/Cessations (by year) are as follows: By Year: • **Nov 1, 2013 to Dec 31 2013:** 14 • **Jan 1, 2014 to Dec 31, 2014:** 236 • **Jan 1, 2015 to Oct 31, 2015:** 280 • **Jan 1, 2016 to Oct 31, 2016:** 213

Part 4 – Organizational Indicators

(All indicators are for the period of November 1, 2013 to October 31, 2016)

Risk Management

IPC Key Indicator Required		CCO's Response
1	The dates that the corporate risk register was reviewed by the PP or PE.	The corporate risk register was reviewed by the Board in April 2015, September 2015, February 2016, and September 2016. Reviews did not occur in 2014 due to revisions occurring in relation to MOHLTC reporting requirements. The Privacy Risk Register and Security Risk Register are reviewed on an ongoing basis by the Privacy and Information Security teams at CCO.
2	Whether amendments were made to the corporate risk register as a result of the review, and if so, a brief description of the amendments made.	There were no amendments made to the corporate risk register as a result of the review. Amendments are made to the Privacy Risk Register and the Security Risk Register on an ongoing basis to add new risks identified, identify mitigating strategies, and update these items on an ongoing basis

Business Continuity and Disaster Recovery

IPC Key Indicator Required		CCO's Response
1	The dates that the business continuity and disaster recovery plan was tested since the prior review by the IPC.	Note: **SQL DB** = Structured Query Language Data Base From November 1, 2013 to June 30, 2016, the following tests were performed: SQL DB Recovery 9/21/2016 15:00 Top of Form Oracle DB Recovery Bottom of Form 9/21/2016 14:00 Hyper-V Server Recovery 9/21/2016 10:20 File Level Recovery 9/13/2016 12:35 File Level Recovery 4/29/2016 13:30

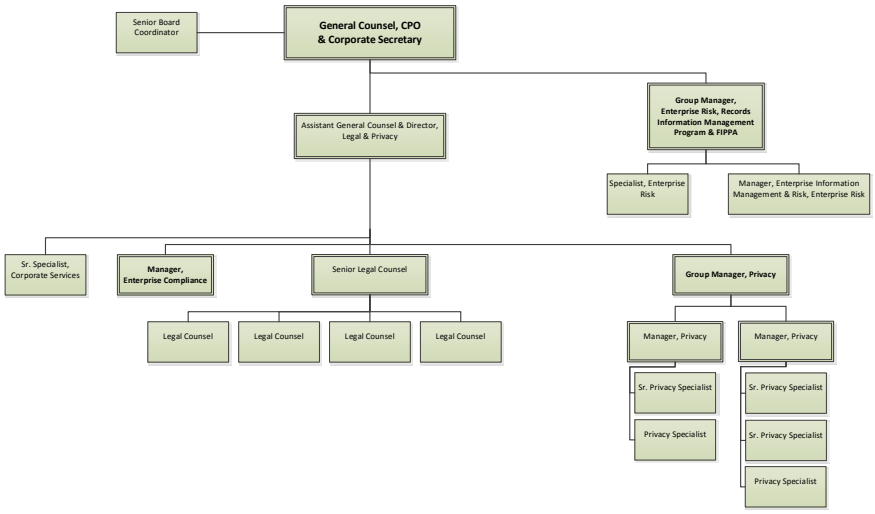
		Hyper-V Server Recovery	4/29/2016 11:30
		Oracle DB Recovery	2/24/2016 14:10
		File Level Recovery	2/24/2016 11:20
		Hyper-V Server Recovery	2/23/2016 10:15
		SQL DB Recovery	1/27/2016 11:35
		Hyper-V Server Recovery	1/27/2016 10:40
		Hyper-V Server Recovery	1/27/2016 10:40
		File Level Recovery	1/19/2016 13:40
		Oracle DB Recovery	12/31/2015 12:10
		File Level Recovery	12/31/2015 11:20
		Hyper-V Server Recovery	12/31/2015 9:30
		SQL DB Recovery	9/23/2015 16:20
		File Level Recovery	9/23/2015 16:15
		VMWare Server Recovery	9/23/2015 15:55
		Hyper-V Server Recovery	9/23/2015 15:45
		Hyper-V Server Recovery	8/12/2015 15:55
		Oracle DB Recovery	8/11/2015 10:45
		File Level Recovery	8/11/2015 10:30
		SQL DB Recovery	7/17/2015 11:40
		File Level Recovery	7/17/2015 11:30
		Hyper-V Server Recovery	7/17/2015 11:20
		VMWare Server Recovery	7/17/2015 11:15
		File Level Recovery	6/10/2015 10:30
		Oracle DB Recovery	6/10/2015 10:30
		Hyper-V Server Recovery	6/10/2015 10:25
		Hyper-V Server Recovery	5/11/2015 12:35
		File Level Recovery	5/11/2015 12:25
		SQL DB Recovery	5/11/2015 11:55
		Hyper-V Server Recovery	4/14/2015 13:00
		Oracle DB Recovery	4/14/2015 12:45
		File Level Recovery	4/14/2015 11:20
		SQL DB Recovery	3/11/2015 16:15
		VMWare Server Recovery	3/11/2015 16:10
		File Level Recovery	3/11/2015 15:20
		Hyper-V Server Recovery	3/11/2015 15:10
		Hyper-V Server Recovery	2/12/2015 14:45
		Oracle DB Recovery	2/12/2015 14:45
		File Level Recovery	2/12/2015 12:55
		Hyper-V Server Recovery	1/13/2015 11:55
		VMWare Server Recovery	1/13/2015 11:50
		SQL DB Recovery	1/13/2015 11:45
		File Level Recovery	1/13/2015 11:40
		File Level Recovery	1/9/2015 10:35
		Hyper-V Server Recovery	12/10/2014 15:35
		Oracle DB Recovery	12/10/2014 15:30
		File Level Recovery	12/10/2014 15:15

		SQL DB Recovery	11/12/2014 14:05
		VMWare Server Recovery	11/12/2014 13:45
		File Level Recovery	11/12/2014 13:30
		Hyper-V Server Recovery	11/12/2014 12:55
		Hyper-V Server Recovery	10/20/2014 17:05
		Oracle DB Recovery	10/20/2014 17:05
		File Level Recovery	10/20/2014 17:00
		SQL DB Recovery	9/16/2014 12:45
		VMWare Server Recovery	9/16/2014 12:30
		Hyper-V Server Recovery	9/16/2014 12:00
		File Level Recovery	9/16/2014 11:50
		Oracle DB Recovery	8/21/2014 8:30
		Hyper-V Server Recovery	8/21/2014 8:20
		File Level Recovery	8/21/2014 8:20
		File Level Recovery	7/15/2014 11:20
		SQL DB Recovery	7/14/2014 10:40
		File Level Recovery	7/14/2014 10:30
		Hyper-V Server Recovery	7/14/2014 10:10
		Oracle DB Recovery	6/11/2014 16:05
		Hyper-V Server Recovery	6/11/2014 15:40
		File Level Recovery	6/11/2014 15:35
		Hyper-V Server Recovery	5/20/2014 12:45
		SQL DB Recovery	5/15/2014 16:35
		File Level Recovery	5/15/2014 16:25
		Oracle DB Recovery	4/17/2014 14:05
		File Level Recovery	4/17/2014 11:30
		Hyper-V Server Recovery	4/17/2014 11:30
		VMWare Server Recovery	3/12/2014 12:55
		SQL DB Recovery	3/12/2014 12:45
		Hyper-V Server Recovery	3/12/2014 12:35
		File Level Recovery	3/12/2014 12:30
		File Level Recovery	2/4/2014 16:20
		Oracle DB Recovery	2/4/2014 15:40
		Hyper-V Server Recovery	2/4/2014 15:25
		Restore managed file transfer (**MFT**) tumbleweed service	1/24/2014 11:00
		620 University Ave power failover system	1/20/2014 10:00
		VMWare Server Recovery	1/8/2014 14:20
		Hyper-V Server Recovery	1/8/2014 14:00
		SQL DB Recovery	1/8/2014 13:50
		File Level Recovery	1/8/2014 13:45
		Hyper-V Server Recovery	12/10/2013 11:25
		Oracle DB Recovery	12/10/2013 11:20
		File Level Recovery	12/10/2013 11:10
		VMWare Server Recovery	11/6/2013 11:50

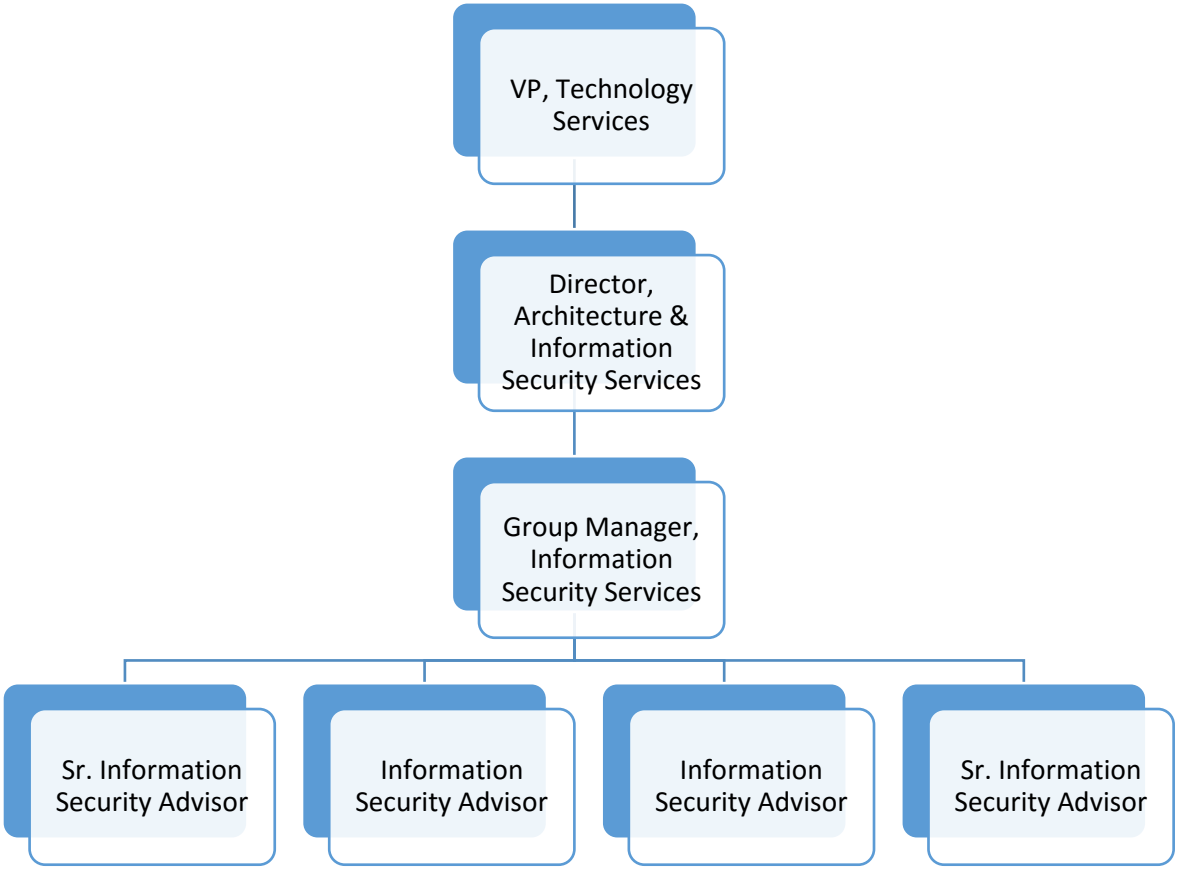
		SQL DB Recovery File Level Recovery Hyper-V Server Recovery	11/6/2013 11:30 11/6/2013 11:15 11/6/2013 11:15
2	Whether amendments were made to the business continuity and disaster recovery plan as a result of the testing, and if so, a brief description of the amendments made.	No changes or amendments were made as a result of testing.	

Appendix A: Current Organizational Structure for the Legal and Privacy Office

Legal & Privacy Office
Organizational Chart



Appendix B: Current Organizational Structure for the Enterprise Information Security Office



Appendix C.1: Privacy – Log of Policy Reviews, Revisions & New Documents

Policy Document	Date of Review (IND-A-01)	Amendments Made? (Y/N) or New (IND-A-02), or other	Brief Description of Amendment or New Policy Document (IND-A-02)	Date Policy Document was Communicated to Agents, and Nature of Communications (IND-A-04)
* Please note that all Privacy-owned policy documents were reviewed and updated in August 2015	Aug-2015	Y	Aligned with new policy document templates and branding as part of CCO's new enterprise policy framework, including standard headings and standard definitions, and to reflect the Privacy & Access Office's name change to the Legal and Privacy Office.	The changes were not communicated as substantive policy changes were not implemented
Application for Disclosure of Information for Research Purposes	February 2014 & November 2014	Y	February 2014 – Minor formatting amendments only. November 2014 – Additional formatting and wording amendments for greater clarity.	Communicated by Data Access Team to all individuals making data requests via email beginning in February 2014.
Data Access Committee Terms of Reference & Decision Criteria for Data Requests	Jul-14	Y	Updated terms of reference to reflect current state and combined with Decision Criteria for Data Requests as an appendix.	Posted on CCO's intranet, eCCO in August 2014.
Data Linkage Policy	Apr-14	Y	Minor amendments to clarify scope of policy and add references to other relevant policy documents.	Posted on CCO's intranet, eCCO in August 2014.
Data Linkage Policy	Aug-16	Y	A number of changes were made to this policy to reflect the new definition of linkages, and to align with the IPC triennial review requirements.	To be posted following approval.
Data Sharing Agreement Initiation Procedure	Jun-14	Y	Minor amendments to clarify approval process and reference another relevant policy document.	Posted on CCO's intranet, eCCO in August 2014.
Data Sharing Agreement Initiation Procedure	Aug-16	Y	Incorporated new process as recommended by Data Acquisitions for DSA.	To be posted following approval.
Data Sharing Agreement Standard	Jun-14	Y	Added reference to other relevant policy documents.	Posted on CCO's intranet, eCCO in August 2014.

Policy Document	Date of Review (IND-A-01)	Amendments Made? (Y/N) or New (IND-A-02), or other	Brief Description of Amendment or New Policy Document (IND-A-02)	Date Policy Document was Communicated to Agents, and Nature of Communications (IND-A-04)
Data Use & Disclosure Standard	Jun-14	Y	Minor amendments to clarify ownership of document, updates titles and clarify third party requirements.	Posted on CCO's intranet, eCCO in August 2014.
Decision Criteria for Data Requests	May-14	Y	Formatting amendment only.	Posted on CCO's intranet, eCCO in August 2014.
Enterprise Risk Management Framework	Aug-14	Y	Minor revisions as requested by IPC in June 2014 Policy Audit.	Posted on CCO's intranet, eCCO in August 2014.
Internal Data Access Request Procedure	Aug-16	N	N/A	N/A
Internal Data Sharing Procedure	Aug-16	New	This is a new policy drafted to facilitate internal data sharing of data.	To be posted following approval.
Policy on Retention of Records Containing Personal Health Information	Feb-14	N	N/A	N/A
Principles and Policies for the Protection of Personal Health Information at CCO ("CCO's Privacy Policy")	Jun-14	Y	Clarified wording in data retention section and updated appendices to reflect current state.	Posted on CCO's intranet, eCCO in August 2014.
Principles and Policies for the Protection of Personal Health Information at CCO ("CCO's Privacy Policy")	Aug-16	Y	Significant changes were made to the order and layout of the policy content as well as minor changes to the wording for clarity and readability. These changes were not intended to reflect a change in CCO's privacy program or privacy practices. Significant changes were also made to incorporate the HINP Privacy Policy contents into CCO's Privacy Policy as some of the content is similar between the two policies (for example, general safeguards used to protect PHI from unauthorized access). Where there is unique policy content relating to CCO's HINP role, the content is now included in CCO's Privacy Policy (for example, under section. 5 'collection, use and disclosure of	To be posted following approval.

Policy Document	Date of Review (IND-A-01)	Amendments Made? (Y/N) or New (IND-A-02), or other	Brief Description of Amendment or New Policy Document (IND-A-02)	Date Policy Document was Communicated to Agents, and Nature of Communications (IND-A-04)
			PHI – Use', the following purpose is included - for the purposes of providing IT services to enable HICs to use electronic means to disclose PHI to one another). These changes are not intended to reflect a change in CCO's privacy program. Changes were also made to reflect the change in process whereby CCO is now processing requests for an individual's PHI through CCO's FOI program. Updates were made to the policy, for example, to reflect new or updated referenced documents (i.e. the FIPPA Privacy Policy).	
Privacy & Security Acknowledgment Form	Nov-14	Y	Minor updates to reflect current status for use in 2014 Privacy & Security Refresher Training.	Was required to be accepted online by all staff following completion of 2014 Privacy & Security Refresher Training.
Privacy and Information Security Risk Management Procedure	Aug-16	Y	Amendments were made to the Privacy and Information Risk Management Procedure to reflect updates in the risk rating criteria and to add a risk acceptance process.	To be posted following approval.
Privacy and Security Training and Awareness Procedure	Apr-14	Y	Minor amendment to language in purpose section for greater clarity.	Posted on CCO's intranet, eCCO in August 2014.
Privacy Audit & Compliance Standard	Apr-14	Y	Minor amendment to language in purpose and definitions sections for greater clarity.	Posted on CCO's intranet, eCCO in August 2014.
Privacy Audit and Compliance Policy	Sep-15	Y	Name changed to Privacy Audit and Compliance Policy to better reflect document purpose and align with enterprise policy framework definitions. Content updated to delete redundancies and better reflect practices.	Communicated internally to privacy team operationalizing policy in September 2015.

Policy Document	Date of Review (IND-A-01)	Amendments Made? (Y/N) or New (IND-A-02), or other	Brief Description of Amendment or New Policy Document (IND-A-02)	Date Policy Document was Communicated to Agents, and Nature of Communications (IND-A-04)
Privacy Breach Management Policy	Aug-16	Y	Reclassified from a Procedure to a Policy. Minor wording and formatting changes made to align with the new Privacy Breach Management Manual developed to support the policy.	To be posted following approval.
Privacy Breach Management Procedure	April 2014 & August 2014	Y	April 2014 – Formatting amendment only. August 2014 – Minor revisions as requested by IPC in June 2014 Policy Audit.	Posted on CCO's intranet, eCCO in August 2014.
Privacy Frequently Asked Questions	Mar-14	Y	Minor updates to reflect current state including the programs CCO operates, type of data collected and that the OBSP now operates under CCO's prescribed person authority.	Posted on CCO's external website in March 2014.
Privacy Impact Assessment Standard	Apr-14	Y	Formatting amendment only.	Posted on CCO's intranet, eCCO in August 2014.
Privacy Impact Assessment Standard	Aug-16	Y	Updating content as per new PIA Framework. Adding definitions for consistency with other privacy policies.	To be posted following approval.
Privacy Inquiries and Complaints Procedure	Apr-14	Y	Clarified wording in scope section.	Posted on CCO's intranet, eCCO in August 2014.
Privacy Risk Management Policy	Apr-14	Y	Formatting amendment only.	Not communicated – replaced by Privacy & Information Security Risk Management Framework (Schedule to the ERM Framework) in August 2014.
Procurement Policy	Sep-15	Y	Minor amendments to quotation requirements for purchases under $5,000 and policy renamed	Posted on CCO's intranet, eCCO in September 2015.
Research Data Request – Expedited Review Form	Jul-14	New	Created supplementary form to facilitate amendments requested to the Application for Disclosure of Information for Research Purposes.	Communicated by Data Access Team to all individuals making data requests via email beginning in July 2014.

Policy Document	Date of Review (IND-A-01)	Amendments Made? (Y/N) or New (IND-A-02), or other	Brief Description of Amendment or New Policy Document (IND-A-02)	Date Policy Document was Communicated to Agents, and Nature of Communications (IND-A-04)
Retention of Records Containing Personal Health Information	Aug-16	Y	Updated to reflect CCO's new records management policy and schedules.	To be posted following approval.
Schedule to the Enterprise Risk Management Framework – Privacy & Information Security Risk Management Framework	Aug-14	Y	Major revisions to combine the Privacy Risk Management Policy and Framework and the Information Security Risk Management documentation into one document, as requested by IPC in June 2014 Policy Audit.	Posted on CCO's intranet, eCCO in August 2014.
Statement of Information Practices	Mar-14	Y	Minor updates to reflect current state including the programs CCO operates,	Posted on CCO's external website in March 2014.

Appendix C.2: Security – Log of Policy Reviews, Revisions and New Documents

Policy Document	Date of Review (IND-A-01)	Amendments Made? (Y/N) or New (IND-A-02), or other	Brief Description of Amendment or New Policy Document (IND-A-02)	Date Policy Document was Communicated to Agents, and Nature of Communications (IND-A-04)
Access Card Procedure	Jul-15	N	N/A	N/A
Access Care Procedure	Aug-16	Y	Minor amendments to update closing of one of CCO physical location.	Posted on CCO's Intranet in October 2016.
Acquisition Development and Application Security Standard	Aug-15	Y	Added involvement of EISO in the procurement process to ensure appropriate security requirements.	Posted on CCO's Intranet eCCO in August 2015.
Change Advisory Board Terms of Reference, Technology Services Renamed: *Information Technology Change Subcommittee (**ITCS**)*	Apr-16	N	Renamed and mandate revised to reflect CCO's updated governance structure.	Posted on CCO's Intranet eCCO in April 2016.

Policy Document	Date of Review (IND-A-01)	Amendments Made? (Y/N) or New (IND-A-02), or other	Brief Description of Amendment or New Policy Document (IND-A-02)	Date Policy Document was Communicated to Agents, and Nature of Communications (IND-A-04)
Change Management Policy	Apr-16	Y	Revision of policy to reflect new requirements and practices, including approval process SLAs and post implementation requirements. Changes include: · Introduction of ITCS (IT Change Sub-Committee) in place of CAB (Change Advisory Board). While essentially they are both change management representatives, the introduction of ITCS better defines owner of IT management process for CCO which is the Technology Services division · ITCS is responsible assessing request and risk associated with request and approving or denying as such based on impact, risk, rollback, testing, etc. · Introduces "CCO Change Management Tool", an online automated system to: o Submit a request o Notify ITCS approving members o Online processing for approval/denial of request o Automated notification to requesting party	Posted on CCO's Intranet eCCO in April 2016.

Policy Document	Date of Review (IND-A-01)	Amendments Made? (Y/N) or New (IND-A-02), or other	Brief Description of Amendment or New Policy Document (IND-A-02)	Date Policy Document was Communicated to Agents, and Nature of Communications (IND-A-04)
			o Follow up on implementation/change results o Track changes and report on them · Introduction of a defined PIR (Post Implementation Review) for all emergency requests and changes: o Completed with issues o Completed outside of approved change window o Failed changes · Better defines concepts of various changes such as: o Standard Change o Normal Change o Emergency Change	
Change Request Control Form, Technology Services	Apr-16	Retired	Result of automated change management process implementation. New requirements and practices reflected in the *Change Management Policy*.	N/A
Data Backup Policy	Feb-14	N	N/A	Posted on CCO's intranet, February 2014.
Data Backup Procedure	Jan-14	N	N/A	N/A

Policy Document	Date of Review (IND-A-01)	Amendments Made? (Y/N) or New (IND-A-02), or other	Brief Description of Amendment or New Policy Document (IND-A-02)	Date Policy Document was Communicated to Agents, and Nature of Communications (IND-A-04)
Data Centre Physical Security Standard	Sep-15	Y	Clarification of standards that must be met.	Posted on CCO's Intranet eCCO in September 2015.
Digital Media Disposal Guideline	August 2015	Superceded	The *Digital Media Disposal Guideline* has been deprecated. Disposal principles and practices have been formalized in the *Digital Media Disposal Standard and Procedure.*	N/A
Digital Media Disposal Procedure	Aug-15	New	This document establishes the procedures for digital media disposal at CCO.	Posted on CCO's Intranet in August 2015.

Policy Document	Date of Review (IND-A-01)	Amendments Made? (Y/N) or New (IND-A-02), or other	Brief Description of Amendment or New Policy Document (IND-A-02)	Date Policy Document was Communicated to Agents, and Nature of Communications (IND-A-04)
Digital Media Disposal Standard	Aug-15	New	The Standard sets CCO's practices for securely disposing of digital storage media and any data contained within. This standard is followed for all data types.	Posted on CCO's Intranet in August 2015.
Digital Personal Health Information Handling Standard	Mar-14	Y	Minor formatting and grammatical changes.	Posted on CCO's intranet, eCCO in August 2014.
Enterprise Information Security Policy	In progress (Jul 15-May 17)	N/A	Full review and revision of the policy is in progress. Under review to ensure policy continues to reflect the goals of information security at CCO in the protection of all CCO information assets, through the management of information and IT security risks.	Posted on CCO's Intranet, eCCO in July 2015.
Hard Copy Personal Health Information Disposal Procedure	Aug-16	Y	Minor amendments were made to this policy including formatting updates to align with new enterprise-wide policy document templates and added a clarification regarding responsibilities for off-site destruction	Posted on CCO's Intranet in October 2016.

Policy Document	Date of Review (IND-A-01)	Amendments Made? (Y/N) or New (IND-A-02), or other	Brief Description of Amendment or New Policy Document (IND-A-02)	Date Policy Document was Communicated to Agents, and Nature of Communications (IND-A-04)
Information Management and Information Technology Gating Policy	Aug-16	Y	Both minor and major amendments were made to this policy. Changes include updated definitions section; updated costing and approval table; updated approver for medium size projects; defined significant cost and schedule variance; user-friendly language added; approval gate changes added; procurement gates were defined; and VP and Business Sponsor attendance requirements were added.	Posted on CCO's Intranet in October 2016.
Information Security Code of Conduct and Acceptable Use Policy	In progress(Oct 16-May 17)	N/A	Review and revision of the policy is in progress.	N/A
Information Security Program Framework	Apr-15	N	N/A	Posted on CCO's Intranet, eCCO in July 2015.
Information Technology Change Management Process Flow	Apr-16	Retired	Result of automated change management process implementation. New requirements and practices reflected in the *Change Management Policy*.	N/A

Policy Document	Date of Review (IND-A-01)	Amendments Made? (Y/N) or New (IND-A-02), or other	Brief Description of Amendment or New Policy Document (IND-A-02)	Date Policy Document was Communicated to Agents, and Nature of Communications (IND-A-04)
Information Technology Change Management Standard: Change Category and Type, Technology Services	Apr-16	Retired	Result of automated change management process implementation. New requirements and practices reflected in the *Change Management Policy*.	N/A
*Information Technology Change Management Standard: Request for Change (**RFC**), Technology Services*	Apr-16	Retired	Result of automated change management process implementation. New requirements and practices reflected in the *Change Management Policy*.	N/A
Information Technology Change Management Standard: Request for Change Lead Time, Technology Services	Apr-16	Retired	Result of automated change management process implementation. New requirements and practices reflected in the *Change Management Policy*.	N/A
Logging, Monitoring and Auditing Standard and Procedure	Aug-15	Y	Updated the standard to include a description of sensitive information, access logging requirements for PHI systems, and other wording updates to tighten control requirements.	Posted on CCO's Intranet eCCO in August 2015.
Logical Access Control Standard	In progress (Oct 16-May 17)	N/A	Review and revision in progress to reflect updated user access control and password strength requirements.	N/A

Policy Document	Date of Review (IND-A-01)	Amendments Made? (Y/N) or New (IND-A-02), or other	Brief Description of Amendment or New Policy Document (IND-A-02)	Date Policy Document was Communicated to Agents, and Nature of Communications (IND-A-04)
Mobile Device Policy	Sep-15	Y	Relevant changes include consultation with EISO on access termination for staff on extended leave. The eligibility criteria have been updated to reflect staff (those on CCO payroll) who meet the policy criteria.	Posted on CCO's Intranet eCCO in November 2015.
Operational Security Standard	Aug-15	N	N/A	N/A
Physical Security Policy	Jul-15	N	N/A	N/A
Physical Security Policy	Aug-16	Y	Minor amendments to update closing of one of CCO physical location and add reference to relevant policy documents.	Posted on CCO's Intranet in October 2016.

Policy Document	Date of Review (IND-A-01)	Amendments Made? (Y/N) or New (IND-A-02), or other	Brief Description of Amendment or New Policy Document (IND-A-02)	Date Policy Document was Communicated to Agents, and Nature of Communications (IND-A-04)
Security Audit, Testing, and Compliance Standard	Aug-15	New	The standard defines the baseline practices for the audit and testing of CCO's information security.	Posted on CCO's Intranet in August 2015.
Security Risk Management Standard	Mar-14	N	N/A	N/A
Video Monitoring Policy	Jul-15	N	N/A	N/A
Video Monitoring Policy	Apr-16	Y	Updates made to reflect current practice	N/A – still in draft
Visitor Access Policy	Jul-15	N	N/A	N/A
Visitor Access Policy	Aug-16	Y	Minor amendments to update closing of one of CCO physical location.	Posted on CCO's Intranet in October 2016.
Visitor Access Procedure	Jul-15	N	N/A	N/A
Visitor Access Procedure	Aug-16	Y	Minor amendments to update closing of one of CCO physical location.	Posted on CCO's Intranet in October 2016.

Appendix D: Indicators – List of Data Linkages

Log of Permanent / Operational Linkages:

#	Data Holdings Linked	Resulting Data Holding Name
1	Screening Hub Stage Registered Persons Database (**RPDB**), Corporate Provider Database (**CPDB**), Screening Hub Stage Client Agency Program Enrolment (**CAPE**), Screening Hub Stage Cytobase, ICMS-OBSP, Screening Hub Stage Ontario Provincial Drug Programs (**OPDP**) (Pharmacy Claims), Screening Hub Stage Colonoscopy Interim Reporting Tool (**CIRT**), Screening Hub Stage Laboratory Reporting Tool (**LRT**), Screening Hub Stage Claims History Database (**CHDB**), Screening Hub Stage Ontario Cancer Registry (**OCR**)	Screening Hub Integration
	Within the Screening Hub Integration:	
2	ICMS-OBSP is linked to Screening Hub Stage RPDB and CPDB	
3	Screening Hub Stage Cytobase is linked to Screening Hub Stage RPDB and CPDB	
4	Screening Hub Stage CAPE is linked to Screening Hub Stage RPDB and CPDB	
5	Screening Hub Stage OPDP is linked to Screening Hub Stage RPDB	
6	Screening Hub Stage CIRT is linked to Screening Hub Stage RPDB and CPDB	
7	Screening Hub Stage LRT is linked to Screening Hub Stage RPDB and CPDB	
8	Screening Hub Stage CHDB is linked to Screening Hub Stage RPDB and CPDB	
9	Screening Hub Stage OCR is linked to Screening Hub Stage RPDB	
	Linkages within the Enterprise Data Warehouse (EDW):	
10	ALR, CIHI Discharge Abstract Database (**DAD**), CIHI National Ambulatory Care Reporting System (**NACRS**), eClaims (PDRP), Out of Province, RPDB, Death Data	OCR
11	Specialized Services Oversight (**SSO**), Regimen Drug Classification	Specialized Services Oversight Information System (**SSOIS**)
12	ISAAC, ALR	Symptom Management Database

#	**Data Holdings Linked**	**Resulting Data Holding Name**
13	OCR, Collaborative Staging Database	Collaborative Staging Integration

Appendix E: Indicators – Log of Privacy Impact Assessments

From November 1st, 2013 to October 31, 2016

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
Diagnostic Assessment Program – Electronic Pathway Solution (**DAP-EPS**) Phase II	PE	11/21/2013	Privacy Specialist	Patients are not required to scroll through the Patient Terms of Use prior to being able to accept the Patient Terms of Use and gaining access to the DAP-EPS. As a result, patients risk accepting the Patient Terms of Use without having actually read such Patient Terms of Use.	The "I Accept" electronic button respecting the Patient Terms of Use should be moved so that it appears below (and not above) the Patient Terms of Use.	LPO (Privacy Specialist); Business Unit Development Team	11/1/2013	The "I Accept" electronic button appears below the Patient Terms of Use.
DAP-EPS Phase II	PE	11/21/2013	Privacy Specialist	Caregivers are not required to scroll through the Caregiver Terms of Use prior to being able to accept the Caregiver Terms of Use and gaining	The "I Accept" electronic button respecting the Caregiver Terms of Use should be moved so that it appears below (and not above) the Caregiver Terms of Use.	LPO (Privacy Specialist); Business Unit Development Team	11/1/2013	The "I Accept" electronic button appears below the Caregiver Terms of Use.

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	P E or P P	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
				access to the DAP-EPS. As a result, Caregivers risk accepting the Caregiver Terms of Use without having actually read such Caregiver Terms of Use.				
DAP-EPS Phase II	P E	11/21/2013	Privacy Specialist	CCO has no control or oversight over the privacy practices and procedures of third party calendar services.	Revised Patient Terms of Use were prepared to require patients to assume the risk of sharing their PHI with a third party calendar service. It is recommended that patients be required to acknowledge and accept such revised terms of use as soon as reasonably possible, particularly given that such calendar feature went “live” absent this privacy risk having been mitigated.	LPO (Privacy Specialist); Business Unit Development Team	11/1/2013	The Patient Terms of Use address the risks of posting/sharing PHI with third party service resources.

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
DAP-EPS Phase II	PE	11/21/2013	Privacy Specialist	CCO has no control or oversight over the privacy practices and procedures of third party calendar services.	Notice language to appear when a patient selects the calendar tool feature in the DAP-EPS, which notice language will remind the patient of the privacy risk associated with sharing PHI with a third party entity. In addition, disclaimer language to be developed to be incorporated into the DAP-EPS.	LPO (Privacy Specialist); Business Unit Development Team	11/1/2013	Notice language is displayed on the "My Appointments" page in the DAP-EPS.
DAP-EPS Phase II	PE	11/21/2013	Privacy Specialist	Risk that DAP-EPS users will choose a personally identifying alias when given the choice to enter an alias prior to posting a DB Post on the DAP-EPS.	Notice language to appear next to the alias selection in the DAP-EPS to advise DAP-EPS users of the privacy risks associated with choosing an alias that risks being personally identifying.	LPO (Privacy Specialist); Business Unit Development Team	11/1/2013	Notice language to appear next to the alias selection in the DAP-EPS on or around November 30, 2013.
DAP-EPS Phase II	PE	11/21/2013	Privacy Specialist	Risk that DAP-EPS users will include PHI in their DB Posts.	Notice language to appear next to the user's draft DB Post in the DAP-EPS to advise DAP-EPS users of the privacy	LPO (Privacy Specialist); Business Unit Development Team	11/1/2013	Notice language is displayed on the draft Discussion Board Posts window.

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
					risks associated with including PHI in DB Posts.			
DAP-EPS Phase II	PE	11/21/2013	Privacy Specialist	Patient's Caregiver could post the patient's PHI on the discussion board absent the patient's consent, control and knowledge.	Current DAP-EPS users to be notified of the new DAP-EPS functionalities prior to being prompted to accept the Patient Terms of Use or the Caregiver Terms of Use, as the case may be. Such notice to outline, in particular, that all users, including Caregivers, have the ability to draft DB Posts and participate in the discussion board feature.	LPO (Privacy Specialist); Business Unit Development Team	11/1/2013	Notice language appears above Patient Terms of Use and Caregiver Terms of Use.
DAP-EPS Phase II	PE	11/21/2013	Privacy Specialist	Patient does not have the ability to remove a Caregiver's access to the patient's blog post once the patient has	Notice language to appear next to a patient's blog sharing option, advising the patient that once a blog post is shared with a Caregiver, such blog	LPO (Privacy Specialist); Business Unit Development Team	11/1/2013	Notice language appears next to the patient's blog sharing option.

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
				granted such access.	post is unable to be "unshared".			
Ontario Positron Emission Tomography Scan Evidence-Based Program (**EB-PET**): Pediatric PET Registry	PE	11/22/2013	Privacy Specialist	CCO has no current contractual controls in place to govern the disclosure of disclosed data to POGO.	Develop a DSA in accordance with the IPC Manual to be entered into between CCO and POGO.	LPO, Business Unit	3/3/2014	Execution of DSA prior to Project Go-Live date
SSOIS	PE	12/2/2013	Privacy Specialist	CCO has no contractual controls in place to govern the collection of the SSO data from the Facilities and CCO's subsequent intended uses and disclosures related therewith.	CCO to develop and enter into agreements with each of the Facilities concerning the collection, use and disclosure of SSO data prior to CCO's collection of any PHI from such Facilities.	LPO (Privacy Specialist), Regional Programs	10/25/2013	Execution of DSA prior to Project Go-Live date

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
SSOIS	PE	12/2/2013	Privacy Specialist	CCO's permanent retention of invalidated Raw SSO data is neither supported by *CCO's Privacy Policy*, nor is it compliant with privacy best practices.	Business Unit to ensure the timely destruction of invalidated Raw SSO data or explain to the LPO why it is necessary for such invalidated Raw SSO data to be retained by CCO indefinitely.	Project Manager, EISO (Information Security Advisor), Technical Architect	1/14/2014	A retention length of 13 months has been decided
SSOIS	PE	12/2/2013	Privacy Specialist	*CCO's Privacy Policy* requires each Program's data steward to maintain an inventory of data holdings that includes information on the format of the data (*i.e.,* paper or electronic), its physical location and the time span of the data.	Business Unit to confirm that a data steward has been assigned to the SSOIS Initiative, and that such individual will maintain an inventory of data holdings that includes information on the format of the data, its physical location and the time span of the data.	Project Manager, Director, Data Management	1/14/2014	List of data holdings is maintained and included in *CCO's Privacy Policy*

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
SSOIS	PE	12/2/2013	Privacy Specialist	CCO's permanent retention of validated Raw SSO data in the SSO Data Quarantine Area (**DQA**) database is not reasonably necessary, and is therefore not in line with privacy best practices.	Business Unit to demonstrate to the LPO how the validated Raw SSO data will be destroyed or removed from the SSO DQA database (subsequent to being copied and retained in the EDW) in a manner approved by EISO, and to confirm with the LPO the timing for such destruction.	Project Manager, EISO (Information Security Advisor), Technical Architect	3/15/2015	The SSO data will be retained in the DQA indefinitely as it is the source and raw data and will be relied upon should there be any errors or data accuracy issues with the data when it is used for reporting and analysis in the EDW. CCO has now established records retention series that have been approved by the Archivist of Ontario and that address the retention of PHI. Each Record Series sets out the approved retention for the data and records it covers based on the purpose of the record or data. CCO's Secure Retention of PHI Policy has been updated to reflect these new schedules. CCO's next step with data such as that in the DQA is to determine what the appropriate

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	P E or P P	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
								Record Series is and apply the appropriate retention period.

SSOIS	PE	12/2/2013	Privacy Specialist	The disclosure(s) contemplated by Disclosure #2 may include small cases, due to the nature of the disease, the specialized services offered by the Facilities, and the limited number of Facilities that provide these services for the specific disease group. There is therefore a low risk of the datasets included in the reports being used to identify an individual.	Business Unit to implement recommendations identified by the LPO in the Small Cell Report, attached hereto as Exhibit C.	Project Manager, Informatics Manager	10/4/2013	1) Program will consult with the LPO should there be an interest in disclosing these reports to stakeholders other than the MOHLTC, CCO agents or SSO facilities, such as publishing the data or presenting it at a conference. (2) All reports to include a footer stating: CONFIDENTIAL: Do not disclose report without CCO's prior consent. This footer should be visible in the reports/graphs presented in iPort and in the print out (paper copies) of the reports.(3) The Business Unit to ensure that all stakeholders who will be reviewing these reports have accepted the terms of the agreement(s) that are applicable to their role, *i.e.,* the CCO *Confidentiality Agreement*; the *Privacy and Security Acknowledgement Form*; and/or the iPort Terms of Use. (4) The Business Unit should consult with the LPO should there be a substantive change to the information that is to be included in the

								reports from what has been reviewed by Privacy

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
OCSP Phase II	PP	3/7/2014	Privacy Specialist	The proposed process to mail Phase II Correspondence via regular mail does not comply with CCO's *Transfer of PHI by Regular Mail Procedure*. As a result of not being in full compliance with its stated policy, the CSP is at risk that correspondence not marked "confidential" will be subject to unauthorized disclosures (*i.e.,* privacy breaches) when opened by someone other than the Intended Recipient.	The CSP should exhaust the current stock of envelopes used for correspondence (anticipated to occur by approximately December 2013) and ensure that when re-ordered, the envelope stock is clearly marked with the label "Confidential".	Business Unit	March/April 2014	As per the recommendation, the existing stock was exhausted before the new stock was ordered

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
eReports (Secure Messaging Solution) – PC SAR Release 1	PP	3/21/2014	Privacy Specialist	CCO has taken the position that it will honour all "legacy consents" provided by women in response to the three questions in the Consent Form. As such, a woman's "no" response to question 1 above must be taken into account in the production of the PC SAR. If this is not done, there is a risk that such PHI may be provided to a PCP where a woman has declined to consent.	The business requirements document (**BRD**) for PC SAR indicates that the system shall ensure that patient enrolment model (**PEM**) physicians and their delegates are not able to see data for women who have opted-out of sharing their information. The PC SAR project team must verify that this requirement has been successfully implemented prior to the launch of the PC SAR.	Business Unit	4/1/2014	The build-up of PC SAR ensure that PEM physicians and their delegates are not able to see data for women who have opted-out of sharing their information.

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
eReports (Secure Messaging Solution) - PC SAR Release 1	PP	3/21/2014	Privacy Specialist	The CCO CC must be prepared to respond to physician inquiries regarding the latest iteration of the PC SAR which will now include cervical and breast screening data in addition to colorectal screening data. Particularly, the CC will need to be prepared to respond to questions about why the PCP cannot see data about particular patients where the status is shown as greyed out in the PC SAR.	Existing CC FAQs and SOPs should be updated to reflect the inclusion of cervical and breast screening data, as well as address questions with respect to patients where it is indicated that no screening status data is available. The SOPs and FAQs must clearly indicate that a woman's opt-out status with respect to breast screening data must not be disclosed to physicians.	Business Unit	March/April 2014	The CC were provided specific SOPs which related to OCSP.

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
eReports (Secure Messaging Solution) - PC SAR Release 1	PP	3/21/2014	Privacy Specialist	The PC SAR BRD has identified the risk that if ICMS is unable to match an opt-out to a master person record in InScreen due to mistakes in ICMS data entry at the OBSP site, that this may result in an opt-out not being assigned, and the woman's breast screening data being included in the PC SAR.	As outlined in the PC SAR Business System Requirements Document (BSRD), cases where an opt-out is unable to be matched to a master person record will be flagged and reviewed prior to issuing the PC SAR. In the case of significant incidence, the matching algorithm may be re-programmed to minimize the risk of a breach. The PC SAR project team must verify that these actions have been successfully implemented prior to the launch of the PC SAR.	Business Unit	4/1/2014	The build-up of PC SAR ensure that PEM physicians and their delegates are not able to see data for women who have opted-out of sharing their information.
eReports (Secure Messaging Solution) – PC SAR Release 1	PP	3/21/2014	Privacy Specialist	The PC SAR ICMS CR has identified a risk of delayed breast cancer diagnoses (*i.e.,* ICMS contains a more timely diagnosis date),	The delayed diagnosis issue caused by the OCR data quality should be addressed in the new release of the PC SAR. Project team to confirm including the ICMS	Business Unit	10/06/2014	The PCSAR is consuming and using cancer information from ICMS for OBSP which is declared as a 'Most Confirmed Cancer' and is timelier than the OCR

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
				which may impact the accuracy of the data included in the PC SAR.	data diagnoses information in the next release.			
eReports (Secure Messaging Solution) – PC SAR Release 1	PP	3/21/2014	Privacy Specialist	The PC SAR BRD has identified the risk that if CC staff can see breast PHI for women who have opted out of sharing this information, that there is no technical control in place preventing the CC staff from identifying this for the PCP.	a) As outlined in the PC SAR BRD, changes to Siebel and Oracle Business Intelligence Enterprise Edition (**OBIEE**) must be implemented to include fields identifying a woman's opt-out status and to include a pop-up alert which will appear each time a record for a woman who has opted-out is accessed in Siebel. The pop up alert will state: "Alert: Patient has opted out. No breast PHI can be disclosed to PCP". The PC SAR project team must verify that these requirements have been successfully	Business Unit	04/07/2014	CC staff are presented with a pop-up message that indicates the client has opted-out of sharing their PHI and the client's PHI contained in Siebel most not be disclosed.

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	P E or P P	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
					implemented prior to the launch of the PC SAR. b) The relevant CC SOPs and FAQs related to PC SAR must be updated to indicate that the fact that a woman has opted out cannot be shared with a PCP. The LPO must review and approve the revised SOPs and FAQs.			

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
OBSP Correspondence Phase I (Invitations and Privacy Notices) & PC SAR "Readiness"	PP	3/31/2014	Privacy Specialist	Notwithstanding the fact that it is necessary for CCO to collect the PHI of non-OBSP clients, in the absence of any authoritative documentation it is not possible to confirm that it is necessary for CCO to collect all of the PHI data elements related to women who are not clients of OBSP for cancer screening purposes. Accordingly, CCO is exposed to the risk that it is collecting PHI in a manner inconsistent with Principle 4 of *CCO's Privacy Policy* 1 – that CCO limits the collection of PHI to that which is necessary for identified	1) CCO must identify the undocumented collection, use and disclosure of non-OBSP client PHI from the Sites as an Enterprise Risk. 2) CCO must begin to consider the internal and external processes, procedures, communications (*e.g.,* to the Sites providing CCO with non-OBSP client PHI) and all other activities (*e.g.,* changes to ICMS) that must be revised in order to ensure that: (a) CCO only collect such non-OBSP client PHI as is required for Cancer Screening purposes; and (b) such collection is acknowledged and documented.	Business Unit	N/A	This risk is being addressed as part of OBSP Program PIA

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	P E or P P	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
				purposes and in accordance with the requirements set out in PHIPA. If the collection of some of this PHI is unnecessary, it follows that any subsequent use and/or disclosure of this non-OBSP client data also represents a privacy risk. In addition, CCO does not indicate in any of its outward facing privacy documentation that it collects this PHI.				

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
OBSP Correspondence Phase I (Invitations and Privacy Notices) & PC SAR "Readiness"	PP	3/31/2014	Privacy Specialist	Contractual authority for Collection #1 may not be in place because all of the Amending Agreements and Funding Agreements for new Sites have not been signed back to CCO prior to the Project go-live.	The Program must confirm that all of the OBSP Amending Agreements and Funding Agreements for new Sites have been signed back to CCO prior to the go-live of the CCO OBSP Correspondence Project – Phase I.	Business Unit	Fiscal 2014/2015	The applicable funding agreements have been executed
OBSP Correspondence Phase I (Invitations and Privacy Notices) & PC SAR "Readiness"	PP	3/31/2014	Privacy Specialist	Notwithstanding the fact that CCO has acknowledged and accepted the risk of proceeding with the Project given the identified vulnerabilities in ICMS, CCO remains exposed to a continuing risk related to the security of the breast screening data and consequently the privacy of the	CCO should ensure that: (a) all of the outstanding remediation items identified in the ICMS VA are either implemented to EISO's satisfaction in the re-design of ICMS, or (b) the security risks associated with continued delay in implementing any of these remediation items must be presented to CCO senior management and accepted by	EISO	Fiscal 2014/2015	This risk is managed by EISO via the VA risk management plan

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
				individuals to whom this PHI relates.	CCO senior management.			
OBSP Correspondence Phase I (Invitations and Privacy Notices) & PC SAR "Readiness"	PP	3/31/2014	Privacy Specialist	OBSP is currently identified as a PE data holding in *Appendix "B"* to *CCO's Privacy Policy.* Post-Transition this will not constitute an accurate statement of either the role in which CCO collects this PHI, or the purposes for which the data is collected. Similarly the description of the Screening Hub Stage-OCSR and Screening	CCO must revise: i. the List of Data Holdings contained in the Appendices to *CCO's Privacy Policy* to reflect the operation of OBSP as a PR; and ii. the CCO and OBSP Statement of Information Practices as needed to reflect CCO's operation of the correspondence program.	LPO	8/1/2016	The policy has been updated to reflect the changes. The second part of the recommendation is being addressed as part of OBSP Program PIA risks.

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	P E or P P	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
				Hub Stage RPDB data holdings will no longer be accurate. The CCO and OBSP Statements of Information Practices do not constitute an accurate statement of the collection, use and disclosure of PHI for the purposes of the OBSP correspondence program.				

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	**PE or PP**	**Date of Completion of PIA (or Date Expected to be Completed)**	**Person Responsible for Completing PIA**	**Privacy Risks arising from the PIA**	**Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA**	**Responsible Party for Addressing Each Recommendation**	**Date that Each Recommendation was Addressed (or is Expected to be Addressed)**	**The Manner in which Each Recommendation was or is Expected to be Addressed**
OBSP Correspondence Phase I (Invitations and Privacy Notices) & PC SAR "Readiness"	PP	3/31/2014	Privacy Specialist	Numerous CCO procedures and processes address the implementation of *CCO's Privacy Policy* as applicable to the OBSP as a PE. There is a risk that they do not address how CCO implements the policy as it will apply to OBSP as a PE post-Transition. Examples of these include the *Integrated Cancer Screening Program (**ICSP**) FAQs; Withdrawal of Consent Form; ICSP PHI Correction Form, ICSP Privacy Acknowledgement Form, ICSP Privacy Inquiries and Complaints Procedure, CCO Access and*	All of CCO's documented cancer screening policies and procedures should be reviewed and, where required, amended to reflect CCO's operation of the OBSP as a PP post-Transition.	LPO and Business Unit	Fiscal 2014/2015	CCO LPO has consolidated privacy policies for both PE and PP to reflect privacy operations as one activity for the organization

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	P E or P P	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
				Correction Procedure and the *ICSP Data Request Procedure.*				

OBSP Correspondence Phase I (Invitations and Privacy Notices) & PC SAR "Readiness"	PP	3/31/2014	Privacy Specialist	It is reasonable to assume that the elimination of the Existing Form (with its associated consents) as part of the transition of OBSP from CCO's role as a PE to a PP, will raise questions in the minds of women attending at the Sites for breast screening. Those who have previously signed the Existing Form may wonder if their previously expressed wishes will still be honoured by CCO. Women who have never been screened may not understand why CCO does not require their consent to collect their PHI. Furthermore, personnel at the Sites must have an excellent understanding of the changes made to the information they	CCO must: i. review its public facing communications material related to the OBSP and amend it as required to include, at minimum, information related to the fact that women will not be required to complete the Existing Form, the reasons therefore and that CCO will now be sending out Privacy Notices to individuals who have not received one from the OCSP, and that restrictions on the use of OBSP data contained in the Existing form will be honoured; ii. develop communications materials for the Sites on the Transition (the Site Materials) and the consequence that as of the transition date, CCO will now be sending out Privacy Notices to individuals and, as a result, clients will not be required to complete the Existing Form; iii. deliver training via conference call or	LPO	Fiscal 2014/2015	Transition to OBSP including sending of privacy notice is complete. The risk related to consent form is managed via the OBSP Program PIA

				provide to women related to the OBSP and the use of their PHI to respond to such questions and any concerns.	other means to the Sites on the Site Materials and require attendance by site Privacy Officers and/or another individual at the site who is responsible for privacy matters; and iv. ensure that the LPO reviews and approves all of the communications and training materials developed to explain the Transition.			

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
OBSP Correspondence Phase I (Invitations and Privacy Notices) & PCSAR "Readiness"	PP	31-Mar-14	Privacy Specialist	CCO has entered into DSAs with numerous entities in which CCO as a PE may be either collecting or disclosing ICMS data. CCO must be able to confirm that any changes to its authority to collect, use and/or disclose ICMS data as the case may be are captured in these agreements.	CCO must: i. review all of its DSAs, both internal to CCO (PE to PP) and external, in which ICMS and/or other OBSP PHI is involved, or which contain data that will be linked with OBSP data; ii. amend these agreements as required to reflect CCO's status as a PP in the operation of OBSP; iii. ensure that as a PP, CCO may still collect, use and disclose the ICMS or other OBSP PHI, as contemplated in each agreement; iv. ensure that the purpose for which CCO may collect, use and disclose such data may be continued when it begins to operate the OBSP as a PP; and v. if it lacks the authority as a PP to collect, use and/or disclose the ICMS or	LPO	May-01-2016	The DSA (PHAC DSA) which reference OBSP role as a PE has been amended to reflect the correct authority for OBSP.

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	P E or P P	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
					other PHI as contemplated in the DSA, consider how such objectives may be accomplished through other legal mechanisms.			

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
OBSP Correspondence Phase I (Invitations and Privacy Notices) & PC SAR "Readiness"	PP	31-Mar-14	Privacy Specialist	The Project represents the first time that CCO has sent OBSP screening correspondence and that ICMS data has been used as a data set for provincial correspondence, albeit mainly to identify women to whom correspondence should not be sent. Accordingly, a risk exists that the OBSP Invitations will be sent to the incorrect address and a privacy breach could result.	CCO should review and, where required, revise SOP #06.10.02 (Address Management Return Rate threshold) to specifically deal with matters related to OBSP Correspondence. The review should include, but not be limited to: - the timing of the evaluation of the Correspondence Return Rates; - the use of the CCC historical data for invitations as the basis for the calculation of the return rates; and - the Level 1 (1.5 times the sample standard deviation) and Level 2 (2 times the sample standard deviation) rates that trigger the actions set out in the SOP.	Business Unit	Fiscal 2014/2015	Return Management is an existing process and was updated to include OBSP correspondence

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
OBSP Correspondence Phase I (Invitations and Privacy Notices) & PC SAR "Readiness"	PP	31-Mar-14	Privacy Specialist	A number of SOPs with associated scripts have been developed to assist CC staff with managing opt-outs as well as responding to questions and/or complaints from individuals who have received screening correspondence from CCC and/or OCSP. It is reasonable to assume that the CC will receive similar communications in response to the sending of the OBSP Correspondence, particularly because of the change in the consent model. Staff must therefore understand how to accurately address privacy-	CCO should review and, where required, revise all relevant cancer screening FAQs and CC SOPs. NOTE: combined with Mitigating Strategy #9 on the Master Recommendations List	Business Unit	March/April 2014	The FAQs have been updated to reflect the changes as a result of OBSP screening program.

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	P E or P P	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
				related inquiries and concerns.				

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
OBSP Correspondence Phase I (Invitations and Privacy Notices) & PC SAR "Readiness"	PP	31-Mar-14	Privacy Specialist	Privacy Notices must be sent to Eligible Participants at least 30 days prior to the sending of Results. There is a risk that if InScreen is not programmed properly, Results could be sent to an Eligible Individual in a period of less than 30 days; *i.e.,* 30 days may have elapsed between the provision of the initial notice (which the Eligible Participant did not receive) but not between the resending of the notice and the sending of Results.	CCO must develop and implement a process to ensure that the date of the provision of any resent Privacy Notices is the date used for the calculation of the 30-day period prior to the sending of Results.	Business Unit	March/April 2014	CCO developed and implemented a process to ensure that the date of the provision of any resent Privacy Notices is the date used for the calculation of the 30-day period prior to the sending of Results.

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
OBSP Correspondence Phase I (Invitations and Privacy Notices) & PC SAR "Readiness"	PP	31-Mar-14	Privacy Specialist	At the present time Amending Agreement #3 to the CCO PE to PP DSA does not address the transfer of those ICMS PHI data elements to InScreen that are required for the production of the breast screening activity report (**SAR**) or the purposes for which such PHI will be used and disclosed.	CCO must confirm that the LPO has revised its internal and external DSA such that CCO may use ICMS, including the OBSP data (breast screening data) that is reasonably necessary for the creation and disclosure of the PC SAR, as a PP.	LPO	N/A	Since OBSP changed from PE to PP, there was no need for any further DSA

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
OBSP Correspondence Phase I (Invitations and Privacy Notices) & PC SAR "Readiness"	PP	31-Mar-14	Privacy Specialist	Because the OBSP has in the past operated on the basis of an "express consent" model, a woman who previously declined to have her breast screening data provided to her PCP may change her mind and subsequently agree to such disclosure of her PHI. In the absence of a process to capture this change in consent, CCO will be unable to honour her wishes, a component of the transition of the OBSP from a PE to a PP.	CCO must develop and implement a process whereby it may track and give effect to a woman's wishes to change her response to Question #1 of the Existing Form from "no" to "yes"; *i.e.,* to provide her OBSP PHI to her PCP.	Business Unit	Feb-26-2014	06.02.07 - OBSP Authorization for the Release of Personal Health Information Form Inquiry has been created for the Contact Centre to handle inquiries from clients wishing to change their responses from past screening visits. Additionally, the OBSP Site FAQs (Q11) provides instructions to OBSP Sites for women who wish to change their responses. The Contact Centre training on this SOP has been completed.

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
ORN Acquisition of OLIS data - Phase I	PE	27-May-14	Privacy Specialist	Contractual authority for Collection #1 is not currently in place because the MOHLTC-CCO DPA Amending Agreement is still in draft form and has not been executed.	Before the date on which CCO begins to collect OLIS data from eHO, the ORN must ensure that the MOHLTC-CCO DPA Amending Agreement has been fully executed (*i.e.,* signed by the MOHLTC and CCO) and that the OLIS data is included as an Appendix thereto. This is a 'pre go-live requirement' for Phase 1.	LPO	June 18, 2014	Agreement has been executed

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
ORN Acquisition of OLIS data - Phase I	PE	27-May-14	Privacy Specialist	eHO's inability to filter out unnecessary OLIS data creates the risk that this transfer of PHI does not comply with s. 30(2) of PHIPA. Subsection 30(2) states that "[a HIC] [*i.e.,* the MOHLTC, acting through its agent, eHO] shall not collect, use or disclose more PHI than is reasonably necessary to meet the purpose of the collection, use or disclosure, as the case may be."	1. All unnecessary OLIS data transferred by eHO to CCO will be filtered out by CCO through its eLab solution; 2. CCO will promptly delete any unnecessary OLIS data through its eLab solution once the raw OLIS data disclosed to CCO by eHO has been filtered; 3. CCO will immediately confirm to the MOHLTC in writing once the secure deletion of the unnecessary OLIS data has been completed; and 4. CCO will not use any unnecessary OLIS data for the purposes of Phase One.	Group Manager, ORN Information Program and Cancer Implementation Team, ATC and ORN Information Program	May 27, 2014	This tool was not used, therefore this risk no longer applied.
ORN Acquisition of OLIS data - Phase I	PE	27-May-14	Privacy Specialist	The ORN has not yet defined the time period for which the OLIS data will	Before the end of Phase 1 and the start of Phase 2, the ORN must confirm the length of time	Group Manager, ORN Information Program and Cancer Implementation Team, ATC and	June 18, 2014	Retention period of data set out in agreement with MOHLTC.

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
				remain in the DQA.	the OLIS data will remain in the DQA.	ORN Information Program		
ORN Acquisition of OLIS data - Phase I	PE	27-May-14	Privacy Specialist	EISO has not yet finalized the TRAthat includes a security review on the DQA at CCO.	EISO must complete a security review and approve the DQA for storage of the OLIS data. This is a 'pre go-live requirement' for Phase 1.	Director, Architecture & Information Security Services, Technology Services/Group Manager, ORN Information Program and Cancer Implementation Team, ATC and ORN Information Program	May 27, 2014	The storage of the OLIS data was reviewed and approved by EISO.
ORN Acquisition of OLIS data - Phase I	PE	27-May-14	Privacy Specialist	The OLIS data has not yet been logged as a new data holding by Informatics.	Informatics must log the OLIS data as a new data holding. This is a 'pre go-live' requirement for Phase 1.	Director, Data Assets, Analytics & Informatics	May 27, 2014	The OLIS data was logged as a data holding.
ORN Acquisition of OLIS data - Phase I	PE	27-May-14	Privacy Specialist	The public has not been provided with notice of CCO's custody and/or control of the OLIS data.	The LPO must amend *CCO's Privacy Policy* so as to appropriately reference the OLIS data as part of its next update to these policies. This amendment must be	LPO	May 27, 2014	This is not applicable as CCO is not retaining data.

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
					completed by June 1, 2014.			
ORN Acquisition of OLIS data - Phase I	PE	27-May-14	Privacy Specialist	EDM to confirm that the OLIS data within the DQA has been registered as a data holding for the purposes of CCO's *Direct Data Access Procedure*.	EISO must confirm that LMAS will apply to the OLIS data within the DQA. This is a 'pre go-live' requirement for Phase 1.	Director, Architecture & Information Security Services, Technology Services	May 27, 2014	LMAS applies to the DQA.
ORN Acquisition of OLIS data - Phase I	PE	27-May-14	Privacy Specialist	EDM to confirm that the OLIS data located on the H: Drive has been registered as a data holding for the purposes of CCO's *Direct Data Access Procedure*.	EISO must confirm that LMAS will apply to the OLIS data that is analyzed in the H: Drive. This is a 'pre go-live' requirement for Phase 1.	Director, Architecture & Information Security Services, Technology Services	May 27, 2014	Data on the H drive is subject to CCO's LMAs system.
ORN Acquisition of OLIS data - Phase I	PE	27-May-14	Privacy Specialist	EDM to confirm that individuals that need access to the OLIS Reports containing PHI	EISO must confirm that LMAS will apply to the OLIS Reports in the H: Drive. This is a 'pre go-live'	Director, Architecture & Information Security Services,	May 27, 2014	Access will occur via CCO's IDAR process.

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
				will do so via the IDAR process.	requirement for Phase 1.	Technology Services		
ORN Acquisition of OLIS data - Phase I	PE	27-May-14	Privacy Specialist	The ORN has not yet provided a time frame for how long the OLIS Reports containing PHI will be kept on the H: Drive.	The ORN must provide a plan for how the OLIS Reports containing PHI will be used and stored, along with the retention period for such OLIS Reports. This plan must be explicitly outlined in Phase 2.	Group Manager, ORN Information Program and Cancer Implementation Team, ATC and ORN Information Program	May 27, 2014	There are no reports stored on H drive, so this is risk is not applicable.
ORN Acquisition of OLIS data - Phase I	PE	27-May-14	Privacy Specialist	EDM to confirm that the ORRS-OLIS data has been registered as a data holding for the purposes of CCO's *Direct Data Access Procedure* in the Statistical Analysis System (**SAS**).	EISO must confirm that LMAS will apply to the ORRS-OLIS data in SAS. This is a 'pre go-live' requirement for Phase 1.	Director, Architecture & Information Security Services, Technology Services	May 27, 2014	Data on the H drive is subject to CCO's LMAs system.
ORN Acquisition of OLIS data - Phase I	PE	27-May-14	Privacy Specialist	EDM to confirm that individuals that need access to the OLIS-ORRS Reports containing PHI	EISO must confirm that LMAS will apply to the OLIS-ORRS Reports in the H: Drive. This is a 'pre	Director, Architecture & Information Security Services,	May 27, 2014	Access will occur via CCO's IDAR process.

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
				will do so via the IDAR process.	go-live' requirement for Phase 1.	Technology Services		
ORN Acquisition of OLIS data - Phase I	PE	27-May-14	Privacy Specialist	The ORN has not yet provided a time frame for how long the OLIS-ORRS Reports will be kept on the H: Drive.	The ORN must provide a plan for how the OLIS-ORRS Reports will be used and stored, along with the retention period for the OLIS-ORRS Reports. This plan must be explicitly referenced in Phase 2.	Group Manager, ORN Information Program and Cancer Implementation Team, ATC and ORN Information Program	May 27, 2014	There are no reports stored on H drive, so this is risk is not applicable.

ORRS Partial Release 4.0 (ORRS R.4.0)	P E	3-Sep-14	Privacy Specialist	Recommendations #34 and #35 made in the First Addendum have yet to be implemented. They recommended that:1 i) CCO include a reference to the License and HINP Agreement, the First Addendum and the TRA(s) conducted on ORRS R.3.0 in the list of "References" that inform the *HINP Policy*; and ii) CCO draft a description of the ORRS R.3.0 web application and upload tool to be included in Appendix "A" to the *HINP Policy*. These Recommendations were made to manage the risk of CCO not being completely open with respect to the information services it provides to HICs and for which it is subject to additional	CCO should implement Recommendations #34 and #35 made in the First Addendum and include a reference to this Second Addendum in the "References" Section of the HINP Privacy Policy. It should also draft a description of the ORRS 3.0 and 4.0 mini applications to include in Appendix "A" of the policy.	LPO	Sep-03-2014	The agreements will be assessed to ensure they meet CCO's legal obligations as a HINP. The HINP Policy has been incorporated into CCO's Privacy Policy.

				privacy requirements under PHIPA. This risk is heightened with the implementation of ORRS R.4.0 mini because the "Services ", as defined in the HINP and License Agreement, will include CCO's facilitation of the communication between the CKD Service Providers of data – the "new PHI" - "… in respect of ORRS…" that is not included in the definition and must therefore be "… set out in CCO's policies and procedures in respect of ORRS…"				

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
Expanded Prostate Cancer Index (**EPIC**) Prostate Cancer Pilot Project	PE	15-Oct-14	Privacy Specialist	Unless and until the data steward includes all of the PHI collected by CCO for the purposes of the Study in the inventory of data holdings as required by *CCO's Privacy Policy*, the Project's practices for the retention and destruction of the collected data do not appear to comply with CCO's policies.	The data steward should create an inventory, including the information required by Principle 5.5 of *CCO's Privacy Policy*, of the data specifically collected for the purposes of the Study: the EPIC–CP data stored in the Ontario Cancer Symptom Management Collaborative (**OCSMC**) Symptom Management Reporting Database received from CV, KGH and CR; and the Expanded Prostate Cancer Index Composite – Short Form data from Princess Margaret Hospital (**PMH**), and the Study Access Database from all four sites stored on the H: Drive.	Director, Analytics and Informatics	Oct-31-2015	Worksheet capturing all the recommendations created (See Worksheet in Appendix C of updated PIA for details)

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
EPIC Prostate Cancer Pilot Project	PE	15-Oct-14	Privacy Specialist	There exists a risk that until CCO addresses the issues related to how long the use output will be retained, where it will be retained, who will have access to this PHI and the manner and timing of its destruction, the Project's practices for the retention and destruction of the collected data do not appear to comply with CCO's policies.	CCO should identify and the retention period, location of storage, access to and the manner and timing of the destruction of this use output rights to this used data and ensure that these practices comply with CCO's policies.	Director, Analytics and Informatics	Oct-31-2015	Worksheet capturing all the recommendations created (See Worksheet in Appendix C of updated PIA for details)
ADT Integration	PE	3-Nov-14	Privacy Specialist	CCO may not be in full compliance with the requirements of ss.6(3) of the Regulation in its operation of ISAAC as a HINP.	CCO must implement the requirements of ss.6(3) of the Regulation.	Business Unit and LPO	Nov./Dec 2013	The plain language description for ISSAC was updated and posted.

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
CCAC/LTC Funding Model	PE	19-Nov-14	Privacy Specialist	If the current OACCAC DSA is not amended and signed by the OACCAC before CCO begins collection of the PHI from the CCACs, there is a risk that CCO does not have the authority to collect the new CCAC data from the OACCAC and does not have the appropriate contractual controls in place to govern the collection of this information.	CCO must ensure that the current OACCAC DSA is amended and signed by the OACCAC before it begins the collection of PHI related to the CCAC patients.	LPO	November 19, 2014	The agreements have been signed.
CCAC/LTC Funding Model	PE	19-Nov-14	Privacy Specialist	If the CKD Management Agreements are not signed back by each of the long-term care homes (**LTCHs**) before CCO begins collection of the PHI from the LTCHs, there	CCO must ensure that the CKD Management Agreements are signed back by all LTCHs before it begins the collection of PHI from them.	LPO	November 19, 2014	Data elements are incorporated into agreements.

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
				is a risk that the agency does not have the appropriate contractual controls in place to govern the collection of the LTCH data.				
CCAC/LTC Funding Model	PE	19-Nov-14	Privacy Specialist	Section D – Performance Monitoring - of Schedule "C" of the 2014/15 CKD Management Agreements with the LTCHs contemplates that the provision of data by the LTCHs to CCO will "evolve over time". Because the PHI to be provided to CCO by the LTCHs is not included in these agreements, there is a risk that any additional PHI	The 2015/16 and all future CKD Management Agreements with the LTCHs should include the list of PHI data elements that are to be provided to CCO pursuant to the agreements.	LPO	Nov-19-2014	Data elements are incorporated into agreements.

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
				data elements that are required in the future will not be assessed to determine if it is "reasonably necessary" that they be collected by CCO for the PE purpose.				
The INTEGRATE Project	PE	21-Jan-15	Privacy Specialist	There is a risk of more data being collected than necessary for the purposes of the evaluation or for the purpose of facilitating linkages with other data sets.	Project team has identified the minimum elements necessary and provided a list to LPO of all elements and the purpose for the collection.	Group Manager, ORN, Integrated Care Strategy Design	January 15, 2015	Project team must provide the elements for review.

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
The INTEGRATE Project	PE	21-Jan-15	Privacy Specialist	There was no contractual relationship between the PCPs and CCO or between the regional cancer centres (**RCCs**) and CCO the authority for the data collection.	Amended DSAs were established with the RCCs and new Collaboration Agreements were established with the PCPs.	Group Manager, ORN, Integrated Care Strategy Design	January 15, 2015	Agreements have been established.
The INTEGRATE Project	PE	21-Jan-15	Privacy Specialist	As the data to be transferred contains PHI the transfer must be secure.	Each project site has been given a secure Tumbleweed account to transfer the data.	Group Manager, ORN, Integrated Care Strategy Design	Jan-15-2015	Secure transfer method established.
The INTEGRATE Project	PE	21-Jan-15	Privacy Specialist	There is a risk the data will be retained longer than necessary and/or abandoned and never deleted once the purpose has been fulfilled.	When the CCO enterprise-wide record retention schedules are approved and implemented, the data should be evaluated to determine which schedule applies. Data should be retained for no longer than the period noted in the schedule.	Director Integrated Care Strategy Design, Ontario Renal Network	January 15, 2015	Data will be kept in accordance with CCO's record retention schedules.

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
The INTEGRATE Project	PE	21-Jan-15	Privacy Specialist	There is a risk data will be used for linkages unnecessarily. There is a risk data will be linked without CCO having the proper authority to make the linkage.	Project team will provide a list of any new data sources used for linkages so that LPO can conduct a linkage analysis.	Group Manager, ORN, Integrated Care Strategy Design	January 15, 2016	Linkages identified and reviewed prior to approval.
The INTEGRATE Project	PE	21-Jan-15	Privacy Specialist	There is a risk that data will be disclosed in a manner that is not in compliance with the applicable DSAs. These include: a) requirements in CCO's DSA with CIHI governing the NACRS data, stating that no data will be published without the required disclaimer provided by CIHI; b) requirements that cell counts	The INTEGRATE Project will notify LPO prior to disclosing any data to third parties and LPO, with the Informatics program, will support the Project team in meeting all requirements for disclosure.	Director Integrated Care Strategy Design, Ontario Renal Network	January 15, 2015	Any disclosures will be provided for review prior to occurring.

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
				of less than 5 be suppressed; c) and several requirements in CCO's DSA with the OACCAC as noted in section 5.2.3.				
The INTEGRATE Project	PE	21-Jan-15	Privacy Specialist	There is a risk if notification obligations required under FIPPA s. 39(2) are not met.	LPO has prepared a Notice of Collection and the project team has incorporated it into the survey.	Group Manager, ORN, Integrated Care Strategy Design	January 15, 2015	Notice of Collection incorporated.
The INTEGRATE Project	PE	21-Jan-15	Privacy Specialist	Only the Enterprise version has been approved for the collection and storage of a minimal amount of PI. There is no version of Fluid Survey currently approved to hold PHI or other	INTEGRATE Project has purchased the Enterprise version of Fluid Survey for the purposes of administering the survey to healthcare providers. INTEGRATE Project to consult with LPO and EISO prior to using Fluid Survey	Group Manager, ORN, Integrated Care Strategy Design	January 15, 2015	Fluid Survey is not being used for the collection of personal health information.

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
				highly sensitive data.	for the collection of more PI or PHI.			
OBSP Correspondence Phase II: Invitation-Reminders, Recalls, Recall-Reminders and Normal Results	PP	22-Jan-15	Privacy Specialist	While the general content of the Phase II correspondence has been determined, it has yet to be finalized. Accordingly, this legislative and privacy analysis is based on the information available at the currency date of this PIA Addendum as described in PIA Table 1. Given that changes to the PI and/or PHI included in the correspondence may be made,	Prior to "go-live", the Provincial Operations Unit of the CS program must provide the LPO with copies of OBSP Phase II correspondence for the LPO's review and assessment of any changes made as identified in Outstanding Privacy Risk #1. Once finalized, copies of the Phase II correspondence should be attached to this document as the Appendices noted in the Table of Contents of this PIA Addendum.	Privacy Specialist (LPO)	Feb-19-2015	Reviewed final letters and confirmed that there were no concerns. PIA appendices updated to include copies of the letters.

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	P E or P P	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
				the legislative and privacy analysis in this PIA Addendum may not be accurate.				

OBSP Correspondence Phase II: Invitation-Reminders, Recalls, Recall-Reminders and Normal Results	PP	22-Jan-15	Privacy Specialist	In providing services as a HINP to the Sites, CCO does not have the authority to use all of the PHI for PP purposes, including breast screening correspondence, unless the data elements are first identified, the necessity of their use for the PP Purpose confirmed and CCO's legislative and contractual authority established. Without these determinations having been made, CCO has not established that it is reasonably necessary to collect and use the non-OBSP client data, as well as all of the PHI of OBSP clients for the purpose of breast screening correspondence.	(i) CCO must identify and document those data elements in ICMS (of both non-OBSP and OBSP Clients) the use of which are reasonably necessary (*i.e.,* set out the purpose for their use) for its operation of the OBSP as a PP, including breast screening correspondence; (ii) Working with the team developing the changes to ICMS and the data segregation project, the OBSP must ensure that the PHI data elements that have been identified and documented in accordance with Privacy Control (i), are managed by CCO in a PP data holding separate and distinct from the ICMS database (the "OBSP PP Database"); (iii) Once Privacy Control (ii) has been implemented, CCO must revise the description of the OBSP as it appears in Appendix C of *CCO's Privacy*	Privacy Specialist (LPO)	Feb-01-2015	This recommendation is also part of the OBSP PIA and will be responded to as part of the OBSP Program PIA.

					Policy 1 - CCO Primary Data Holdings for the Prescribed Person; and (iv) CCO must develop policies and procedures to ensure that only PHI from the OBSP PP Database and only that PHI that is reasonably necessary for the purposes of breast cancer screening correspondence is used as noted in the PHI data flow diagram: a. For Use #1: linkage with OCR to determine the Eligible Participants b. For Use #2: the creation of the subset (the InScreen nammogram (**MM**)-related screening data) of the breast screening data for subsequent transfer to the InScreen Hub			

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
OBSP Correspondence Phase II: Invitation-Reminders, Recalls, Recall-Reminders and Normal Results	PP	22-Jan-15	Privacy Specialist	All OBSP correspondence is sent by regular mail. It is possible that the OBSP policy of a 2-week time period for the sending of results after screening is not sufficient to allow CCO to "deem" that a woman has received the Privacy Notice prior to the sending of her Normal Results (*i.e.,* to account for the time taken for the Privacy Notice to be delivered, returned if the address is incorrect and logged in InScreen). There is a privacy risk that a woman may not have received the Privacy Notice before CCO	CCO, including a representative of the LPO, must develop and implement a process for the delivery of the Privacy Notice for OBSP Correspondence Phase II to ensure that at least 30 day have passed between the sending of the Notice and the sending of the results such that CCO may deem the Notice to have been received if it is not returned to CCO within that time period.	Business Unit	Mar-05-2015	The Privacy Notice delivery schedule was developed

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	P E or P P	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
				sends the OBSP Normal Results correspondence and thus not be in compliance with the general understanding that the “30-day rule” was to also apply to OBSP Correspondence.				

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
OBSP Correspondence Phase II: Invitation-Reminders, Recalls, Recall-Reminders and Normal Results	PP	22-Jan-15	Privacy Specialist	As currently drafted, the Funding Agreements do not clearly identify the PHI that the Sites are to provide to CCO in its role as a PP. The current reference to the "data elements" in Schedule "C" appears to be based on CCO's role as a HINP, rather than a PP. There is a risk that CCO's authority to collect and use the PHI from the Sites to operate the OBSP as a PP, including the sending of breast screening correspondence, is not clear.	Once CCO has implemented Privacy Controls #1 and #2, the Funding Agreements for subsequent fiscal years should specifically reference the data elements that the Sites are to provide to CCO in its capacity as a PP.	Regional Programs	N/A	See response to recommendation #2

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
OBSP Correspondence Phase II: Invitation-Reminders, Recalls, Recall-Reminders and Normal Results	PP	22-Jan-15	Privacy Specialist	Contractual authority for CCO's collection of the breast screening data may not be in place because all of the Funding Agreements and MDSAs have not been signed back to CCO prior to the "go-live" of OBSP Phase II.	The Program must confirm that all of the OBSP 2014/15 Funding Agreements and the MDSAs have been signed back to CCO prior to the go-live of the OBSP Phase II.	Regional Programs	Feb-13-2015	Confirmed by email that CCO has received all 2014/15 Funding Agreements.

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
OBSP Correspondence Phase II: Invitation-Reminders, Recalls, Recall-Reminders and Normal Results	PP	22-Jan-15	Privacy Specialist	Because it is not clear whether the SOPs were in fact amended to decrease the risks identified in the VA, all of those risks are currently not subject to any mitigating controls as agreed to. Furthermore those changes that may have been made to the SOPs have yet to be reviewed by EISO to assess their efficacy in risk mitigation. Finally, even after such changes are made and reviewed by EISO as helping to mitigate some of the risks, the risks will require resolution. It was agreed that the VA risks were to	(i) the SOPs referred to in the OBSP Correspondence Phase I PIA Recommendations power point deck are drafted, reviewed by EISO and confirmed, or amended as required to help mitigate the risks identified in the VA; (ii) once approved by EISO, the amended SOPs are implemented at the Sites; and (iii) as agreed, the outstanding risks identified in the VA are managed in the ICMS redesign.	Business Unit	fiscal 2017	ICMS redesign project is underway and expected to be complete in 2017

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	P E or P P	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
				be included in the ICMS redesign which is targeted to be implemented in the fall of 2015.				

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
OBSP Correspondence Phase II: Invitation-Reminders, Recalls, Recall-Reminders and Normal Results	PP	22-Jan-15	Privacy Specialist	In the absence of having any information about quality assurance (**QA**) measures taken at the Sites to validate client addresses, CCO may well be using inaccurate information if the address logic identifies the ICMS address as the one to be used for Phase II Correspondence. Because all of the Phase II Correspondence, not just the results, contains sensitive PHI even the "privacy breach" rate derived from the sending of the Phase II Correspondence could expose CCO to numerous privacy breaches.	CCO should develop and implement a new SOP to track OBSP Phase II Correspondence Return Rates on the basis of the data source used for the address of the mailing and develop a threshold for return rates by data source beyond which the issue is immediately escalated to the CCO Sr. Manager Provincial Operations and the LPO to determine what steps need to be taken to avoid any (additional) privacy breaches.	Privacy Specialist	Feb-23-2015	Sop 06.10.29: Address Management Return Rate Threshold by Address Source has been approved. The LPO reviewed and approved this SOP. The scope of the older SOP 06.10.29 was updated to include all correspondence, including OBSP correspondence, and has since become part of SOP CC-O-11 *Address Management and Return Rate Threshold*. This SOP requires the monitoring of return rates for the purpose of mitigating a breach and to implement the appropriate process where a breach has been identified.

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
OBSP Correspondence Phase II: Invitation-Reminders, Recalls, Recall-Reminders and Normal Results	PP	22-Jan-15	Privacy Specialist	Women may pose questions and/or make complaints to the CC related to CCO's sending of the Normal Results correspondence. Staff at the CC must be able to accurately respond to these issues in order that women receive an appropriate explanation. If staff cannot do this, there is a risk that women do not understand CCO's authority to collect, use and disclose their PHI without their consent, and escalate their concerns by filing a complaint with the IPC.	(i) CCO should review and, where required, revise all relevant cancer screening FAQs and CC SOPs to ensure that they include information related to the sending by CCO of Phase II correspondence, including results correspondence; (ii) In implementing Privacy Control # 8, CCO shouldensure that the information provided to the CC is consistent with that posted on CCO's website: CSPs and PHI: Questions and Answers for Ontarians as it relates to breast cancer screening; (iii) The LPO must review all new and/or revised SOPs and FAQs developed for Phase II and(iv) CCO CC staff must be trained on allnew and/or	Privacy Specialist (LPO)	Feb-26-2015	The following SOPs and related Q&As have been revised and approved by the LPO, including the review for consistency with CCO's website: - SOP 06.07.04: Fulfillment House (**FH**) Returned Mail Address Management. - SOP 06.07.02: FH Significant Address Correction Management CC training was completed on Feb 26, 2015.

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	P E or P P	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
					revised SOPs and FAQs developed for Phase II.			

OBSP Correspondence Phase II: Invitation-Reminders, Recalls, Recall-Reminders and Normal Results	PP	22-Jan-15	Privacy Specialist	Women may pose questions and or make complaints to the Sites related to CCO's sending of the Normal Results correspondence. Staff at the Sites must be able to accurately respond to these issues in order that women receive an appropriate explanation. If staff cannot do this, there is a risk is that women do not understand CCO's authority to collect, use and disclose their PHI without their consent and escalate their concerns by filing a complaint with the IPC.	(i) CCO should develop communications materials, and/or revise currently existing materials, for the Sites on the sending of Phase II correspondence to ensure that Site staff have the necessary information to respond accurately to women posing questions related to CCO's role and, in particular, CCO's sending of Normal Results correspondence; (ii) In implementing Privacy Control # 9, CCO shouldensure that the information provided to the Sites is consistent with that posted on CCO's website: CSPs and PHI: Questions and Answers for Ontarians as it relates to Breast Cancer Screening; (iii) The LPO must review all new and/or revised Sitecommunications materials developed for Phase II; and (iv) Site staff, including the Site Privacy Officer orindividual	Privacy Specialist (LPO)	Feb-18-2015	The following support materials were reviewed by the LPO and provided to OBSP sites on Jan 12, 2015: - Informational poster to be displayed at sites to inform clients of changes in the way they will receive correspondence as of March 2015 - Key messages to provide RCPs and sites with consistent, main messages related to centralized correspondence, CCO, and privacy - Clients FAQs to aid sites in explaining project-related changes to their clients- Project Summary including a privacy section and privacy-related project FAQs. These materials were reviewed with Regional Correspondence Coordinators during Regional Correspondence Coordinator webinar #2 on Jan 15, 2015. a Privacy Specialist presented the privacy material and has assisted in responding to follow up questions from Regional Correspondence Coordinators and site privacy leads. The

					responsible for privacy matters at the Site, must be trained on all new and/or revised communications materials developed for Phase II.			privacy information was summarized in a document that was reviewed by LPO and provided to QBSP site privacy leads via the RCCS on Jan 16, 2015. As a project indicator (required activity), Regional Correspondence Coordinators reviewed the materials with the privacy lead at each site in their region and confirmed completion to CCO by Feb 18, 2015.

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
OBSP Correspondence Phase II: Invitation-Reminders, Recalls, Recall-Reminders and Normal Results	PP	22-Jan-15	Privacy Specialist	Principle 8.1 of *CCO's Privacy Policy* states that: "CCO makes information about its policies and practices for the collection, use and disclosure of PHI freely available, in paper and electronic form." As previously noted in this Section, women may not completely understand the impact of OBSP Phase I, the elimination of the Existing Form and CCO's centralization of OBSP correspondence until they receive Normal Results correspondence from CCO. CCO's public facing materials on its collection,	CCO should: (i) Review its public facing communications material related to the OBSP and amend them as required to include, at minimum, information related to the fact that CCO, and not the Sites, will now be sending out Normal Results correspondence; and (ii) Include in these materials: A) a reference to the fact that the requirement to complete the existing consent form was eliminated on March 3, 2014; B) that CCO will continue to send Privacy Notices to individuals who have not received one as part of Phase I or the OCSP; and C) that restrictions on the use of OBSP data contained in	Privacy Specialist (LPO)	Mar-02-2015	LPO has reviewed the Correspondence web page updates and confirmed that these requirements are met. The website updates went live March 2, 2015.

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	P E or P P	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
				use and disclosure of PHI for breast screening correspondence, including the sending of normal results, should clearly explain CCO's authority for these activities to avoid the risk of women filing complaints with the IPC.	the Existing Form will be honored.			

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
OBSP	PP	25-Mar-15	Privacy Specialist	In the absence of documented PHI data flows, CCO may not have knowledge of all of the collections, uses and disclosures made of OBSP data. Without having a complete picture of this information (*e.g.,* PHI that is entering and leaving the organization), CCO may well be exposed to privacy risks of which it is unaware and thus cannot take steps to manage.	1) CCO should: i) develop and implement a systematic process for documenting PHI data flows and changes to such data flows; and ii) require all Business Units operating within the OBSP, as well as those using and/or disclosing OBSP data, to record such information. 2) After CCO implements Recommendation #1 by documenting all of the PHI data flows involved in the operation and delivery of the OBSP, as well as those using and/or disclosing OBSP data, it should, in consultation with the LPO: (i) identify any of those data flows that are not assessed in this PIA or been the subject of a previous review	Director, Operations, Cancer Screening, Prevention & Cancer Control	Jan-15-2016	1. OBSP Program will be completing the LPO engagement form every time there is a change in the way OBSP operates and/or data is collected. 2. Based on the information provided in the LPO Engagement form, Privacy will identify if all data flows have been assessed in the existing PIAs, if not an addendum will be conducted to assess data flows not assessed in the OBSP Program/Correspondence PIAs

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	P E or P P	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
					by the LPO; and (ii) ensure that those outstanding privacy risks identified by the LPO are subject to the appropriate privacy assessment.			

OBSP	P P	25-Mar-15	Privacy Specialist	Should CCO identify data elements of non-OBSP clients that fall within the purpose of the OBSP database, there is a privacy risk that these women are not aware that CCO is collecting their PHI for the purposes of a program in which they are not participating.	If CCO identifies data elements of non-OBSP clients that fall within the purpose of the OBSP database, it should: i) specifically identify that it is collecting some PHI related to non-OBSP Clients and why it is reasonably necessary (*i.e.,* the rationale) for it to collect this information for the purposes of the OBSP; ii) communicate with the Sites regarding this information; and iii) develop and make publicly available information related to its collection, use and disclosure of non-OBSP client PHI as identified in detail in Recommendation #22	Director, Operations, Cancer Screening, Prevention & Cancer Control	Jan-15-2016	1. Any new use of non-OBSP data will require the OBSP Program to complete the LPO Engagement form. The LPO Engagement form will be assessed by the Privacy Office to determine authority for use of the data. (Lindsay - Please ensure completion of LPO Engagement form is included in your process).2. OBSP Program to follow existing process to notify sites. Notification will be dependent on the result of assessment conducted by the LPO Office.3. Public Statement will be dependent on the results of the assessment conducted by the LPO.

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
OBSP	PP	25-Mar-15	Privacy Specialist	If OBSP does not identify the location of all of its data holdings (including the numerous linked data sets), as well as the purposes for which is uses each of these data sets, a risk exists that the PHI used for the Program will be retained longer than the periods established in the *CCO Records Retention Policy*. PHI retained longer than is necessary increases CCO's risk because the consequences of a privacy breach are increased when PHI that the agency no longer requires is the subject of unauthorized access, use,	In order to align with CCO's forthcoming *Records Retention Policy*, OBSP should ensure that it has identified all of its data holdings, their location and the purposes for which the PHI is used.	Director, Operations, Cancer Screening, Prevention & Cancer Control	Mar-31-2017	As part of the work conducted by Deloitte, a detailed list of data holdings has been developed. As well, as part of the IPC triennial review, data holdings and the statement of purpose for each of the data holding will be noted.Additionally, the business unit is in the process for hiring a Compliance team that should be in place by March 31, 2015. They will then develop processes to ensure compliance and data quality within CS, including the OBSP. They also will document use and purpose for ICMS.

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	P E or P P	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
				disclosure, modification and/or copying.				

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
OBSP	PP	25-Mar-15	Privacy Specialist	Because there is no systemic formalized approach taken by CCO to address data quality issues related to other (non-address) OBSP data attributes, inaccurate information may be used and/or linked for any of the purposes for which CCO uses the ICMS data as a PP. If this occurs, erroneous decisions could be made related to OBSP Clients and/or on OBSP policy and operational matters.	CCO should implement a Data Quality model similar to that used for OCSP and CCC as soon as possible.	Director, Operations, Cancer Screening, Prevention & Cancer Control	Mar-31-2017	The business unit is in the process for hiring a Compliance team that should be in place by March 31, 2015. They will then develop processes to ensure compliance and data quality within CS including the OBSP.

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
OBSP	PP	25-Mar-15	Privacy Specialist	CCO does not know if PHI is being collected, used, disclosed and/or retained for purposes of the OBSP in accordance with the organization's information security policies, procedures and standards. This lack of knowledge exposes CCO to the risk of a data breach because OBSP PHI may not be managed in accordance with the required security controls.	OBSP should work with EISO to conduct a review and refresh of the OBSP data handling practices to ensure that they satisfy CCO's security controls requirements.	EISO	Dec-01-2015	EISO has participated in ICMS redesign and confident and reviewed architecture document plus TRA will be conducted and satisfied that controls are in place.

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
OBSP	PP	25-Mar-15	Privacy Specialist	Unlike the situation involving the use of non-OBSP client data for screening correspondence, CCO has not identified why it is reasonably necessary to use non-OBSP client data for the Cancer System Quality Index report from which the screening participation rate indicator in Use #2 (NLD)is drawn. In the absence of a reason as to why these rates are calculated based on the inclusion of PHI of women who do not participate in the OBSP, we are not satisfied that it is reasonably necessary for CCO to use this	7) As part of the implementation of Recommendation #2 in the OBSP Correspondence Phase II PIA (documenting uses of non-OBSP client PHI), CCO must (i) identify why the use of this PHI is reasonably necessary to calculate screening participation rates; and (ii) if the OBSPcan demonstrate that information related to women who do not participate in the OBSP is reasonably necessary, why PHI; *i.e.,* individually identifying information, needs to be used.	Director, Operations, Cancer Screening, Prevention & Cancer Control	Sep-30-2016	~~The business unit will assess the requirement for use of this data upon completion of the ICMS redesign project.~~ The non-OBSP data is required to calculate the screening participation rate indicator for the Cancer System Quality Index report to provide a more complete and accurate provincial screening rate.

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
				information for this purpose.				
OBSP	PP	25-Mar-15	Privacy Specialist	In the absence of a demonstrable explanation of the rationale of why the use of non-OBSP client data is reasonably necessary for Use #2(NLD), CCO risks not being in compliance with PHIPA or its *Privacy Policy.*	8) See Recommendation #7. As part of the implementation of Recommendation #2 in the OBSP Correspondence Phase II PIA (documenting uses of non-OBSP client PHI), CCO must identify why the use of this PHI is reasonably necessary to	Director, Operations, Cancer Screening, Prevention & Cancer Control	Sep-30-2016	See recommendation #7

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
					calculate screening participation rates.			
OBSP	PP	25-Mar-15	Privacy Specialist	In the absence of a demonstrable explanation of the rationale of why the use of non-OBSP client data is reasonably necessary for Use #2, CCO may not be in compliance with its representation in ss.2.4 of the MDSA.	9) See Recommendations #7 and #8.	Director, Operations, Cancer Screening, Prevention & Cancer Control	Sep-30-2016	This recommendation will be addressed once the program has concluded its investigation re: use of non-OBSP data as noted in recommendation # 7 above.

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
OBSP	PP	25-Mar-15	Privacy Specialist	The Sr. Research Associate has questioned whether record-level data is necessary for Use #3 (NLD) or whether aggregate data is sufficient. If, in fact, aggregate data is sufficient for this purpose then there is a privacy risk that CCO is using record-level PHI without demonstrating that such use is reasonably necessary.	As noted by the Sr. Research Associate, the OBSP should consult with CCO's Informatics department to determine if the data extract for inclusion in the iPort (MicroStrategy) be produced using aggregate, as opposed to record-level ICMS data and, if so, use only aggregate data for the production of this report.	Director, Operations, Cancer Screening, Prevention & Cancer Control	Sep-30-2016	The business unit to confirm the assertion if aggregate data is sufficient for this purpose or that record-level data is required.
OBSP	PP	25-Mar-15	Privacy Specialist	In the absence of a demonstrable explanation of the rationale of why the use of record-level ICMS data is reasonably necessary for Use #3 (NLD), CCO may not be	As noted by the Sr. Research Associate, the OBSP should consult with CCO's Informatics department to determine if the data extract for inclusion in the iPort (MicroStrategy) be produced using aggregate, as	Director, Operations, Cancer Screening, Prevention & Cancer Control	Sep-30-2016	This recommendation will be addressed once the program has concluded its assessment on the use of aggregate data vs record-level data.

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	P E or P P	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
				in compliance with its representation in ss.2.4 of the MDSA.	opposed to record-level ICMS data and, if so, use only aggregate data for the production of this report.			

OBSP	P P	25-Mar-15	Privacy Specialist	The manner in which CCO currently and an ongoing basis will respond to queries from women and their healthcare providers relating to the woman's screening PHI is unknown. However CCO does not have a formalized and commonly-understood process that follows best practices for privacy controls such as those set out in the *Interval Cancer Review (**ICR**) Request Procedure*, the analogous provisions of *CCO's Privacy Policy* that address access by CCO employees to PHI, or appropriate security safeguards. In these circumstances, there exists a risk of a privacy breach resulting	CCO should: i) review how its responds to such queries; ii) develop a process to ensure that queries are responded to in a manner that follows the applicable provisions of CCO's *ICSP Data Request Procedure* and the *Business Process for Data Requests*; iii) at minimum, include in the process: a. an assessment of what, if any, PHI is necessary to respond to the query; b. who may have access to this PHI; c. from where this PIA may be accessed; d. to whom it may be disclosed; e. how it must be protected while in use; f. the length of time it may be retained outside of its CCO data holding for the purpose of responding to the query; and g. how it must be destroyed when no longer required.	Director, Operations, Cancer Screening, Prevention & Cancer Control	Sep-30-2016	The process for responding to OBSP queries from women and healthcare providers has been integrated with the existing CC procedure for responding to queries for CCC and Cervical Screening Program.The CC has SOPs in place for client and provider authentication before providing the PHI. Additionally, the Screening Program is putting in place a process for responding to queries received via the screening mail box.

				from an unauthorized individual having access to the PHI and/or CCO disclosing it without the requisite authority under PHIPA.	iv) document the processes/procedures to be followed in responding to such queries; v) have the process reviewed and approved by the LPO and the EISO; ensure that CCO staff who are involved in responding to such queries are made aware of the processes/procedures; and vi) communicate the process to the RCP.			

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
OBSP	PP	25-Mar-15	Privacy Specialist	A small risk remains that the option to opt-out of printing cases which may contain PHI will not be used when an invoice is printed such that an outstanding case containing PHI will be printed and a privacy breach will occur as a result of a CCO employee viewing the information for which they have no authorization.	The ability to print off outstanding cases when generating invoices per OBSP should be eliminated from the ICMS functionality.	Director, Operations, Cancer Screening, Prevention & Cancer Control	TBD	The business unit to assess and confirm if this functionality can be turned off in the ICMS. If it cannot be turned off then identify a business solution for this risk.

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
OBSP	PP	25-Mar-15	Privacy Specialist	13) Without identifying the PHI data elements collected by CCO as a PE and used for linkages with ICMS data to create those OBSP reports identified in this PIA that required on an ongoing basis, there is a privacy risk that such PHI will be used by CCO as a PP without the legislative authority to do so.	13) i) E&R should identify all the PHI data elements which it requires for the "Linked Uses" set out in this PIA to which it currently does not have continuing access and provide the list to the LPO;ii) the LPO should work with the E&R to implement the new process to be developed to authorize the use by CCO as a PP of PHI collected as a PE to ensure that the information is available on an ongoing basis for those purposes related to CCO's operation of the OBSP as a PP.	Director, Operations, Cancer Screening, Prevention & Cancer Control	Sep-30-2016	CCO has developed an Internal Data Sharing Policy and Procedure. The Internal Data Sharing Policy/Procedure replaces the need for the agreement between CCO working as a PE and PP.The work conducted by E&R comes under the authority of PE and per the process any new data sharing for analysis is governed by the *Data Sharing Policy/Procedure.*

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
OBSP	PP	25-Mar-15	Privacy Specialist	The lack of information related to who has access to the crosswalk table containing PHI and the Case Set number, where, under what controls, if any, and the length of time for which the table is retained, coupled with the fact that neither EISO nor the LPO has appeared to have reviewed and approved the management of this information potentially poses several risks to CCO because the PHI may be exposed to unauthorized access, retained under circumstances for which there	CCO should: i) have Policy Operations prepare and provide to EISO and the LPO a detailed description of the manner in which the crosswalk table is managed, including who has access to it, where and under what circumstances it is retained and for how long and the manner in which it is destroyed after it is no longer required for the ICR; ii) engage EISO and the LPO to review the description prepared by Policy Operations to identify any privacy and/or security risks; and iii) have EISO and the KPO work with Policy Operations to manage any identified risks.	Director, Operations, Cancer Screening, Prevention & Cancer Control	Mar-31-2017	At the time of this PIA, the OBSP team created crosswalk tables for the purpose of supporting the Interval Cancer Review. The OBSP business unit has provided the Privacy team with information on the crosswalk table, including the type of PHI included in the table, who has access to it, as well as the purpose for which the information is being used. Currently, the Interval Cancer Review work is on hold and thus, no new crosswalk tables are created or used by the OBSP program. PHI that was retained in previously created crosswalk tables is being securely destroyed. EISO has been consulted.

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	P E or P P	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
				are no security controls and for longer than is necessary for the conduct of the ICR. These risks relate to CCO's non-compliance with PHIPA, as well as its own policies and procedures				

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
OBSP	PP	25-Mar-15	Privacy Specialist	There is a long period of time before the expiration of the retention period for the PHI collected by CCO to produce the ICR reports; CCO staff may change and corporate memory of the intention to work with EISO to ensure secure destruction of the PHI may be lost. Unless CCO develops and maintains clear procedures for the engagement of EISO in this process, a risk exists that the PHI will be retained outside of the retention period or destroyed in a manner that is not secure.	CCO should develop, document and maintain clear procedures for the engagement of EISO upon the expiration of the retention period for the PHI collected by CCO to develop the ICR reports.	Director, Operations, Cancer Screening, Prevention & Cancer Control	TBD	Program to develop process on how to engage the EISO

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	P E or P P	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
OBSP	P P	25-Mar-15	Privacy Specialist	See Outstanding Privacy Risk #13	See Recommendation #13	See response to risk #13 above	Sep 30, 2016	See response to risk #13 above
OBSP	P P	25-Mar-15	Privacy Specialist	The PHI in the H: drive may be subject to a privacy breach resulting from unauthorized access to the information because CCO staff access privileges are not immediately revoked when no longer required.	We understand that CCO is currently investigating the acquisition of new software (a Human Capital Management System – HCMS) that would link H:/drive access privileges to CCO's human resources records such that when an individual leaves the organization their access privileges would be immediately terminated. This acquisition should proceed as soon as possible to manage the risk of unauthorized access to the PHI stored on this drive.	EISO	Apr-01-2016	~~CCO is in the process of awarding the contract. As part of the implementation of the software, there will be a business process review at the same time.~~ The Human Capital Management System (HCMS) has been procured and implemented. The HCMS has an integration with CCO's corporate network directory (Active Directory), therefore supporting automated provisioning (add), de-provisioning (remove), and disablement of user accounts based on employment status.

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
OBSP	PP	25-Mar-15	Privacy Specialist	CCO appears to not be in compliance with either the IPC Manual or its own *Privacy Policy* as it does not have a *Retention Policy* that establishes the time period for the retention of PHI stored in the H:/drive.	Once CCO has completed its *PHI Retention Policy*, it should ensure that it develops and make all staff aware of the processes and procedures to implement the *Retention Policy* such that retention periods for each category of PHI identified in the policy may be tracked and the PHI destroyed in a secure manner once its retention period has expired.	LPO	Oct-01-2016	Record Retention schedule for records have been developed by RIM. All staff is required to undergo RIM training by October 30th. Each business unit is expected to follow the record retention schedule developed by RIM
OBSP	PP	25-Mar-15	Privacy Specialist	A privacy breach involving PHI stored in the H:/drive may be of a much larger magnitude because of the authorized access etc. to PHI retained by CCO in the absence of an ongoing business purpose for	Once CCO has completed its *PHI Retention Policy*, it should ensure that it develops and make all staff aware of the processes and procedures to implement the *Retention Policy* such that retention periods for each category of PHI identified in the policy may be	LPO	Oct-01-2016	Record Retention schedule for records have been developed by RIM. All staff is required to undergo RIM training by October 30th. Each business unit is expected to follow the record retention schedule developed by RIM

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
				continued retention.	tracked and the PHI destroyed in a secure manner once its retention period has expired.			
OBSP	PP	25-Mar-15	Privacy Specialist	In using PHI (*i.e.,* identifying information) of OBSP Clients and non-OBSP Clients for Uses #1, 2 and 3 (NLD) and Uses 1, 2, 3, 4 and 5 (LD), CCO is using PHI in circumstances in which de-identified information will serve the purpose. Accordingly, this use of PHI is inconsistent with CCO's statement	CCO should consider de-identifying the PHI of OBSP Clients and non-OBSP Clients where the purposes for the use of ICMS data does not require that the identity of a specific woman be known (*i.e.,* for Uses #1, 2 and 3 (NLD) and Uses 1, 2, 3, 4 and 5 (LD)).	Director, Operations, Cancer Screening, Prevention & Cancer Control	TBD	Director, Operations, Cancer Screening, Prevention & Cancer Controlto confirm with Program staff if non identified data is sufficient. If so, then implement this recommendation.

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
				in its *Privacy Policy*. We note that this is a risk not specific to this use of OBSP data.				
OBSP	PP	25-Mar-15	Anita Fineberg	If CCO may use de-identified ICMS data for a number of purposes as described in this PIA, it may not be in compliance with its representation in ss.2.4 of the MDSA.	CCO should consider de-identifying the PHI of OBSP Clients and non-OBSP Clients where the purposes for the use of ICMS data does not require that the identity of a specific woman be known (*i.e.,* for Uses #1, 2 and 3 (NLD) and Uses 1, 2, 3, 4 and 5 (LD)).	Director, Operations, Cancer Screening, Prevention & Cancer Control	TBD	See above

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
OBSP	PP	25-Mar-15	Anita Fineberg	Non-OBSP Clients may not be aware of and, if aware, understand the rationale for the provision of their PHI to CCO by the Sites and/or the purposes for which CCO uses and discloses their PHI. As a result of this lack of understanding, they may question the Site and/or file a complaint with the IPC.	Once it has implemented Recommendations 7 and 8 such that it has documented the PHI of non-OBSP Clients that it collects and uses and the purposes therefore, CCO should: i) work with the Sites to prepare some FAQs to be provided to non-OBSP Clients so that they are made aware of and understand the reason why some of their PHI is provided to CCO and the purposes for which their information is subsequently used and disclosed; ii) review the publicly available information on its website and its draft SOPs to be provided to the Sites to ensure that all of the information (*e.g.,* the Statement of Information Practices, Breast	Director, Operations, Cancer Screening, Prevention & Cancer Control	Mar-31-2017	Confirm if 7 & 8 is true. If so, then we comply with this recommendation

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	P E or P P	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
					Cancer Screening FAQs, draft SOP 5.0) accurately represent the ICMS data that CCO collects from the Sites.			

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
OBSP	PP	25-Mar-15	Anita Fineberg	CCO has not communicated a consistent message to the Sites with respect to the manner in which they must securely transfer PHI to all entities for all purposes related to the operation of the OBSP. Because the standards appear to vary depending on the nature of the PHI and the circumstances in which it is being disclosed, there is a risk that the Sites may not follow the standards set out in the IPC Fact Sheet which represent best practices. If these are not applied a privacy breach could result.	CCO must develop and communicate to the OBSP Sites a common standard and requirement that all PHI must be transferred in compliance with the IPC Fact Sheet – in the Funding Agreements, the MDSA and the SOPs.	Director, Operations, Cancer Screening, Prevention & Cancer Control and EISO	Mar-31-2017	OBSP site are HICs and thus should have in place practices for secure information of PHI. In addition to those, OBSP in consultation with LPO can draft guidelines for secure transmission and distribute it to sites. This will done as part of the OBSP SOP update for fiscal 2016/2017. Funding agreement and MDSA are high-level documents and will not be updated to include this recommendation.

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
OBSP	PP	25-Mar-15	Privacy Specialist	Subsection 5.5 of the SOPs and specifically ss.5.5.1 only apply to the Process for transferring Client Records to and from OBSP Sites when an OBSP Client wishes to have her records transferred from a Site at which she was previously assessed to a New Site. Because of the limited application of this SOP, it is possible that the Sites do not understand that they should consult the IPC Fact Sheet when determining the transfer method for any and all client PHI to any entity for any purposes (*e.g.,*	CCO must develop and communicate to the OBSP Sites a common standard and requirement that all PHI must be transferred in compliance with the IPC Fact Sheet – in the Funding Agreements, the MDSA and the SOPs.	Director, Operations, Cancer Screening, Prevention & Cancer Control and EISO	Mar-31-2017	See the response to the recommendation above

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	P E or P P	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
				to CCO for the ICR). A privacy breach could occur if a Site does not consult the Fact Sheet and thus does not use a secure method to transfer client PHI in these circumstances.				

OBSP	P P	25-Mar-15	Privacy Specialist	The High Risk and Genetic Clinic Agreements do not establish the PHIPA authority of the Genetic Clinics to disclose the genetic assessment data to the High Risk Screening Centres for the purposes of disclosing it to CCO. The absence of this contractual authority exposes CCO to the risk of requiring the Genetic Clinics to provide the genetic assessment data to the High Risk Centres for ultimate provision to CCO without the Genetic Clinics having the legal authority under PHIPA to disclose the PHI to the High Risk Centre in the first place.	CCO should investigate and implement a contractual and/or technical solution that would manage the current risk of the lack of legislative and contractual authority of the Genetic Clinics to disclose to the High Risk Centres, and the High Risk Centres to collect the genetic assessment data solely for the purpose of the provision of this PHI to CCO by the Genetic Clinics.	Director, Operations, Cancer Screening, Prevention & Cancer Control	Q4 2015/2016	As per the Schedule C of the 'High Risk Genetic Assessment Funding agreement', the data is only shared and entered in the ICMS once the patient has consented. As well, it is assumed that Genetic Clinics as a separate HIC would determine their own PHIPA authority for disclosing the information to CCO and thus there is no need to reflect this in the agreement.As well each Genetic Assessment Clinic has executed an MDSA which notes that CCO is authorized to collect PHI for the purpose of PP. Section 4.2 of the MDSA warrants from the HIC that they are in compliance with PHIPA and that they have the authority under PHIPA to disclose PHI to CCO.

OBSP	P P	25-Mar-15	Privacy Specialist	The continued use of the Genetic Release Form may well be confusing to women, does not appear to have been followed in practice and is inconsistent with the approach taken by CCO with its elimination of the Existing Form and reliance on its statutory and contractual authority to collect PHI related to OBSP screening. The continued use of the form exposes CCO to a privacy risk if women determine that their request to not share their assessment data with CCO was not honoured and file a complaint with the IPC.	CCO should: (i) discontinue the use of the Genetic Release Form at the Genetic Clinics;(ii) amend its Statement of Information Practices to include "genetic assessment information" as one of the examples given of the type of cancer data collected by CCO in response to the question "What types of PHI does CCO collect?" (iii) as was the case with the elimination of the consent form for the Average Risk sites, ensure that the High Risk Centres develop a process to manage and "grandfather" the "no's" such that the genetics assessment information of women who have not provided their consent to share genetic assessment information with CCO is not entered into ICMS by the Centre and thus is not only not available to CCO but not available to other Sites as well;(iv) provide	Director, Operations, Cancer Screening, Prevention & Cancer Control	Mar-31-2017	Program to explore what will be required to implement the recommendation. The forms will be targeted for removal by end of fiscal 2016/2017

					communications materials to the Genetic Clinics to explain CCO's authority to collect the genetic assessment information without requiring the consent of the woman to do so; and(v) amend Section 3.0 (High Risk Screening) of the SOPs to reflect the elimination of the Genetic Release Form.(vi) if it still wishes to collect the information on women who have been screened at genetics clinics who were not found to be eligible for the OBSP High Risk screening program (and are younger than 50 such that they are not eligible for the program and thus are non-OBSP clients, as is the case with the other PHI CCO collects for non-OBSP clients, identify why it is reasonably necessary for it to collect this information as a PP and include this explanation in response to the			

					question “What types of PHI does CCO collect?”			

OBSP	P P	25-Mar-15	Privacy Specialist	The Genetic Assessment Agreement does include a representation and warranty by the clinic that it is in compliance with its obligations as a HIC under PHIPA. However, by requiring the Genetic Clinics to provide the Genetic Assessment Results Form to a High Risk Centre that is part of a woman's "circle of care", it may appear that CCO has not considered the obligation of the clinics under PHIPA to afford the woman the opportunity to withhold or withdraw her consent to the provision of her PHI to the Centre for care and treatment purposes. There is a risk that CCO may appear to be placing the	CCO should amend the Genetic Assessment Agreement to make it clear that its requirement to provide the Genetics Result Form to the High Risk Centre for provision to CCO, does not release the Genetic Clinics from their obligations under PHIPA to ensure that they have the authority to disclose PHI with the High Risk Centre for other purposes such as patient care and treatment.	Director, Operations, Cancer Screening, Prevention & Cancer Control and Legal	Q4 2015/2016	As per the Schedule C of the 'High Risk Genetic Assessment Funding agreement', the data is only shared and entered in the ICMS once the patient has consented. As well, it is assumed that Genetic Clinics as a separate HIC would determine their own PHIPA authority for disclosing the information to CCO and thus there is no need to reflect this in the agreement. As well each Genetic Assessment Clinic has executed an MDSA which notes that CCO is authorized to collect PHI for the purpose of PP. Section 4.2 of the MDSA warrants from the HIC that they are in compliance with PHIPA and that they have the authority under PHIPA to disclose PHI to CCO.

				Genetic Clinics in non-compliance with PHIPA.				

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
OBSP	PP	25-Mar-15	Privacy Specialist	Because it appears that the details of the operation of the OBSP Data Quality Accuracy and Completeness Checks have yet been determined, there is a privacy risk that PHI will not be collected, used and/or disclosed by CCO in accordance with PHIPA and CCO policy in the conduct of the data quality checks.	CCO should ensure that the LPO reviews the proposed sharing of OBSP data related to high risk women before the operation of the OBSP Data Quality Accuracy and Completeness Checks resume.	Director, Operations, Cancer Screening, Prevention & Cancer Control	March 31,2017	The OBSP program is in the process of hiring a compliance team to implement data quality and compliance processes for OBSP. The target is for the data quality and compliance activity to occur over the fiscal year 2016/2017. Engagement of the LPO will be built into Compliance team processes.

OBSP	P P	25-Mar-15	Privacy Specialist	The Funding Agreements with the High Risk Centres and the OBSP Sites that provide breast assessment services do not establish their PHIPA authority to collect assessment data from non-OBSP sites and provide it to CCO, or to the RCPs for subsequent provision to CCO for the purposes of the OBSP. The absence of this contractual authority exposes CCO to the risk of requiring these Sites to collect and disclose this PHI to CCO in the absence of any legislative authority to do so.	CCO should investigate and implement a contractual and/or technical solution that would manage the current risk of the lack of legislative and contractual authority of the High Risk Centres and OBSP Sites that provide breast assessment services to collect breast assessment data from non-OBSP sites. A similar solution should also be investigated and implemented to ensure that whatever entity of the RCP receives the breast assessment data from the High Screening Centres has the requisite authority.	Director, Operations, Cancer Screening, Prevention & Cancer Control & Legal	TBD	As per the Schedule C of the 'High Risk Genetic Assessment Funding agreement', the data is only shared and entered in the ICMS once the patient has consented. As well, it is assumed that Genetic Clinics as a separate HIC would determine their own PHIPA authority for disclosing the information to CCO and thus there is no need to reflect this in the agreement. As well each Genetic Assessment Clinic has executed an MDSA which notes that CCO is authorized to collect PHI for the purpose of PP. Section 4.2 of the MDSA warrants from the HIC that they are in compliance with PHIPA and that they have the authority under PHIPA to disclose PHI to CCO.

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
OBSP	PP	25-Mar-15	Privacy Specialist	The same privacy risk as identified in the ORN PIA Addendum exists in CCO's operation of the OBSP as both a HINP and a PP. That is, the variations between the *HINP Privacy Policy* and *Privacy Breach Management Procedure*, make it difficult for CCO staff to know what procedure to follow in the event of a breach of OBSP client PHI. This is exacerbated by the fact that CCO's obligation as set out in ss. 3.3(i) of the MDSA is written at an extremely high level.	CCO must review the *HINP Privacy Policy* and the *Privacy Breach Management Procedure* to clarify the procedures to be followed by CCO staff in the event of a privacy breach of ICMS data that CCO manages in its dual role under PHIPA as a PP and a HINP.	Director, Operations, Cancer Screening, Prevention & Cancer Control and Privacy Specialist	Jun-30-2016	LPO is undertaking a review of the CCO PBM program. This recommendation will be addressed as part of this review.

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
OBSP	PP	25-Mar-15	Privacy Specialist	In its role as a HINP, CCO has established the three-point HIC (Site) Privacy Officer contact as described above. Without a contact list of all of these individuals CCO cannot fulfill its responsibilities as set out in the *HINP Privacy Policy* in a timely manner.	CCO must: i) develop a list of the Site Privacy Officers and their contact information at each of the Sites; and ii) ensure that the contact list of the Site Privacy Officers is available to the LPO for its use should notification of these individuals be required in the event of a privacy breach relating to the PHI provided to CCO via ICMS by the Sites.	Director, Operations, Cancer Screening, Prevention & Cancer Control	Mar-01-2016	As part of Release 2.0 and 2.1, the business will be collecting and maintaining list of privacy contact for all OBSP sites. As well, privacy breach management will include reference to the list maintained by the business unit.
OBSP	PP	25-Mar-15	Privacy Specialist	32) There is no documentation related to the OBSP which describes the services provided to the Sites by CCO operating the OBSP as a HINP. This lack of documentation is a privacy risk as CCO is not in compliance with the Regulation,	29) CCO should prepare a “plain language” statement of the services it provides to the Sites, including a general statement of the safeguards in place to protect against unauthorized use and disclosure, and to protect the integrity of the information and provide this statement to all	LPO	Jun-30-2016	LPO will draft the plain language description

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
				its *HINP Privacy Policy* or the terms of the OBSP Funding Agreements and the MDSAMDSA.	Sites to make it publicly available to clients whose PHI is provided to CCO through entry into the ICMS.			
OBSP	PP	25-Mar-15	Privacy Specialist	Neither the References nor the Appendix to the *HINP Privacy Policy* include a reference to the ICMS as the information system utilized by OBSP in its delivery of IT services. This is to be expected given that CCO has not "formally" recognized its role as a HINP in the delivery of this program. However, the	CCO must: i) include a reference to the License and HINP Agreement (see Recommendation # 35), this PIA and, once completed, the TRA(s) (See Recommendation #33) conducted on OBSP and ICMS in the list of References to the *HINP Privacy Policy*; and ii) draft a description of the ICMS to be included in *Appendix "A"* to the *HINP Privacy Policy.*	LPO	Oct-30-2015	As part of the review of the HINP policy, explicit references to various HINP programs are being removed from the Policy. Hence, this risk is no longer applicable

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
				absence of such information means that CCO is not completely open with respect to the information systems it provides to HICs and for which it is subject to additional privacy and security requirements as a HINP.				
OBSP	PP	25-Mar-15	Privacy Specialist	See Privacy Risk #32	See Recommendation #29	See response to Recommendation 29	Fiscal 14/15	See response to Recommendation 29
OBSP	PP	25-Mar-15	Privacy Specialist	CCO risks being in non-compliance with the Regulation if it does not provide the OBSP Sites with a written copy of the results of this PIA as it relates to the services	CCO must provide the Sites with written copy of the results of this PIA as it relates to the services provided by CCO as a HINP.	LPO	Jun-30-2016	The PIA is scheduled to be completed by May 2016. The PIA summary will be made available to HIC upon request.

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
				provided by CCO as a HINP.				
OBSP	PP	25-Mar-15	Privacy Specialist	CCO risks being in non-compliance with the Regulation as well as its *Privacy Policy* because it has not conducted a TRA or other security assessment on ICMS. Accordingly, CCO may be unaware of security risks to which the PHI transmitted to CCO by the Sites through ICMS may be exposed. These in turn expose CCO to the risk of a privacy breach resulting from unsecure	CCO is in the process of the ICMS redesign, which is anticipated to be completed by the fall of 2015. Once the redesign is complete, CCO must complete a TRA or other security assessment on the redesign and provide the OBSP Sites with a written copy of the results of the TRA or other security analysis conducted on ICMS as a result of the implementation of this Recommendation.	EISO	Dec-01-2016	A TRA was completed on ICMS and was finalized in January 2016.

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
				security practices.				
OBSP	PP	25-Mar-15	Privacy Specialist	A risk exists that the third party retained by CCO to develop and implement the ICMS consent management capability will not be required to comply with the restrictions and conditions of ss.6(3) of the Regulation, thus exposing CCO to the risk of non-compliance.	CCO must ensure that, should it proceed to procure the services of a third party to develop and implement consent management capability into ICMS and/or assist the agency in any way to provide its services as a HINP to the Sites, it enters into an agreement with the third party that satisfies the requirements of	LPO	Mar-01-2016	The vendor will be onboarded in Nov 2015. The requirement re: agreement is a standard clause in all agreements. The agreement with vendor has been executed.

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
					ss.6(3)6 of the Regulation.			
OBSP	PP	25-Mar-15	Privacy Specialist	CCO risks being in non-compliance with the Regulation as well as its *HINP Privacy Policy* because it has not entered into a written agreement with the Sites concerning the services it provides as a HINP through the operation of the ICMS.	CCO must enter into a written agreement with each Site concerning the services it provides as HINP through the operation of the ICMS. In order to comply with ss.6(3)7 of the Regulation, the agreement must: i) describe the services CCO is required to provide to the Sites; ii) describe the technical, administrative and physical safeguards relating to the confidentiality and security of the	Group Manager, Operations, Cancer Screening - Operations	Oct-01-2015	The HINP agreement has been sent all OBSP sites with the instructions to return the signed agreement by October 16, 2015.

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	P E or P P	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
					OBSP data; and iii) requires CCO to comply with PHIPA and the Regulation.			

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
OBSP	PP	25-Mar-15	Privacy Specialist	At present, given the design approach taken to ICMS, there are minimal controls on ICMS users and the PHI to which they have access. This exposes CCO to the risk that unauthorized individuals will access PHI in the system and/or authorized users will use the PHI for unauthorized purposes.	CCO should adopt the approach taken by the ORN in the development of a HINP and License Agreement to address the appropriate use of and access to PHI in ICMS as required by the new RBAC. CCO must ensure that any provisions in this agreement are consistent with and/or incorporate by reference, the relevant provisions of the OBSP Funding Agreement and those in the MDSA related to PHI.	LPO	May-01-2015	Data segregation within ICMS combined with License/HINP agreement will address this recommendation.This is complete as RBAC and various roles have been created in the ICMS. The roles provide different functionality to different users. As well, every site will be signing the HINP License agreement.

OBSP	P P	25-Mar-15	Privacy Specialist	The Sites do not provide women with a notice explaining the purposes for this sharing or that they may decide to opt-out or withdraw their consent to such sharing. There is no process implemented at the Sites that operationalizes the opt-out process or allows a woman to subsequently "opt-back in" if she so chooses; nor is there any technical capability in ICMS to "flag" or "block" access by a Site to PHI which a woman has directed not be shared and "lift the flag" if the woman later changes her mind. The risk exists that CCO has not acted on its due diligence as a HINP in that it is aware of but has acceded to the Sites not complying with PHIPA in their sharing of PHI.	CCO should take the following steps: i) the ICMS redesign should incorporate the following features of "consent management": • A decision needs to first be made with respect to the level of granularity that will be afforded to patients related to their exercise of opt-out rights; • ICMS must be capable of identifying the PHI of a woman who has exercised her right to opt-out; • ICMS must be capable of blocking access by another Site/individual to the PHI (depending on the granularity) which a woman has decided she does not want to share in those circumstances; • ICMS must be able to provide a Site that searches for PHI which is blocked with a notification that advises the Site that such information is not available; and • ICMS must be able to "lift" the "block" either in whole or in	LPO	Nov-01-2016	This risk will be mitigated with the ICMS HINP consent project. The BRD for consent management has been approved. Vendor will be onboarded in fall 2015 to add consent functionality to the ICMS. The consent management facility is expected to go live in September 2016.

					part should a woman decide to change her mind with respect to sharing PHI with other Sites; ii) CCO must work with the Sites to draft, develop and implement:• A notice that sets out the purposes for which the Sites share PHI and the nature of the PHI that is shared for these purposes; • The notice must make it clear that the opt-out to sharing applies only to PHI shared between the Sites (*i.e.,* that it does not apply to PHI provided to CCO it is capacity as a PP for which the Sites do not require the consent of a woman to provide it to CCO, nor CCO to collect it); • An administrative process by which the Sites can capture a woman's opt-out and her subsequent "opt back in" should she change her mind; • A process by which the opt-out captured by the Sites is entered by			

					the Sites into ICMS when the Site inputs the woman's PHI and a process whereby the Sites may "reverse" the opt-out in ICMS should the woman subsequently change her mind.			

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
OBSP	PP	25-Mar-15	Privacy Specialist	ICMS is configured as an open model through which Sites have access to almost all PHI of women at other Sites for any purposes. In the context of CCO's operation of the OBSP as a HINP, the sharing of PHI by the Sites must be limited to that which is required "for the purpose of providing health care or assisting in the provision of health care" in order that the information be shared on the basis of "assumed implied consent". As ICMS is currently configured, there is a risk that not only will the Sites have	CCO should work with the Sites to identify those data elements entered by the Sites into ICMS that need to be shared by the Sites "for the purpose of providing health care or assisting in the provision of health care". As is the case with the CCO "death data" and the non-OBSP client data, the Sites should not be able to access any other PHI in ICMS.	Director, Operations, Cancer Screening, Prevention & Cancer Control	TBD	The HINP consent project will allow patients to block certain pieces of the information within ICMS. ICMS acts as both HINP and ESP.

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	P E or P P	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
				access to PHI that they do not require for the care and treatment of a patient but also use it for a purpose for which it is not required.				

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
OBSP	PP	25-Mar-15	Privacy Specialist	42) The current system of functional user permissions to establish access to PHI in ICMS fails to meet industry and security best practices in that it does not address the principle of the limitation of user access to that PHI which is required in order to fulfill their employment responsibilities. Accordingly, there is a risk of privacy breaches in that users at Sites who do not require access to perform their job (*e.g.,* a booking clerk having access to detailed MRI information) can access information.	39) ICMS users need to be associated with roles/permissions through the strong authorization mechanisms such as RBAC to control access to system functions and data. These ICMS User Roles and Permissions are currently in development. Prior to these being finalized, CCO should: i) confirm the roles and permissions with the Sites to ensure that those individuals who require access to specific PHI in order to perform their job have such access rights; and those who do not require such access do not have such rights; and ii) confirm this assessment with the LPO.	Director, Operations, Cancer Screening, Prevention & Cancer Control	The ICMS redesign project is on hold until Fall, 2017.	ICMS redesign is introducing RBAC. Role types have been established with the ICMS redesign.

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
OBSP	PP	25-Mar-15	Privacy Specialist	43) By requiring the RCP at an RCC to conduct the MRT Imaging reviews based on the current process and agreements, CCO appears to have prescribed a QA activity that requires the collection, use and disclosure of PHI that is not authorized by PHIPA. This poses a risk to CCO because it is providing HINP services to permit both the RCCs and the Sites as HICs to collect, use and disclose PHI for purposes for which it is not authorized in the absence of patient consent.	40) The Sites and the Regional Reviewers would have the authority under PHIPA to collect, use and disclose PHI as required for MRT Imaging Reviews if the RCC were to engage in these data management activities as the PHIPA agent of CCO. Accordingly, the MDSA should be amended to explicitly identify that the RCC is functioning in this role for the purposes of participation in certain projects noted in the DSA.	LPO	Fiscal 17/18	The funding agreement between CCO and the Regional Cancer Centres (RCCs) will be updated to clarify that the RCCs are acting on behalf of CCO when completing the MRT imaging reviews.
OBSP	PP	25-Mar-15	Privacy Specialist	See Privacy Risk #42	See Recommendation #39	Director, Operations,	The ICMS redesign project	Role-based access controls will be

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	P E or P P	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
				The access to the PHI in ICMS by individuals in these roles should be limited to that which is required to perform their employment responsibilities. The current system of functional user permissions to establish access to PHI in ICMS fails to meet industry and security best practices in that it does not address the principle of the limitation of user access to that PHI which is required in order to fulfill their employment responsibilities. Accordingly, there is a risk of privacy breaches in that users at	CCO should work with the Sites to identify those data elements entered by the Sites into ICMS that need to be shared by the Sites "for the purpose of providing health care or assisting in the provision of health care".	Cancer Screening, Prevention & Cancer Control	is on hold until Fall, 2017.	implemented as part of the ICMS redesign project.

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
				Sites who do not require access to perform their job (e.g. a booking clerk having access to detailed MRI information) can access information.				
OBSP	PP	25-Mar-15	Privacy Specialist	The following data quality activities are generally performed by individuals employed by the RCC; • Data Entry and Quality Management, • Assessment and Case Closure Audits, • Monitoring of Performance Indicators for Breast Cancer Assessment Wait Times and	The RCCs would have the authority under PHIPA to collect, use and disclose PHI as required for the data quality activities if the RCC were to engage in these activities as the PHIPA agent of CCO. Accordingly, the agreement between CCO and the RCCs should be amended to explicitly identify that the RCC is functioning in this role as CCO's agent.	Director, Operations, Cancer Screening, Prevention & Cancer Control	Fiscal 17/18	The funding agreement between CCO and the Regional Cancer Centres (RCCs) will be updated to clarify that the RCCs are acting on behalf of CCO when completing the data quality activities.

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
				• Escalation to Facilitate the ICR Process				
OBSP	PP	25-Mar-15	Privacy Specialist	In the absence of information describing the PHI data flows originating from access to ICMS it is not possible to determine if the collections, uses and disclosures of the PHI are authorized by PHIPA. CCO could thus be exposed to privacy risks in its operation of ICMS as a HINP of which it is unaware because of the inability to conduct a comprehensive due diligence review of these activities.	CCO should: i) obtain the information required to assess the PHI data flows originating from ICMS and collected, used and disclosed by the RCPs in conducting its activities, including those related to data entry and quality management, assessment and case closure audits, monitoring of performance indicators for breast cancer assessment wait times and escalation to facilitate the ICR process; and ii) conduct a comprehensive PIA on these activities.	Legal & Privacy Office	The ICMS redesign project is currently on hold until Fall, 2017.	A PIA has been drafted for the ICMS redesign project. This PIA outlines the PHI data flows originating from ICMS. This PIA is expected to be finalized prior to the implementation of the ICMS redesign project.
SCT Program PIA Addendum	PE	15-Nov-13	Privacy Specialist	There were no privacy risks	N/A	N/A	N/A	N/A

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
				identified in the PIA addendum				
MRI Process Improvement Project (PIP), Phase III - PIA Addendum	PE	13-Jan-14	Privacy Specialist	There were no privacy risks identified in the PIA addendum	N/A	N/A	N/A	N/A
WTIS Release 17 & 18 - PIA Addendum	PE	28-Oct-14	Privacy Specialist	There were no privacy risks identified in the PIA addendum	N/A	N/A	N/A	N/A
SSO-IS - Interventional Radiology	PE	8-Sep-16	Privacy Specialist	There is a risk of CCO performing an unauthorized use under PHIPA if the interventional radiology PHI is linked and used with other CCO data holdings without the appropriate authority under PHIPA to do so.	The SSO business team will engage the LPO to review any anticipated linkages of interventional radiology PHI with other CCO data holdings, prior to the linkages occurring.	Group Manager, Specialized Services Oversight, Clinical Engagement Programs	Sept-8-2-2016	As per recommendation, the business unit will engage LPO through the LPER prior to any linkages. Group Manager, Specialized Services Oversight, Clinical Engagement Programs has reminded the business team through their team meeting

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
eCTAS	PE	29-Aug-16	Privacy Specialist	Patients or their authorized Substitute Decision-Maker (**SDMs**) have the legal right under PHIPA to restrict HICs from sharing their PHI for the purpose of providing or assisting in the provision of health care. The express instruction of a patient to his or her healthcare provider not to use or disclose his or her PHI by either expressly withdrawing or withholding consent is commonly referred to as the "lock box" or a consent directive. Given the circumstances, consent directives could arise during an	Project team will develop a procedure to give effect to consent directives. LPO should review the proposed procedure developed by the project team to ensure that it complies with PHIPA.	Business Unit	**Feb 28, 2017**	A patient consent withdrawal process will be available through the eCTAS application and may be accessed any time during the ED visit. The withdrawal of consent will prevent the Patient PHI from being further accessed at the ED that created the record, or shared across other participating EDs. Consent is withdrawn during record creation by selecting a checkbox.

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	P E or P P	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
				ED visit or be communicated afterward. Functionality to implement a consent directive has not been incorporated into the eCTAS system. As a result, PHI could be used or disclosed contrary to a patient's express directions, in breach of PHIPA.				

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
eCTAS	PE	29-Aug-16	Privacy Specialist	CCO has not developed a plain language description of the HINP-related services that meets PHIPA's HINP requirements. Such a description must be provided to participating hospitals and made available to the public.	A plain language description of the HINP-related services that meets PHIPA's HINP requirements must be provided to participating hospitals and made available to the public. The project team should work with LPO to finalize a plain language description of the HINP-related services that meets PHIPA's HINP requirements, and provide it to participating hospitals and make it available to the public.	Business Unit	Feb 28, 2017	CCO drafted a plain language description of the HINP-related services that meets PHIPA's HINP requirements. This description will be provided to participating hospitals and made available to the public through CCO's public website

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
eCTAS	PE	29-Aug-16	Privacy Specialist	It is unclear how CCO will make available, at the request of a participating hospital, access to information about the handling of patient triage record summaries during the 10 day period following their upload to the eCTAS system – specifically: (i) who has accessed that hospital's patient triage record summaries (including the time and date of access); (ii) who initiated a disclosure of that hospital's patient triage record summaries to another participating hospital (*e.g.,* the user at the	The project team should determine what access and disclosure information can be tracked about a given patient triage record summary during the 10 day period following its upload by a participating hospital. The project team should work with LPO to develop a procedure under which a participating hospital can request that CCO provide information about the access and disclosure of that hospital's patient triage record summaries, and for CCO to provide sufficient responses to those requests. Note, this procedure will only apply during the 10 days following the upload of a given patient triage record summary. Also, the	Business Unit	Feb 28, 2017	The auditing requirements will be included in the final product. A specific process for managing requests from hospitals will be developed.

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	P E or P P	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
				hospital that conducted the search for recent ED visits); (iii) what hospital received a copy of the patient triage record summaries; and (iv) the date and time of the disclosure.	project team should consult with EISO to determine whether the eCTAS database will fall within the scope of LMAS, as this may assist to address the privacy risk.			

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
eCTAS	PE	29-Aug-16	Privacy Specialist	CCO has not yet conducted a TRA, or compiled related information about security and integrity of PHI, and impacts on privacy, that meets PHIPA's HINP requirements. This PIA has not been prepared with reference to a TRA.	EISO to conduct a TRA of eCTAS. The project team should work with EISO to ensure that any EISO recommendations are implemented and that the analysis and related information is provided to participating hospitals.	Business Unit	Feb 28, 2017	A Security assessment has been conducted by CCO, Accenture and a third party vendor to meet PHIPA's HINP requirements. The summary of the TRA will be made available to hospitals.
eCTAS	PE	29-Aug-16	Privacy Specialist	Given the legislative gaps, there is some uncertainty as to whether FIPPA applies to CCO in its role as a HINP and PE for the eCTAS program. This uncertainty may undermine CCO's compliance measures.	CCO should seek to clarify FIPPA's applicability to CCO through an amendment to PHIPA and/or its Regulation, clarifying that FIPPA does not apply to CCO's collection, use or disclosure of PHI, when acting under its various PHIPA authorities, such as a service provider/HINP; and a s. 45 PE. This would be further to a July 27, 2012	Business Unit/LPO	July 31, 2017	LPO will engage appropriate MOHLTC contacts to seek clarification of CCO's role under PHIPA and FIPPA.

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
					submission to the MOHLTC on the same topic.			
eCTAS	PE	29-Aug-16	Privacy Specialist	FIPPA ss. 39(2) requires institutions (*e.g.*, CCO and participating hospitals) to provide notice to individuals of the collection of PI, including (a) the legal authority for the collection; (b) the principal purpose or purposes for which the PI is intended to be used; and (c) the title, business address and business	LPO should ensure that, in the form of Participation Agreements, the participating hospital is required to provide patients with a form of notice that complies with FIPPA ss. 39(2), and to do so on behalf of ATC/CCO (in its Service Provider/HINP Role). The notice should describe CCO's Service Provider/HINP Role. LPO should consider developing the form of notice	Business Unit	Feb 28, 2017	The LPO has concluded that the notice obligation rests with the HIC, pursuant to PHIPA as is also noted in the eCTAS Participation and HINP Agreement.

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
				telephone number of a public official who can answer the individual's questions about the collection. It is unclear how this specific notice will be provided to patients, creating a potential risk of non-compliance with FIPPA.	and attaching it as an exhibit to the Participation Agreements.			
eCTAS	PE	29-Aug-16	Privacy Specialist	The eHO ONE ID Service has been proposed for use with the eCTAS system to ensure that only authorized triage nurses are able to input and access PHI; however it is unclear how that service will be	LPO should ensure that the use of the eHO ONE ID Service as part of the eCTAS system is within the scope of any existing agreement between CCO and eHO. If it is not in scope, then a new or amending agreement should be signed to	Business Unit	Feb 28, 2017	The OneID service agreement will be amended as required to ensure it addresses the eCTAS initiative's use of the service.

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
				engaged by CCO.	address this use of the service.			
eCTAS	PE	29-Aug-16	Privacy Specialist	The "breach notification" requirement (imposed on CCO as part of PHIPA's HINP requirements) is only partially met by CCO's agreement with Microsoft. PHIPA requires notification to be "immediate" (rather than "prompt"), and to arise on both actual and suspected privacy breaches (rather than just "successful" privacy breaches).	Due to the confidential nature of the details of the analysis, CCO has excluded a description of the analysis from the public version of this report, however, these details have been provided to the IPC.	LPO	Feb 28, 2017	The LPO has reviewed guidelines issued by the Information and Privacy Commissioner of Ontario. The LPO has determined the breach notification provisions contained in CCO's agreement with Microsoft align with these guidelines.

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
eCTAS	PE	29-Aug-16	Daniel Fabiano and Rosario G. Cartagena, Fasken Martineau DuMoulin LLP	The requirement that Microsoft comply with CCO's privacy and security restrictions and conditions (imposed on CCO as part of PHIPA's HINP requirements) is only partially met by CCO's agreement with Microsoft. There is no express requirement for Microsoft to comply with PHIPA or with CCO's own policies. It is worth noting that, on the whole, this is a relatively low-level risk because the obligations imposed on Microsoft are extensive.	Due to the confidential nature of the details of the analysis, CCO has excluded a description of the analysis from the public version of this report, however, these details have been provided to the IPC.	LPO	Feb 28, 2017	The LPO has determined that the obligations imposed on Microsoft in its agreement with CCO are sufficiently comprehensive.

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
eCTAS	PE	29-Aug-16	Privacy Specialist	CCO is required under FIPPA s. 44 to publish a PI bank in respect of all PI under CCO's control that is organized or intended to be retrieved by the individual's name or by an identifying number. A PI bank is required in connection with PHI collected via the eCTAS in CCO's PE role. It is unclear whether a PI bank will be created.	LPO will need to determine whether the PHI collected in CCO's PE role falls into an existing PI bank or merits a new or amended PI bank.	Business Unit/LPO	July 31, 2017	LPO to confirm whether a new or modified personal information bank will be required.
eCTAS	PE	29-Aug-16	Privacy Specialist	CCO's public disclosure channels may not discuss or address the eCTAS initiative. This may result in complaints or challenges as to CCO's openness in its handling of PHI.	LPO should review CCO's public disclosure channels, notably CCO's Statement of Information Practices and a Statement of Purpose (included in *CCO's Privacy Policy*), and update each to reflect the	Business Unit/LPO	July 31, 2017	LPO will review the existing publicly available material to ensure the eCTAS initiative is sufficiently addressed by the existing material.

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
					collection, use and disclosure of a patient's triage record summaries as part of the eCTAS nitiative.			
eCTAS	PE	29-Aug-16	Privacy Specialist	There is a risk that, despite CCO's intentions, the reports may contain PHI. This may arise through human error or because the de-identification methods were inadequate.	The project team and LPO should review the de-identification protocols that will apply to the eCTAS database to ensure that they will adequately de-identify PHI so that it is not disclosed as part of any reports.	LPO	Nov 1, 2017	The de-identification protocols will be provided to the eCTAS team when the development of reports takes place and before they are disseminated.

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
eCTAS	PE	29-Aug-16	Privacy Specialist	The IPC guidance document advises that CCO conduct a TRA on any cloud computing arrangement. CCO has not yet completed and documented such a TRA. In addition to addressing the HINP requirements (per Privacy Risk [#4]), the TRA should also address risks and controls specific to the Microsoft Azure services.	Same as Privacy Risk [#4].	Business Unit/LPO	Feb 28, 2017erepo	A Security assessment has been conducted by CCO vendors to meet CCO's Security Office's requirements.

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
Quality Management Partnership (**QMP**) Phase 1	PE	31-Mar-15	Consultants	The data elements stored in the Hub from all sources must be limited to that required to create the QMP reports.	Data required for QMP reports is pulled out of CCO's Hub and into a Data Mart. Only data required for QMP reports is consumed in the Data Mart. This enables CCO to implement role-based access for the Data Mart so that access is limited to CCO analysts who require it to produce the reports. The Data Mart is monitored by CCO's LMAS.	Business Unit	Mar-31-2015	All mitigation strategies were accepted by the business unit.
QMP Phase 1	PE	31-Mar-15	Consultants	While establishing the logistics around the preparation of the QMP reports, attention will need to be paid the physical, technical and administrative safeguards, such as limiting access to the data, printing rights, and	QMP reports contain aggregate data and cell counts of less than 6 have been suppressed. Therefore, CCO can email reports without password protection to recipients since patients and providers cannot be identified. Aggregate reports will only be disseminated to a small audience of facility, regional,	Business Unit	Mar-31-2015	All mitigation strategies were accepted by the business unit.

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
				access/print logging and monitoring.	administrative and provincial leads. Since the reports			
QMP Phase 1	PE	31-Mar-15	Consultants	The preparation of the colonoscopy report will require the amalgamation of data from the Hub as well as the Data Quarantine. This amalgamation process may present risk if appropriate safeguards are not put in place around how it is undertaken (*e.g.,* saving data in the alternate location in order	Data sourced from the Hub and Data Quarantine will feed into a Data Mart which is monitored by LMAS. In addition, role-based access has been implemented for the Data Mart to ensure that only those analysts developing QMP reports will have access. During the linkage process, data will not be saved outside of the Data Mart.	Business Unit	Mar-31-2015	All mitigation strategies were accepted by the business unit.

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
				to marry it with data from the second source could be a proposed solution but would require additional safeguards around access, accuracy, transfer and deletion).				
QMP Phase 1	PE	31-Mar-15	Consultants	While establishing the logistics around the distribution of the QMP reports, attention will need to be paid to physical, technical and administrative safeguards, specifically for the method of delivery.	QMP reports at the facility, regional and provincial levels will not contain identifiable data and will be emailed to recipients. CCO has added a confidentiality disclaimer to remind recipients to widely distribute the reports. Provider level mammography reports which will contain PI will be	Business Unit	Mar-31-2015	All mitigation strategies were accepted by the business unit.

The Data Holding, Information System, Technology or Program Involving PHI that is at Issue	PE or PP	Date of Completion of PIA (or Date Expected to be Completed)	Person Responsible for Completing PIA	Privacy Risks arising from the PIA	Recommendations, Mitigation, Strategies, and/or Privacy Controls arising from the PIA	Responsible Party for Addressing Each Recommendation	Date that Each Recommendation was Addressed (or is Expected to be Addressed)	The Manner in which Each Recommendation was or is Expected to be Addressed
					password protected in transit on the advice of CCO's EISO.			
QMP Phase 1	PE	31-Mar-15	Consultants	Once the data in the Hub has been used to prepare the applicable QMP reports, limitations will need to be in place for the retention of such data.	Data contained in CCO's Hub is being leverage for QMP Year 1 reports. At the present time CCO does not delete data contained in the Hub as it is required for CSP operations. CCO is in the process of developing a records management program and retention schedules for Hub data will align with the program.	Business Unit	Mar-31-2015	All mitigation strategies were accepted by the business unit.

Appendix F: Indicators – Summary from the Log of Legal & Privacy Engagement Request Forms / Privacy Service Engagement Requests

Date PSER/LPER Submitted	Initiative/Project Name	Program/Business Unit	Impacted Data Holding	PIA to be Conducted	Rationale for the Decision	Privacy Specialist
8-Nov-13	Prevention & Surveillance	Smoking Cessation Program	N/A	Yes	The Proposed project involves the Collection, use and disclosure of PHI from ambulatory care patients	Privacy Specialist
14-Nov-13	Evaluation and Reporting	Evaluation and Reporting Data Mart	N/A	Yes	This initiative require copying of data from the Hub to new Data Mart to ensure that flow of data is consistent with existing PIA and data flows.	Privacy Specialist
3-Dec-13	Informatics	MSTR Report Development		Yes	A procurement PIA to be conducted as the initiative may involve exposure of PI/PHI to the vendor	Privacy Specialist

Date PSER/LPER Submitted	Initiative/Project Name	Program/Business Unit	Impacted Data Holding	PIA to be Conducted	Rationale for the Decision	Privacy Specialist
4-Dec-13	Cancer Information Program	BI Developer - MD Level Reporting		Yes	A procurement PIA to be conducted as the initiative may involve exposure of PI/PHI to the vendor	Privacy Specialist
11-Dec-13	Primary Care Cancer Screening	Regional Provider-Level Report		No	The inclusion of additional data elements to the Regional Provider-Level Report did not require a separate privacy assessment. Instead privacy requirements were provided in a BN format.	Privacy Specialist
12-Dec-13	Informatics	RFS for MSTR Upgrade		Yes	A procurement PIA to be conducted as the initiative may involve exposure of	Privacy Specialist

Date PSER/LPER Submitted	Initiative/Project Name	Program/Business Unit	Impacted Data Holding	PIA to be Conducted	Rationale for the Decision	Privacy Specialist
					PI/PHI to the vendor	
13-Dec-13	Prevention & Cancer Control	Siebel Upgrade Project	Hub	Yes	The initiative involved the application of a set of patches to the already in-production COTS application. There are approximately 2 years' worth of patches that will be applied, and some new features and functionality will be introduced along with a number of bug fixes for known defects. No new features and functionality will be turned on for this project, but will	Privacy Specialist

Date PSER/LPER Submitted	Initiative/Project Name	Program/Business Unit	Impacted Data Holding	PIA to be Conducted	Rationale for the Decision	Privacy Specialist
					be available for potential downstream projects. A procurement PIA was conducted for this initiative	
17-Dec-13	Regional Operations	Mobile Coaches	N/A	No	A PIA is not needed, however, a privacy risk management plan will be developed and implemented.	Privacy Specialist
18-Dec-13	Patient Experience	Real-Time Measurement: Patient Experience Survey Pilot	N/A	No	This initiative does not involve collection, use or disclosure of PI/PHI	Privacy Specialist
18-Dec-13	Access to Care - Surgery & Diagnostic Imaging Wait Times	Surgeon Scorecard	N/A	No	It was concluded that a PIA is not required for this initiative however; the PAO will	Privacy Specialist

Date PSER/LPER Submitted	Initiative/Project Name	Program/Business Unit	Impacted Data Holding	PIA to be Conducted	Rationale for the Decision	Privacy Specialist
					support the project to define the requirements for the dissemination of the scorecard via email.	
18-Dec-13	Informatics	EDW - OCR Feed for PCCIP	EDW	No	There is no change to PI/PHI collected instead the DSA will be update to reflect the new source of information.	Privacy Specialist
9-Jan-14	Regional Operations	Community-Based Clinic Strategy	N/A	No	The project has been advised to re-engage the PAO as it proceeds to define the data collection, use and reporting requirements and its	Privacy Specialist

Date PSER/LPER Submitted	Initiative/Project Name	Program/Business Unit	Impacted Data Holding	PIA to be Conducted	Rationale for the Decision	Privacy Specialist
					timelines and deliverables	
13-Jan-14	Ontario Cancer Symptom Management Collaborative	Integration of Admission Discharge & Transfer System (ADT) Information to ISAAC	N/A	Yes	This project involves the automation of the patient registration and update processes through system modifications to the ISAAC system in which patient admission, discharge and transfer information from the hospital EHR will automatically be inputted into or changed, as the case may be, in ISAAC.	Privacy Specialist

Date PSER/LPER Submitted	Initiative/Project Name	Program/Business Unit	Impacted Data Holding	PIA to be Conducted	Rationale for the Decision	Privacy Specialist
14-Jan-14	ATC Informatics	ALC Analytical Roadmap	N/A	No	There is no PI/PHI required for the purpose of developing the roadmap.	Privacy Specialist
17-Jan-14	Access to Care - Product Development	WTIS Release 17	WTIS	Yes	Release 17 will enhance the WTIS by modifying dashboard and search criteria and data validation for surgery and DI efficiency which may involve PI/PHI. Hence a PIA addendum will be conducted.	Privacy Specialist
30-Jan-14	Informatics	Symptom Management Dashboard	EDW	Yes	This project involve PHI. It seeks to automate the reporting process by migrating the reports to the	Privacy Specialist

Date PSER/LPER Submitted	Initiative/Project Name	Program/Business Unit	Impacted Data Holding	PIA to be Conducted	Rationale for the Decision	Privacy Specialist
					EDW; having reports generated through MicroStrategy; and accessed by users through iPort.	
4-Feb-14	Regional Operations	Sandy Lake SAR Pilot – SAR 2	N/A	No	There is no additional collection, use or disclosure of PI/PHI. Instead this is an internal evaluation of the project	Privacy Specialist
5-Feb-14	Cancer Information Program	Mobile ISAAC site implementation and integration with AHAC and Family Health Team (FHT) electronic medical record (eMR)	N/A	No	Pending review of the PNAW (including privacy deliverables and timelines) with the business unit. Once reviewed and accepted by the business unit,	Privacy Specialist

Date PSER/LPER Submitted	Initiative/Project Name	Program/Business Unit	Impacted Data Holding	PIA to be Conducted	Rationale for the Decision	Privacy Specialist
					will send PNAW for Sam's signature. PSER re-submitted; PAO to review. Follow up meeting held on Jan 30. Target of evaluation established. PNAW in draft – to be completed by end of week. PNAW complete.	
10-Feb-14	CIO	Establishing a Cloud Computing MSA	N/A	No	This engagement was for procurement of a cloud vendor. There is no PI/PHI involved in the procurement process.	Privacy Specialist

Date PSER/LPER Submitted	Initiative/Project Name	Program/Business Unit	Impacted Data Holding	PIA to be Conducted	Rationale for the Decision	Privacy Specialist
10-Feb-14	PMO Shared Services	PPM Enhancement Phase III	N/A	No	PAO Services not required	Privacy Specialist
12-Feb-14	Prevention & Surveillance	Smoking Cessation in the RCPs, Phase II – Data capture through ALR DataBook	N/A	No	Re-submitted from 2013-31	Privacy Specialist
14-Feb-14	Enterprise Services Information Program (ESIP)	CRM email router implementation	N/A	No	There is no PI/PHI involved in this project. This project will be installing router for CRM email.	Privacy Specialist
18-Feb-14	Prevention & Cancer Control	MIVS/PACS	N/A	Yes	This initiative involve collection, use and disclosure of PI/PHI. A procurement PIA was completed for this project	Privacy Specialist
25-Feb-14	Regional Operations	Scorecard Data Reporting to the RCP	N/A	No	Report card is created from the data PHI	Privacy Specialist

Date PSER/LPER Submitted	Initiative/Project Name	Program/Business Unit	Impacted Data Holding	PIA to be Conducted	Rationale for the Decision	Privacy Specialist
					data. The report are aggregate and do not contain any PI/PHI.	
27-Feb-14	Patient Experience	Real-Time Measurement Survey	N/A	Yes	A procurement PIA to be conducted as the initiative may involve exposure of PI/PHI to the vendor	Privacy Specialist
3-Mar-14	Ontario Renal Network	CCAC/LTC Funding Model	N/A	Yes	This initiative involves the new collection, use and disclosure of PHI, namely chronic kidney disease related (CKD) data by CCO. A PIA thus will be conducted.	Privacy Specialist
10-Mar-14	Prevention & Cancer Control	ICMS Redesign	ICMS	Yes	This initiative involve redesign of the tool which	Privacy Specialist

Date PSER/LPER Submitted	Initiative/Project Name	Program/Business Unit	Impacted Data Holding	PIA to be Conducted	Rationale for the Decision	Privacy Specialist
					collects, uses and discloses PHI. A PIA will be conducted.	
14-Mar-14	Knowledge Transfer Exchange & Education (KTE&E)	Public Engagement Strategy (PES) Pilot #1 (Exam Room Video on Tablet)	N/A	No	The initiative involved collection of PHI. However, the collection was not broad enough to conduct a full PIA. Instead a privacy risk management plan was developed for this initiative.	Privacy Specialist
17-Mar-14	Knowledge Transfer Exchange & Education (KTE&E)	Public Engagement Strategy (PES) Pilot #2 (EMR Optimization Cervical Reminder Phone Calls)	N/A	No	CCO will not have access to clinic PHI as part of the project. However, CCO will collect aggregate level pre-and-post initiative cancer screening	Privacy Specialist

Date PSER/LPER Submitted	Initiative/Project Name	Program/Business Unit	Impacted Data Holding	PIA to be Conducted	Rationale for the Decision	Privacy Specialist
					rates from each participating clinic.	
21-Mar-14	Cancer Screening & Regional Operations	High Risk OBSP Enhancement Project	ICMS	No	The High Risk OBSP Enhancement Project aims to implement improvements to the program, which launched in July 2011. This improvements do not include collection, use and disclosure of PI/PHI.	Privacy Specialist
28-Mar-14	DAP-EPS	Real-Time Integration Report	N/A	No	The key objective of this initiative is to display HL7 rejected messages to hospital DAP-EPS administrators so that they	Privacy Specialist

Date PSER/LPER Submitted	Initiative/Project Name	Program/Business Unit	Impacted Data Holding	PIA to be Conducted	Rationale for the Decision	Privacy Specialist
					can take corrective action in a timely manner. The automation of error message reviews through this initiative has no implications on the privacy controls currently utilized by the DAP-EPS.	
28-Mar-14	Policy, Knowledge Translation and Exchange and Primary Care (PKTEPC)	EMR Optimization CANES FHT Pilot	N/A	No	This project will not result in collection, use and disclosure of PI/PHI by CCO. A PIA is not thus required.	Privacy Specialist
3/31/2014	Evaluation and Reporting	Correspondence Evaluation – OCSP Recall Evaluation	N/A	No	A PIA was not conducted as this was an evaluation of methodology.	Privacy Specialist

Date PSER/LPER Submitted	Initiative/Project Name	Program/Business Unit	Impacted Data Holding	PIA to be Conducted	Rationale for the Decision	Privacy Specialist
					Privacy Office was consulted as part of the evaluation	
3/31/2014	Evaluation and Reporting	Correspondence Evaluation – OCSP Abnormal Results Letters	N/A	No	A PIA was not conducted as this was an evaluation of methodology. Privacy Office was consulted as part of the evaluation	Privacy Specialist
3/31/2014	Evaluation and Reporting	Correspondence Evaluation – OCSP Invitation Letters	N/A	No	A PIA was not conducted as this was an evaluation of methodology. Privacy Office was consulted as part of the evaluation	Privacy Specialist
4-Apr-14	Primary Care Cancer Screening	Regional Provider-Level Report	SAR	No	This initiative require use of PHI for the creation of Regional Provider Level Report. A	Privacy Specialist

Date PSER/LPER Submitted	Initiative/Project Name	Program/Business Unit	Impacted Data Holding	PIA to be Conducted	Rationale for the Decision	Privacy Specialist
					privacy analysis was conducted in a Briefing Note format.	
4/4/2014	Evaluation and Reporting	Predictive Modelling of the system impact of FIT screening in Ontario	N/A	No	This initiative did not move forward.	Privacy Specialist
7-Apr-14	Policy, Knowledge Translation and Exchange and Primary Care (PKTEPC)	Ontario Cervical Screening Program (OCSP) Clinical Engagement	Hub	No	A PIA is not required for this initiative. Instead privacy requirements are provided in a Briefing Note to the business unit	Privacy Specialist
11-Apr-14	Evaluation and Reporting	OCSP Scientific Lead	N/A	No	PAO not required to be engaged for Procurement	Privacy Specialist
11-Apr-14	Evaluation and Reporting	CCC Scientific Lead	N/A	No	PAO not required to be engaged for Procurement	Privacy Specialist

Date PSER/LPER Submitted	Initiative/Project Name	Program/Business Unit	Impacted Data Holding	PIA to be Conducted	Rationale for the Decision	Privacy Specialist
21-Apr-14	Evaluation and Reporting	Correspondence Evaluation – OBSP Invitation Evaluation	Hub	No	Privacy Needs Assessment was completed and determined that a full PIA is not required for this initiative. Instead a privacy risk management plan was developed to manage privacy risks.	Privacy Specialist
4/22/2014	Enterprise Data Management	EDW-OCR Feed for PCCIP	N/A	No	This initiative involved a change in the data feed between the OCRIS and the Hub. OCRIS is being decommissioned and will be replaced with OCR-EDW.	Privacy Specialist

Date PSER/LPER Submitted	Initiative/Project Name	Program/Business Unit	Impacted Data Holding	PIA to be Conducted	Rationale for the Decision	Privacy Specialist
4/30/2014	Prevention & Cancer Control	ICMS-InScreen Feed for PCCIP	Hub	No	New data elements related to high risk screeners were required in the Hub. The LPO reviewed the data and determined this new use is permissible and a PIA amendment would not be required.	Privacy Specialist
1-May-14	Regional Operations	RNFS Transition to Operations		No	This is a transition of a pilot project to operations. There is no new collection, use or disclosure of PHI.	Privacy Specialist
5/5/2014	Prevention & Cancer Control	ICMS-InScreen Deceased PCCIP	Hub	No	This initiative involved an update to the data feed from	Privacy Specialist

Date PSER/LPER Submitted	Initiative/Project Name	Program/Business Unit	Impacted Data Holding	PIA to be Conducted	Rationale for the Decision	Privacy Specialist
					ICMS to the Hub so that death data contained in ICMS flows into the Hub. The LPO determined a PIA was not required for this initiative since this data flow was detailed in the OBSP PIA.	
12-Jun-14	Policy, Knowledge Translation and Exchange and Primary Care (PKTEPC)	HPV Planning and Program Design	N/A	No	In order to support planning and program design for HPV testing within the Ontario Cervical Screening Program, CCO has set up an internal HPV Leadership Working Group. Data	Privacy Specialist

Date PSER/LPER Submitted	Initiative/Project Name	Program/Business Unit	Impacted Data Holding	PIA to be Conducted	Rationale for the Decision	Privacy Specialist
					analyses have been conducted to estimate the volume of women entering and exiting the colposcopy system and thereby the demand on the colposcopy system with and without HPV testing. The analyses are aggregate data with no personal health information.	
13-Jun-14	Provincial Operations	Correspondence 2014/15 (Physician-Linked)	Hub	No	This initiative included name of physician on the invitation letter for screening to patient. A note to file was	Privacy Specialist

Date PSER/LPER Submitted	Initiative/Project Name	Program/Business Unit	Impacted Data Holding	PIA to be Conducted	Rationale for the Decision	Privacy Specialist
					drafted to assess privacy risks with this initiative instead of a full PIA.	
13-Jun-14	Provincial Operations	Correspondence 2014/15 (Preferred-Language Correspondence)	Hub	No	As part of the 2014/15 Correspondence Initiative, Preferred-Language Correspondence on all correspondence screening programs (English or French only) will be implemented to eligible participants in Ontario. A note to file was drafted to assess privacy risks with this initiative	Privacy Specialist

Date PSER/LPER Submitted	Initiative/Project Name	Program/Business Unit	Impacted Data Holding	PIA to be Conducted	Rationale for the Decision	Privacy Specialist
					instead of a full PIA.	
16-Jun-14	Provincial Operations	Correspondence 2014/15 (CCC Components)	Hub		This initiative is an enhancement to an already existing CCC screening program for reminders and abnormal result follow-up reminders. A risk mitigation plan was created to manage privacy risks as a result of this enhancement.	Privacy Specialist
9-Jul-14	Regional Operations	RNFS Transition to Operations (Data Acquisition)	N/A	Yes	This initiative involved collection and integration of RNFS data with a new	Privacy Specialist

Date PSER/LPER Submitted	Initiative/Project Name	Program/Business Unit	Impacted Data Holding	PIA to be Conducted	Rationale for the Decision	Privacy Specialist
					system thus a PIA is required.	
16-Jul-14	Provincial Operations	SAR Release 2 Implementation	SAR	No	This initiative involves enhancing the existing SAR report to provide more functionality to the Primary Care Providers. A PIA was conducted on the initial iteration of the SAR report. A privacy risk management plan was developed to address privacy risks associated with enhancement to SAR report.	Privacy Specialist

Date PSER/LPER Submitted	Initiative/Project Name	Program/Business Unit	Impacted Data Holding	PIA to be Conducted	Rationale for the Decision	Privacy Specialist
11-Aug-14	Integrated Care	The INTEGRATE Project	N/A	Yes	This initiative involves collection of PHI. A PIA was conducted.	Privacy Specialist
2-Apr-15	Digital Centre of Excellence	People, Strategy, and Communications	N/A	No	There is no collection of PI/PHI by this initiative.	Privacy Specialist
2-Apr-15	Social Media Monitoring and Measurement	People, Strategy, and Communications	N/A	No	There is no collection of PI/PHI by this initiative.	Privacy Specialist
2-Apr-15	Social Media Strategy	People, Strategy, and Communications	N/A	No	There is no collection of PI/PHI by this initiative.	Privacy Specialist
9-Apr-15	e-Learning Management System	Primary Care, Cancer Screening	N/A	No	The project is to implement e-Learning Management system. The e-Learning system was to enhance professional education opportunities	Privacy Specialist

Date PSER/LPER Submitted	Initiative/Project Name	Program/Business Unit	Impacted Data Holding	PIA to be Conducted	Rationale for the Decision	Privacy Specialist
					for health care professionals. Terms and Conditions were drafted with assistance from Legal.	
16-Apr-15	ER - Revisit Rate	Access to Care	WTIS	No	The type of analysis planned under this initiative is permitted under CCO authority of PHIPA section 45 prescribed entity. A BN was drafted to explain the legal authority for this type of analysis.	Privacy Specialist
27-Apr-15	Drug Formulary Redesign	People, Strategy, and Communications	N/A	No	There is no collection of PI/PHI by this initiative.	Privacy Specialist
16-Jun-15	WTIS Release 19	Access to Care	WTIS	No	Technical upgrades are conducted to	Privacy Specialist

Date PSER/LPER Submitted	Initiative/Project Name	Program/Business Unit	Impacted Data Holding	PIA to be Conducted	Rationale for the Decision	Privacy Specialist
					WTIS as part of this initiative. There is no new collection, use and disclosure of PI/PHI.	
23-Jun-15	eCCO redesign	People, Strategy, and Communications	N/A	No	This is a CCO internal project with little to no collection, use, or disclosure of PHI and PI.	Privacy Specialist
2-Jul-15	Sioux Lookout SAR	Aboriginal Cancer Control Unit	N/A	Yes	A PIA will be conducted for this initiative. The initiative involve disclosing of First Nations screening activity report to the health care providers in the First Nation communities.	Privacy Specialist

Date PSER/LPER Submitted	Initiative/Project Name	Program/Business Unit	Impacted Data Holding	PIA to be Conducted	Rationale for the Decision	Privacy Specialist
4-Jul-15	Office 365 Transition	Chief Technology Office	N/A	No	The scope of this project does not include PHI.	Privacy Specialist
17-Jul-15	Surgeon Wait time Dashboard	Access to Care	WTIS	No	The type of analysis planned under this initiative is permitted under CCO authority of PHIPA section 45 prescribed entity.	Privacy Specialist
6-Aug-15	Accessing IRS	Aboriginal Cancer Control Unit	N/A	No	A briefing note was drafted describing the rationale for applicability of Freedom of Information Protection of Privacy Act to the release of information in custody and control of CCO.	Privacy Specialist

Date PSER/LPER Submitted	Initiative/Project Name	Program/Business Unit	Impacted Data Holding	PIA to be Conducted	Rationale for the Decision	Privacy Specialist
13-Aug-15	WTIS Registration – Credentials Sub-Process Automation	WTIS	N/A	No	This initiative created a new way of delivery of user credentials to users. Security provided a secure way of communicating credentials. PIA was not required.	Privacy Specialist
28-Aug-15	Corporate Scorecard Tool	Corporate Performance Management	N/A	No	There was no PI/PHI involved in this initiative. The corporate scorecard consisted of aggregation of non PI/PHI data elements.	Privacy Specialist
22-Sep-15	Cervical Cancer Assessment Period	Access to Care	N/A	No	The type of analysis planned under this initiative is permitted under CCO	Privacy Specialist

Date PSER/LPER Submitted	Initiative/Project Name	Program/Business Unit	Impacted Data Holding	PIA to be Conducted	Rationale for the Decision	Privacy Specialist
					authority of PHIPA section 45 prescribed entity.	
19-Jan-16	First Treatment First Referral	Access to Care	WTIS	No	The type of analysis planned under this initiative is permitted under CCO authority of PHIPA section 45 prescribed entity.	Privacy Specialist
29-Jan-16	Siebel Upgrade	Product Management Cancer Service	N/A	No	Premium Support for the current Oracle 11g databases is coming to an end in Jan 2016. Hence, CCO IT operations are planning on upgrading all Oracle 11g databases at CCO to the latest release i.e. 12c, to	Privacy Specialist

Date PSER/LPER Submitted	Initiative/Project Name	Program/Business Unit	Impacted Data Holding	PIA to be Conducted	Rationale for the Decision	Privacy Specialist
					ensure databases are fully supported by the vendor. There is no new collection, use and disclosure of PI/PHI as part of this initiative.	
17-Feb-16	2016 Employee Engagement Survey	People, Strategy, and Communications	N/A	No	Privacy recommendations were minimal.	Privacy Specialist
7-Mar-16	Machine Learning to Identify Breast Cancer Recurrence Using Administrative Data	Disease Pathway Management, Strategic Analytics	N/A	No	This was a grant submission; privacy will not have any feedback until the grant is successful and protocols are being developed.	Privacy Specialist
12-May-16	Community Cancer Profile	Aboriginal Cancer Control Unit	N/A	No	This project will create an aggregate	Privacy Specialist

Date PSER/LPER Submitted	Initiative/Project Name	Program/Business Unit	Impacted Data Holding	PIA to be Conducted	Rationale for the Decision	Privacy Specialist
					cancer profile report on aboriginal communities. The report will not display PI/PHI.	
14-Jun-16	Colorectal Cancer Well Follow-Up Projects	Survivorship	N/A	No	This addendum to the well follow-up project does not involve collection of any new data elements, only follow-up to collect a data element previously assessed. Collection of data by CCO from HICs is permissible under its authority as a prescribed entity.	Privacy Specialist

Date PSER/LPER Submitted	Initiative/Project Name	Program/Business Unit	Impacted Data Holding	PIA to be Conducted	Rationale for the Decision	Privacy Specialist
11-Sep-14	DAP Chart Audit	Regional Planning	N/A	No	This project did not involve a significant collection, use, or disclosure of PHI or a change to systems, technology, programs, etc. that would require a PIA.	Privacy Specialist
10-Jan-15	AZA Data Pull	PDRP	N/A	No	This project did not involve a significant collection, use, or disclosure of PHI or a change to systems, technology, programs, etc. that would require a PIA.	Privacy Specialist
10-Nov-14	ORN CKD EMR Pilot Project	Ontario Renal Network	ORN	No	This project did not involve a significant collection, use, or disclosure of	Privacy Specialist

Date PSER/LPER Submitted	Initiative/Project Name	Program/Business Unit	Impacted Data Holding	PIA to be Conducted	Rationale for the Decision	Privacy Specialist
					PHI or a change to systems, technology, programs, etc. that would require a PIA.	
1-Apr-15	PSW Home Dialysis	Ontario Renal Network	ORN	No	This project did not involve a significant collection, use, or disclosure of PHI or a change to systems, technology, programs, etc. that would require a PIA.	Privacy Specialist
2-Sep-14	PFA Online Collaboration Site	Communications	N/A	No	PHI is not being hosted on this site.	Privacy Specialist
20-Jan-14	ORRS 4-PSER, NTF, PIA Addendum (completed by Anita)	Ontario Renal Network	ORN	Yes	This initiative involve collection, use and disclosure of PI/PHI. A PIA addendum	Privacy Specialist

Date PSER/LPER Submitted	Initiative/Project Name	Program/Business Unit	Impacted Data Holding	PIA to be Conducted	Rationale for the Decision	Privacy Specialist
					was completed for this project	
21-Jan-15	Shredding Services RFP	CTO	N/A	No	This was an operational RFP.	Privacy Specialist
26-Oct-15	Patient Included Designation - CQCO	Clinical Programs and Quality Improvement	N/A	No	Did not result in a PIA. There was no collection, use, or disclosure of PHI involved in obtaining a Patient Included designation, thus no Privacy engagement was actually required.	Privacy Specialist
4-Dec-15	OPCN year-end aggregate data report to LHINs and regional partners	Clinical Programs and Quality Improvement	N/A	No	Did not result in a PIA. Small cells had been suppressed; the data was aggregate. An appropriate acknowledgement statement	Privacy Specialist

Date PSER/LPER Submitted	Initiative/Project Name	Program/Business Unit	Impacted Data Holding	PIA to be Conducted	Rationale for the Decision	Privacy Specialist
					was also enclosed pursuant to CCO's data sharing agreement with CIHI.	
21-Aug-15	Integration of iPort Products with ONE ID	CTO	N/A	No	No formal PIA was conducted, nor was there a risk mitigation plan. This project did not involve any new collections, uses, or disclosures of PHI.	Privacy Specialist
16-Jun-15	ORRS R5	Ontario Renal Network	ORN	No	A Note to file was drafted instead of a complete PIA. The privacy risks and any recommendations were noted in the Note to file.	Privacy Specialist

Date PSER/LPER Submitted	Initiative/Project Name	Program/Business Unit	Impacted Data Holding	PIA to be Conducted	Rationale for the Decision	Privacy Specialist
30-Jun-15	Quantum GIS	CTO or A & I	N/A	No	This project had no impact on PHI. The toll uses aggregate information.	Privacy Specialist
6-Jul-15	My CancerIQ Kidney and Melanoma	Population Health Surveillance	N/A	No	A PIA was done on My Cancer IQ and this change was not significant enough to warrant another.	Privacy Specialist
23-Jun-15	eCCO Redesign	People, Strategy, and Communications	N/A	No	This project has no privacy requirements (CP4 and CP9 were waived). It is an internal project with little to no collection, use, or disclosure of personal health information	Privacy Specialist

Date PSER/LPER Submitted	Initiative/Project Name	Program/Business Unit	Impacted Data Holding	PIA to be Conducted	Rationale for the Decision	Privacy Specialist
					and personal information.	
7-Mar-16	FNIM Discovery	ORN		No	This has no impact on PHI. Limited PHI will be accessed/used for this initiative (i.e., postal code and associated renal treatment type only); postal code may be shared with appropriate individuals at sites but will not be associated with any patient or health information outside of CCO.	Privacy Specialist

Date PSER/LPER Submitted	Initiative/Project Name	Program/Business Unit	Impacted Data Holding	PIA to be Conducted	Rationale for the Decision	Privacy Specialist
23-Jun-15	CRM Implementation	People, Strategy, and Communications	N/A	No	The scope of this project does not include PHI.	Privacy Specialist
1-Aug-15	Dementia Capacity Planning: Proposed Stakeholder Engagement Approach	Ontario Renal Network	N/A	No	The scope of this project does not include PHI.	Privacy Specialist
6-Jul-15	My CancerIQ Evaluation	Population Health Surveillance	N/A	No	This did not impact PHI as the evaluation of the CancerIQ Tool did not use PI/PHI.	Privacy Specialist
Not Available	Transitions Project	CRO	N/A	No	Requirements were provided and embedded through the DDSC process.	Privacy Specialist

Date PSER/LPER Submitted	Initiative/Project Name	Program/Business Unit	Impacted Data Holding	PIA to be Conducted	Rationale for the Decision	Privacy Specialist
24-Jun-16	CIRT Upgrade	Technology Services	CIRT	No	This is a technology related project where by existing CIRT application will be migrated from the Nortel Gateway (no longer supported by the vendor) to the WAP Gateway. There will be no change in the manner PHI is collected, used or disclosed by CCO.	Privacy Specialist
21-Jul-16	WTIS Application Insight Implementation	Product Development	WTIS	No	PIA will not be conducted for this initiative. Implementation of cloud based Microsoft insight will result in	Privacy Specialist

Date PSER/LPER Submitted	Initiative/Project Name	Program/Business Unit	Impacted Data Holding	PIA to be Conducted	Rationale for the Decision	Privacy Specialist
					submission of performance related of WTIS application data. The performance/crash data does not include PI/PHI collected by the WTIS application.	
24-Jun-16	LIRT Upgrade	Technology Services	LIRT	No	This is a technology related project where by existing LIRT application will be migrated from the Nortel Gateway (no longer supported by the vendor) to the WAP Gateway. There will be no change in the manner	Privacy Specialist

Date PSER/LPER Submitted	Initiative/Project Name	Program/Business Unit	Impacted Data Holding	PIA to be Conducted	Rationale for the Decision	Privacy Specialist
					PHI is collected, used or disclosed by CCO.	
21-Jul-16	OBSP Equipment Quality Assurance	Cancer Screening, Implementation	N/A	No	This initiative will review an assessment of quality assurance processes in other jurisdictions to ensure the OBSP has adequate oversight and quality assurance for breast screening equipment. There is no collection, use or disclosure of PI/PHI. A privacy impact assessment is thus not needed.	Privacy Specialist

Date PSER/LPER Submitted	Initiative/Project Name	Program/Business Unit	Impacted Data Holding	PIA to be Conducted	Rationale for the Decision	Privacy Specialist
13-Jul-16	OBSP Transition FY 16/17	Cancer Screening, Implementation	N/A	No	This initiative is adding more OBSP sites to the existing OBSP program. The type of data collected/used and disclosed will be same as the data currently collected, used and disclosed by the existing OBSP sites hence a PIA is not required for this initiative. However, the project team would have to execute applicable agreement (such as funding and HINP agreement) with the new	Privacy Specialist

Date PSER/LPER Submitted	Initiative/Project Name	Program/Business Unit	Impacted Data Holding	PIA to be Conducted	Rationale for the Decision	Privacy Specialist
					OBSP sites. It is thus recommended to have the agreements reviewed by Legal and Privacy before executing them with OBSP sites.	
21-Jul-16	OBSP Equipment Quality Assurance	Prevention & Cancer Control, Primary Care	N/A	No	This initiative will not involve PI/PHI.	Privacy Specialist
28-Apr-16	QMP Reporting – Integration of Expanded RPDB and CHDB Data Feeds	Prevention & Cancer Control, QMP	RPDB/CHDB	No	This initiative is a sub-project of the QMP. The scope of this change will be captured in the QMP program PIA.	Privacy Specialist
25-Nov-14	Mobile Coach Reporting in ICS Monthly Reports	Prevention & Cancer Control, Evaluation and Reporting	N/A	No	This initiative involves a change to aggregate-level reports. There is no	Privacy Specialist

Date PSER/LPER Submitted	Initiative/Project Name	Program/Business Unit	Impacted Data Holding	PIA to be Conducted	Rationale for the Decision	Privacy Specialist
					change to CCO data holdings.	
18-Nov-14	RNFS Transition to Operations	Prevention & Cancer Control	N/A	No	A PIA was not conducted as there was no change to CCO data holdings.	Privacy Specialist
21-Nov-14	Colonoscopy EQI #6- Feasibility Assessment of an ADR Indicator	Prevention & Cancer Control, QMP	ePath	No	This initiative is a sub-project of the QMP. The scope of this change will be captured in the QMP program PIA.	Privacy Specialist
19-Dec-14	Registered Nurse Flexible Sigmoidoscopy (RNFS) Regional Volume Reporting	Prevention & Cancer Control	N/A	No	This initiate involves the addition of aggregate performance metrics to existing screening program reports. There is no change to	Privacy Specialist

Date PSER/LPER Submitted	Initiative/Project Name	Program/Business Unit	Impacted Data Holding	PIA to be Conducted	Rationale for the Decision	Privacy Specialist
					CCO data holdings.	
19-Jan-15	OBSP Transition Project	Prevention & Cancer Control	N/A	No	This imitative includes a number of activities that will bring non-OBSP screening sites formally into the OBSP. The scope of the project includes a current state assessment of non-OBSP sites and transition planning activities. There will be no impact on CCO's data holdings.	Privacy Specialist
23-Jan-15	OBSP Client Activity by Physician Report	Prevention & Cancer Control	N/A	No	This initiative involves the creation of a new OBSP	Privacy Specialist

Date PSER/LPER Submitted	Initiative/Project Name	Program/Business Unit	Impacted Data Holding	PIA to be Conducted	Rationale for the Decision	Privacy Specialist
					activity report sent to certain OBSP physicians containing screening interval data for their patients.	
4-Dec-14	Regional Provider Level Report Release 4	Prevention & Cancer Control	N/A	No	This initiative involved the addition of a few new metrics to the Regional Provider Level Report. These enhancement had no impact on CCO's existing data holdings.	Privacy Specialist
14-Nov-13	Evaluation and Reporting Data mart	Prevention & Cancer Control	N/A	No	This initiative involves the creation of a data mart using data already contain in CCO	Privacy Specialist

Date PSER/LPER Submitted	Initiative/Project Name	Program/Business Unit	Impacted Data Holding	PIA to be Conducted	Rationale for the Decision	Privacy Specialist
					Integration Hub	
16-Oct-14	Siebel Mail Enhancements	PCCIP	N/A	No	Enhancements were made to Siebel to allow for easier triaging of incoming client emails.	Privacy Specialist
13-Dec-13	Siebel Upgrade	PCCIP	N/A	No	This projects involves applying patches to Siebel to ensure to fix known bugs and enhance functionality. A PIA is not required as this project does not involve PI/PHI.	Privacy Specialist
24-Nov-15	Physician-Linked Correspondence - Consent Opt-in process evaluation	Prevention & Cancer Control	N/A	No	This project will involve interviews with PEM physicians who have opted-in	Privacy Specialist

Date PSER/LPER Submitted	Initiative/Project Name	Program/Business Unit	Impacted Data Holding	PIA to be Conducted	Rationale for the Decision	Privacy Specialist
					and opted-out of physician-linked correspondence. There will be no changes to CCO data holdings.	
2/8/2016	High Risk Lung Cancer	Cancer Screening, Implementation	yes	yes	new project, new data collection and data holding	Privacy Specialist
23-Sep-15	Physician-Linked Correspondence - CCC Implementation	Prevention & Cancer Control	N/A	No	This initiative is an expansion to an already existing CCC screening pilot. A risk mitigation plan was created to manage privacy risks.	Privacy Specialist
9-Jun-16	Provincial EPIC Expansion	CPQI	ISAAC	No	A PIA was conducted for the pilot. This initiative is an expansion to an already existing pilot.	Privacy Specialist

Date PSER/LPER Submitted	Initiative/Project Name	Program/Business Unit	Impacted Data Holding	PIA to be Conducted	Rationale for the Decision	Privacy Specialist
					A risk mitigation plan/Note to File will be created to manage privacy risks.	
17-Jun-16	ISAAC - Disease Identification (EPIC)	CPQI	ISAAC	No	A PIA was conducted for the pilot. This initiative is an expansion to an already existing pilot. Additional elements are being added to the interface, no changes in access, use, disclosure of data.	Privacy Specialist
9-May-16	Transition to FIT - Phase 1	Prevention & Cancer Control	N/A	No	This phase does not have any PHI relevance and therefore Privacy input is not required.	Privacy Specialist

Date PSER/LPER Submitted	Initiative/Project Name	Program/Business Unit	Impacted Data Holding	PIA to be Conducted	Rationale for the Decision	Privacy Specialist
23-Feb-16	Patient/Family Advisor Experience Survey – Usability Testing	CPQI	N/A	No	PFA Program has adequate administrative safeguards approved by Privacy in place to carry out this project. No further risk mitigation is required.	Privacy Specialist
16-Dec-15	Patient Engagement in the Public and Patient Engagement Evaluation Tool Study	CPQI	N/A	No	Program decided to limit the scope of this project, no PIA required.	Privacy Specialist
9-Nov-15	ERDM Data Synchronization	Prevention & Cancer Control	N/A	No	Privacy provided a Risk Mitigation Plan as the project did not warrant a PIA. No external stakeholders or data disclosure involved.	Privacy Specialist

Date PSER/LPER Submitted	Initiative/Project Name	Program/Business Unit	Impacted Data Holding	PIA to be Conducted	Rationale for the Decision	Privacy Specialist
23-Sep-15	SETP Encryption	Access to Care - Compliance	N/A	No	Privacy consultation summary: MRN number stand alone does not constitute PHI. Current project of creating an encryption detection logic does not warrant a PIA as there is no PHI relevance.	Privacy Specialist
24-Jul-15	Cancer System Quality Index (CSQI)	CQCO	N/A	No	A patient cancer interview required administrative safeguards in place (i.e.: consent form). No PHI access/use/disclosure involved.	Privacy Specialist
22-Jul-15	Cancer Screening	Prevention & Cancer Control	N/A	No	Cancer screening	Privacy Specialist

Date PSER/LPER Submitted	Initiative/Project Name	Program/Business Unit	Impacted Data Holding	PIA to be Conducted	Rationale for the Decision	Privacy Specialist
	Person Centred Care Program Development				program is incorporating person centered care approach and required Privacy consultation. No PHI relevance.	
21-Apr-15	Kidney Connect Peer Support Program Evaluation	Enhanced Program Evaluation Unit	N/A	No	Consultations summary: no PIA required. Privacy support provided through various administrative safeguards.	Privacy Specialist
10-Feb-15	iPEHOC implementation in ISAAC	CPQI	N/A	No	Risk Mitigation Plan and a Briefing Note was provided to communicate potential privacy risks and agreements	Privacy Specialist

Date PSER/LPER Submitted	Initiative/Project Name	Program/Business Unit	Impacted Data Holding	PIA to be Conducted	Rationale for the Decision	Privacy Specialist
					were executed to follow through as per the mitigation strategy.	
7-Oct-16	PCC Patient Reported Experience Measures ("ORN PREMS")	Ontario Renal Network	N/A	Yes	This initiative will involve new uses and disclosures of PHI, and possible collection of PHI (to be determined).	Privacy Specialist
3-Oct-16	Durham Region Cancer Screening Rate Request	Quality Assurance and QMP	N/A	No	This initiative will involve the disclosure of aggregate data, therefore a PIA was not required.	Privacy Specialist
3-Oct-16	OCSP Participation Gaps Study	Quality Assurance and QMP	N/A	No	This initiative will involve the disclosure of aggregate data, therefore a PIA was not required.	Privacy Specialist

Date PSER/LPER Submitted	Initiative/Project Name	Program/Business Unit	Impacted Data Holding	PIA to be Conducted	Rationale for the Decision	Privacy Specialist
3-Oct-16	QMP Regional Pathology Leads	Quality Assurance and QMP	N/A	No	This initiative will involve a privacy review of the terms of a participation and services agreement for QMP's pathology leads. There will not be collections, uses or disclosures of PHI/PI with this initiative.	Privacy Specialist
11-Oct-16	WTIS - Self Service Password Reset and Recovery	Product Management Cancer Services	N/A	No	No PIA will be required as this project will not have any impact on PHI contained in the WTIS.	Privacy Specialist
11-Oct-16	WTIS Registration	Product Management Cancer Services	N/A	No	No PIA will be required as this project will not have any impact on PHI	Privacy Specialist

Date PSER/LPER Submitted	Initiative/Project Name	Program/Business Unit	Impacted Data Holding	PIA to be Conducted	Rationale for the Decision	Privacy Specialist
					contained in the WTIS.	
21-Sep-16	ISAAC Automatic Login from Site Patient Portal	Patient Centred Care, CPQI	ISAAC	No	Changes are application related – there will be no impact to PHI.	Privacy Specialist
3-Nov-16	FIT KIT Implementation	Cancer Screening, Implementation	DSP	Yes	This initiative will introduce changes to the PHI collected, used, and disclosed	Privacy Specialist

Appendix G: Indicators – Log of PHI Access and Privacy Audits

Audit ID	Nature & Type of the Privacy Audit conducted	Date that the Privacy Audit was completed	Agent(s) responsible for completing the Privacy Audit	Privacy Risk(s) Identified	Recommendations arising from the Privacy Audit	Agent(s) responsible for addressing each Recommendation	Date that each Recommendation was or is expected to be addressed	The manner in which each Recommendation was or is expected to be addressed	Monitoring plan for implementation
2014-01	**PHI Access Audit**: user access to record-level personal health information on H Drive and Servers	July 2015	Legal & Privacy Office together with Data Assets (Identifying users that no longer require access to PHI); IT Operations (Decommissioning user access and managing Access Control Staff)	Users had access that was no longer required	Decommission user access when no longer required.	Legal and Privacy Office and IT Operations	October 2014	Users were manually decommissioned.	Privacy to work with Data Assets and Information Security teams to review IAM software.
2015-01	Privacy Audit: A review of physical safeguards of all CCO premises, including: • Adequate functioning of security cameras • Distribution, recovery, and use of access cards • Practices preventing unauthorized access to CCO systems and premises, including the log of visitors • General physical security practices exercised by employees with respect to securing and disposing of PHI An in-person interview was conducted to discuss the above. The following relevant policy documents were also reviewed, including: • Video Monitoring Standard • Access Card Procedure • Visitor Access Policy • Visitor Access Procedure • Physical Security Policy	Jul-17-2015	Manager, Enterprise Compliance	1) Video monitoring may be required at additional CCO locations	1) Facilities should consider whether CCO's other locations at 525 University Avenue, Toronto and in London should be incorporated under the Video Monitoring Policy.	Director, Facilities	October 2017	The Director, Facilities is currently getting quotes for cost of video monitoring at additional locations. Decision to move forward will depend on plan for moving locations once lease expires in 2017. (Note: Due to uncertainties with respect to renewal of leases at building locations, this recommendation is expected to be addressed once leases are finalized in September 2017).	Plan re: video monitoring to be finalized once moving locations plans are finalized. Privacy to follow up on resulting policy review once leases are finalized

Audit ID	Nature & Type of the Privacy Audit conducted	Date that the Privacy Audit was completed	Agent(s) responsible for completing the Privacy Audit	Privacy Risk(s) Identified	Recommendations arising from the Privacy Audit	Agent(s) responsible for addressing each Recommendation	Date that each Recommendation was or is expected to be addressed	The manner in which each Recommendation was or is expected to be addressed	Monitoring plan for implementation
2015-01	Privacy Audit: A review of physical safeguards of all CCO premises, including: • Adequate functioning of security cameras • Distribution, recovery, and use of access cards • Practices preventing unauthorized access to CCO systems and premises, including the log of visitors • General physical security practices exercised by employees with respect to securing and disposing of PHI An in-person interview was conducted to discuss the above. The following relevant policy documents were also reviewed, including: • Video Monitoring Standard • Access Card Procedure • Visitor Access Policy • Visitor Access Procedure • Physical Security Policy	Jul-17-2015	Manager, Enterprise Compliance	2) Access to CCO premises may not be revoked in a timely manner upon termination of employment	2) Additional information and training should be provided to Managers to ensure they are aware of their responsibility to return access cards to Facilities in accordance with the Procedure.	Director, Facilities & Director, People & Culture	Ongoing	A new process has been implemented whereby HR, IT and Facilities receive a notification in the HCMS system when an employee is terminated. Access cards are disabled upon receipt of this notice within 48 hours of the termination.	N/A – Process has been implemented.
2015-01	Privacy Audit: A review of physical safeguards of all CCO premises, including: • Adequate functioning of security cameras • Distribution, recovery, and use of access cards • Practices preventing unauthorized access to CCO systems and premises, including the log of visitors • General physical security practices exercised by employees with respect to securing and disposing of PHI An in-person interview was conducted to discuss the above. The following relevant policy documents were also reviewed, including: • Video Monitoring Standard • Access Card Procedure • Visitor Access Policy • Visitor Access Procedure • Physical Security Policy	Jul-17-2015	Manager, Enterprise Compliance	3) Landlord access to 620 University Ave. may not be in accordance with CCO's Visitor Access Policy and Procedure	3) Facilities should remind the landlord at 620 University Avenue to provide appropriate notice when access via the 16th floor is required.	Director, Facilities	Nov-30-2015	The Director, Facilities sent a follow up email to Landlord to request provision of appropriate notice when accessing 16th floor at 620 University Ave.	Director, Facilities to advise Manager, Enterprise Compliance if issue continues. Director, Facilities has advised that this is no longer an issue as the landlord is now giving appropriate notice as requested.

Audit ID	Nature & Type of the Privacy Audit conducted	Date that the Privacy Audit was completed	Agent(s) responsible for completing the Privacy Audit	Privacy Risk(s) Identified	Recommendations arising from the Privacy Audit	Agent(s) responsible for addressing each Recommendation	Date that each Recommendation was or is expected to be addressed	The manner in which each Recommendation was or is expected to be addressed	Monitoring plan for implementation
2015-01	Privacy Audit: A review of physical safeguards of all CCO premises, including: • Adequate functioning of security cameras • Distribution, recovery, and use of access cards • Practices preventing unauthorized access to CCO systems and premises, including the log of visitors • General physical security practices exercised by employees with respect to securing and disposing of PHI An in-person interview was conducted to discuss the above. The following relevant policy documents were also reviewed, including: • Video Monitoring Standard • Access Card Procedure • Visitor Access Policy • Visitor Access Procedure • Physical Security Policy	Jul-17-2015	Manager, Enterprise Compliance	4) It is not clear whether there is a mechanism in place to track receipt and removal of electronic hardware and media that contain PHI in and out of CCO facilities as required by the Physical Security Policy	4) The mechanism established to meet the requirement to track the receipt and removal of electronic hardware and media that contain PHI in and out of CCO facilities should be identified. If a mechanism is not in place, once must be developed.	Director, Facilities	August 2016	The Physical Security Policy was revised to include reference to the relevant policy documents.	N/A – addressed.
2015-01	Privacy Audit: A review of physical safeguards of all CCO premises, including: • Adequate functioning of security cameras • Distribution, recovery, and use of access cards • Practices preventing unauthorized access to CCO systems and premises, including the log of visitors • General physical security practices exercised by employees with respect to securing and disposing of PHI An in-person interview was conducted to discuss the above. The following relevant policy documents were also reviewed, including: • Video Monitoring Standard • Access Card Procedure • Visitor Access Policy • Visitor Access Procedure • Physical Security Policy	Jul-17-2015	Manager, Enterprise Compliance	5) Facilities policy documents reviewed do not reflect current state and may not be in line with the most recent IPC guidance (e.g. Video Monitoring Policy)	5) The following reviews/revisions should be made to Facilities policy documents: a) Video Monitoring Policy should be reviewed to ensure any new guidance from the IPC is incorporated and implemented b) Access Card Procedure should be revised to remove references to the now closed Thunder Bay satellite office. c) Visitor Access Procedure should be revised to include reception procedures for 525 University Avenue, Toronto and to remove references to the now closed Thunder Bay satellite office. d) Physical Security Policy be revised to identify the	Director, Facilities & Manager, Privacy	August 2016	The relevant policy documents were reviewed and revised as necessary.	N/A – addressed

Audit ID	Nature & Type of the Privacy Audit conducted	Date that the Privacy Audit was completed	Agent(s) responsible for completing the Privacy Audit	Privacy Risk(s) Identified	Recommendations arising from the Privacy Audit	Agent(s) responsible for addressing each Recommendation	Date that each Recommendation was or is expected to be addressed	The manner in which each Recommendation was or is expected to be addressed	Monitoring plan for implementation
					mechanism to track receipt and removal of electronic hardware and media or to refer to the relevant CCO policy document that meets this requirement (Same as recommendation 4 above)				
2015-02	**PHI Access Audit:** Review of all user accounts at CCO that have access to Personal Health Information (PHI). Active Directory user accounts that have access to H Drive folders and any IT Solution listed in the IDAR tool were in scope for this audit	Dec-18-2015	Legal & Privacy Office: (coordinated between Analytics & Informatics and IT Operations, calculated and summarized metrics & details for review, created Master Audit List to record responses)Analytics & Informatics Department: (provided IDAR expertise, corresponded with users and determined & recorded access needs)IT Operations: (provided H Drive membership list detailed H Drive user access)	1. Users had access that was no longer required	1. Users who no longer require access were recorded in the Master List and forwarded to the IT Operations team for removal	1. IT Operations:, IT Service Mgmt Team (for decommissioning of users)	1. January 2016	1. Users were manually decommissioned by IT Service Mgmt Team	1. Access details to be reviewed on a regular basis as part of the corporate scorecard.
2015-02	**PHI Access Audit:** Review of all user accounts at CCO that have access to Personal Health Information (PHI). Active Directory user accounts that have access to H Drive folders and any IT Solution listed in the IDAR tool were in scope for this audit	Dec-18-2015	Legal & Privacy Office: (coordinated between Analytics & Informatics and IT Operations, calculated and summarized metrics & details for review, created Master Audit List to record responses)Analytics & Informatics Department: (provided IDAR expertise, corresponded with users and determined & recorded access needs)IT Operations: (provided H Drive membership list detailed H Drive user access)	2. The IDAR tool has limited capabilities to decommission user accounts	2. PHI Access Working Group to be established to discuss findings and possible solutions relating to Identity Access Management (IAM).	2. Legal & Privacy Office and Data Assets to establish working group	2. May 2016	2. Working group established with members from Privacy, Security, Architecture, Data Assets and Data Governance	Ongoing quarterly working group meetings.

Audit ID	Nature & Type of the Privacy Audit conducted	Date that the Privacy Audit was completed	Agent(s) responsible for completing the Privacy Audit	Privacy Risk(s) Identified	Recommendations arising from the Privacy Audit	Agent(s) responsible for addressing each Recommendation	Date that each Recommendation was or is expected to be addressed	The manner in which each Recommendation was or is expected to be addressed	Monitoring plan for implementation
2015-03	Privacy Audit: CCO completed a privacy compliance audit at the request of the Canadian Institute for Health Information (CIHI) with respect to a confidentiality agreement enabling CCO to acquire de-identified data from CIHI for a project related to cancer drug utilization. CIHI requested the audit to ensure that CCO was continuing to meet its privacy and security obligations under the confidentiality agreement.	Dec-01-2015	Legal and Privacy Office	N/A	No recommendations as CCO met the requirements of the confidentiality agreement	N/A	N/A	N/A	N/A
2016-01	Privacy Audit – The Legal and Privacy Office audited the following privacy policies against the organizational practices • Secure Retention of PHI • Privacy Policy • PIA Standard • Privacy and Information Security Risk Management Procedure • Data Sharing Agreement Initiation Procedure • Internal Data Access Request Procedure	Sep-30-2016	The Legal and Privacy Office	Gaps in the operation and policy statements	Update policies to reflect the current organizational practices. As well, as communication of polices to relevant stakeholders	Legal and Privacy Office	Oct-16	Policies will be updated and communicated relevant stakeholders	N/A

Audit ID	Nature & Type of the Privacy Audit conducted	Date that the Privacy Audit was completed	Agent(s) responsible for completing the Privacy Audit	Privacy Risk(s) Identified	Recommendations arising from the Privacy Audit	Agent(s) responsible for addressing each Recommendation	Date that each Recommendation was or is expected to be addressed	The manner in which each Recommendation was or is expected to be addressed	Monitoring plan for implementation
2016-02	PHI Access Audit: Review of all user accounts that have access to PHI, active directory user accounts that have access to H: drive folders and any IT solution listed in IDAR were in scope for this audit for the period of January 1, 2016 to March 31, 2016.	May-2-2016	Legal & Privacy Office: (coordinated between Analytics & Informatics and IT Operations, calculated and summarized metrics & details for review) Analytics & Informatics Department: (provided IDAR expertise, corresponded with users) IT Operations: (provided H Drive membership list detailed H Drive user access)	Users had access that was no longer required	Users who no longer required access were recorded in the master list and forwarded to the IT operations team for removal.	IT Operations and IT Service Management Team	June 30, 2016	Users were manually decommissioned.	Access details to be reviewed on a regular basis as part of the corporate scorecard.
2016-03	PHI Access Audit: Review of all user accounts that have access to PHI, active directory user accounts that have access to H: drive folders and any IT solution listed in IDAR were in scope for this audit for the period of April 1, 2016 to June 30, 2016.	July 7, 2016	Legal & Privacy Office: (coordinated between Analytics & Informatics and IT Operations, calculated and summarized metrics & details for review) Analytics & Informatics Department: (provided IDAR expertise, corresponded with users) IT Operations: (provided H Drive membership list detailed H Drive user access)	Users had access that was no longer required	Users who no longer required access were recorded in the master list and forwarded to the IT operations team for removal.	IT Operations and IT Service Management Team	Sept. 30, 2016	Users were manually decommissioned.	Access details to be reviewed on a regular basis as part of the corporate scorecard.

Audit ID	Nature & Type of the Privacy Audit conducted	Date that the Privacy Audit was completed	Agent(s) responsible for completing the Privacy Audit	Privacy Risk(s) Identified	Recommendations arising from the Privacy Audit	Agent(s) responsible for addressing each Recommendation	Date that each Recommendation was or is expected to be addressed	The manner in which each Recommendation was or is expected to be addressed	Monitoring plan for implementation
2016-04	PHI Access Audit: Review of all user accounts that have access to PHI, active directory user accounts that have access to H: drive folders and any IT solution listed in IDAR were in scope for this audit for the period of Julyl1, 2016 to Sept 30, 2016.	Oct. 21, 2016	Legal & Privacy Office: (coordinated between Analytics & Informatics and IT Operations, calculated and summarized metrics & details for review) Analytics & Informatics Department: (provided IDAR expertise, corresponded with users) IT Operations: (provided H Drive membership list detailed H Drive user access)	Users had access that was no longer required	Users who no longer required access were recorded in the master list and forwarded to the IT operations team for removal.	IT Operations and IT Service Management Team	Dec. 31, 2016	Users were manually decommissioned.	Access details to be reviewed on a regular basis as part of the corporate scorecard. PHI access issues log created.

Appendix H: Indicators – Summary from the Log of Privacy Breaches

Prescribed Entity

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
ORN	2013-11-01	2013-11-01	External	2013-12-18	Email breach. PHI included patient name, HIN, DOB, 1 renal treatment code and date of treatment.	PHI was emailed to the ORN by the Healthcare Service Provider. The email was sent in an effort to resolve an issue that the sender was having with submitting to ORRS.	2013-11-01	The LPO asked the sender and recipients of the email to delete the email from all folders.	2013-11-01	N/A	Senior Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2013
P&RP	2013-11-07	2013-11-08	External	2013-11-15	Email breach. Attachment contained PHI (patient chart numbers, HINs, diagnosis codes).	PHI was included in an email to the Project Team Lead from the Healthcare Service Provider.. The email was sent in regards to the ALR Transition Project.	2013-11-08	The Project Team Lead deleted the email from her inbox and deleted items folders. The Project Team Lead emailed the sender, informed them that the email they had sent contained PHI, and instructed them to delete the email from their sent items and deleted items folders. Project Team Lead sent out a reminder to all hospital sites that PHI must not be	2013-11-08	2013-11-08	Senior Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit & Privacy Specialist	N/A	See "Containment Measure".	2013

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
								emailed to CCO.										
N/A	2013-11-08	2013-11-08	External	2014-01-03	Email breach. Screenshot attachment included PHI (DOB, HIN and chart number).	Healthcare Service Provider. emailed CCO a screenshot of new patient enrollment containing PHI, in order to ask a question about eClaims.	2013-11-08	Associate Product Manager replied to the sender informing them that they had sent PHI, and followed up with a phone call asking the sender to delete the email from all folders on their end. The email was deleted from all folders at CCO's end.	2013-11-08	2013-11-08	Senior Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	2013-11-08	See "Containment Measure".	2013
P&RP	2013-12-04	2013-12-04	External	2014-01-09	Mail breach. The mailed survey contained patient name, HIN, hospital card imprint, address, home telephone number, and DOB.	A patient satisfaction survey was sent to the Diagnostic Assessment Program (DAP) in error. The DAP has an anonymous patient experience survey distributed by the regional DAPs to patients. Patients complete the survey and send it to CCO directly. When the DAP received this	2013-12-19	The coordinator who discovered the PHI passed the letter onto the Research Associate to determine next steps. The Research Associate separated the survey containing PHI from the DAP survey and reported the breach to the LPO. The survey was secured in a filing cabinet. The Privacy	N/A	2013-12-19	Privacy Analyst	Privacy breach	PE breach	N/A	Business Unit & Privacy Specialist	N/A	See "Containment Measure".	2013

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						patient experience survey in the mail, the envelope also contained a post-op satisfaction survey and a symptom assessment form meant for a local hospital.		Analyst attempted to contact the patient and inform them of the breach but could not reach them after several contact attempts. Later, the Privacy Analyst shredded the survey containing PHI.										
N/A	2013-12-12	2013-12-12	External	2014-03-07	Email breach. PHI included patient name and drug treatments for six patients.	A Pharmacy Technician at Healthcare Service Provider. sent an email containing PHI to the Associate Product Manager at CCO in an effort to get clarification about reimbursement of certain treatments in eClaims. The breach was reported to the LPO.	2013-12-12	The Associate Product Manager informed the sender of the breach, and removed the thread from their own inbox and the deleted items folder. The sender was instructed to do the same.	2013-12-12	2013-12-12	Senior Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	2013-12-12	See "Containment Measure".	2013
N/A	2013-12-12	2013-12-12	External	2014-04-10	Email breach. PHI included patient name and drug treatments for six patients.	Healthcare Service Provider. sent PHI for six patients to CCO via email, in order to get clarification about the reimbursement of certain	2013-12-12	The eClaims user was contacted [by the relevant business unit at CCO?], and informed that his message contained PHI. He was	N/A	2013-12-12	Senior Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2013

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						treatments in eClaims.		asked to remove the thread from all mail folders. The sender was instructed to do same. The sender was cautioned not to send PHI via email.										
ATC - SETP	2013-12-16	2013-12-19	External	2014-05-06	Email breach. Attachment contained PHI (medical record numbers and hospital account number).	The primary SETP Administrator at Healthcare Service Provider. send an email to the Clinical Liaison for SETP at CCO, asking for advice regarding the functionality of the SETP data check tool. A file containing record-level data with PHI was attached to the email in order to illustrate an error from a previous data submission (Aug. 2013).	2013-12-19	[Name omitted] at CCO tried to contact the SETP Administrator by phone on Dec. 18 and 19. They followed up with an email notifying the Administrator of the privacy breach. Senior Business Analyst reminded the sender that data must not be submitted to CCO via email and support requests must not contain PHI.	2013-12-19	2013-12-19	Senior Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2013
ATC - SETP	2013-12-18	2013-12-18	External	2014-04-16	Case file upload breach. Breached data included PHI (account number and MRN). Not sure how the	The primary SETP Administrator at Healthcare Service Provider. uploaded an unencrypted case file containing	2013-12-18	The SETP Senior Business Analyst spoke with the Backup Administrator at the hospital, notifying them that	2013-12-18	2013-12-18	Senior Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit & Privacy Specialist	N/A	See "Containment Measure".	2013

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
					data was transferred.	PHI as part of their November data submission.		the privacy policy was violated and that CCO's LPO would be informed. The SETP Manager notified the SETP Primary Administrator at the hospital that the privacy policy was violated and that CCO's LPO would be informed. A SETP bulletin was sent on Jan 28, 2013 [believe this should say 2014] to all SETP Administrators reminding them about SETP privacy requirements and the need to encrypt monthly data submission files.										
P&RP	2014-01-03	2014-01-03	External	2014-05-07	Email breach. PHI included patient name, HIN, and chart number.	Healthcare Service Provider sent an email containing PHI to CCO's Systemic Treatment Information Program. The sender wanted to ask a question about an	2014-01-03	The sender was informed of the breach, and was asked by the Associate Product Manager at CCO to remove the email from their inbox and deleted items folder. They were cautioned	2014-01-03	2014-01-03	Senior Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2014

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						invalid number error that arose when changing a patient's postal code in eClaims.		not to send PHI in future support requests. The Associate Product Manager also deleted the email from his inbox and deleted items folders.										
ATC	2014-01-13	2014-01-14	External	2014-02-10	Email breach. Screenshot attached contained PHI (medical record number and account number).	Healthcare Service Provider. reached out to ATC by email, stating that they were experiencing difficulty with data submission. ATC advised them to send data via MFT, but the hospital still sent the data as a screenshot and attached to an email.	2014-01-14	The ATC Senior Business Analyst advised the sender that tumbleweed must be used to submit data to CCO. The Senior Business Analyst advised the sender to delete the email from their sent and deleted items folders. The Senior Business Analyst did the same on CCO's side.	2014-01-14	2014-01-14	Senior Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2014
ATC	2014-03-07	2014-03-07	External	2014-12-11	Email breach. PHI included patient name, details of appointments at the hospital.	The MRI efficiency program receives data from hospitals through Tumbleweed. A hospital found and error in their data and the back-up coordinator send the corrected	2014-03-07	The Senior Business Analyst, MRI Efficiency, deleted the email from her inbox and deleted items folder. She then requested the hospital resubmit their data using Tumbleweed	2014-03-07	2014-03-07	Senior Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2014

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						data to CCO via email rather than Tumbleweed.		. She also reminded the coordinator at the hospital that submitting data to CCO via email is against CCO's privacy and security policies.										
P&RP	2014-04-10	2014-04-10	External	2014-12-15	Email breach. PHI included 70 patient chart numbers and related treatment information.	A hospital had a question about an ALR metrics report and emailed the PHI CCO's Systemic Treatment Program Project Lead and two other CCO staff with the program.	2014-04-10	The Project Lead contacted the two other CCO recipients and they all deleted the email from their inboxes and deleted items folders. The sender of the email was contact and informed a privacy breach had occurred. The recipient was instructed to delete the email from their sent and deleted items folders.	2014-04-10	2014-04-10	Senior Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2014
P&RP	2014-04-16	2014-04-16	External	2014-12-15	Email breach. PHI included chart numbers and related treatment information for 450 patients.	A hospital had a question about ALR data they submit to CCO's Systemic Treatment Program. The hospital emailed the questions	2014-04-16	The Senior Manager, Systemic Treatment Program delete the email from her inbox and deleted items folder. The Senior Manager informed the	2014-04-16	2014-04-16	Senior Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2014

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						and attached a file containing their previous data submission to CCO.		sender of the privacy breach, reminded them no to email PHI and asked them to delete the email from their sent and deleted items folders.										
P&RP	2014-05-06	2014-05-06	External	2014-12-16	Email breach. PHI included health card number, dates of patient appointments.	PHI data was sent in two attachments within an email by a data coordinator from a hospital. The email was sent in effort to resolve an issue the sender was having with submitting data for the DAP Data Upload Tool (DDUT).	2014-05-06	The Manager, DAP, contacted the data coordinator at the hospital to inform them of the breach. She indicated data submission issues should be resolved over the phone. The email was deleted from the recipient inbox and deleted items folders.	2014-05-06	2014-05-06	Senior Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2014
CPQI	2014-05-07	2014-05-07	External	2015-01-01	Email breach. PHI included health card numbers and dates of oncology visits.	An email containing PHI was sent to the Program Manager, Survivorship. The email was sent by a hospital The information is usually sent securely to CCO using Tumbleweed.	2014-05-07	The Program Manager contacted the hospital to had them resubmit the data through Tumbleweed. The email was deleted from the recipient's Outlook.	2014-05-07	2014-05-07	Senior Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2014

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
ATC	2014-05-09	2014-05-09	External	2015-01-02	Email breach. Patient chart number and treatment related data.	The MRI efficiency program receives data from hospitals through Tumbleweed. A hospital found and error in their data and the back-up coordinator send the corrected data to CCO via email rather than Tumbleweed.	2014-05-09	The Senior Business Analyst, MRI Efficiency, deleted the email from her inbox and deleted items folder. She then requested the hospital resubmit their data using Tumbleweed. She also reminded the coordinator at the hospital that submitting data to CCO via email is against CCO's privacy and security policies.	2014-05-09	2014-05-09	Senior Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2014
P&RP	2014-07-02	2014-07-02	External	2015-01-02	Email breach. Patient name and medical record number.	The email was sent by a hospital to 10 recipients who are employees from 2 separate hospitals and CCO. Two of the recipients were CCO employees. The email was sent in an effort to resolve a data issue with one patient record.	2014-07-02	The Interim Manager, Systemic Treatment Program, emailed all 10 recipients of the email, as well as the sender to notify them of the breach. The sender and all 10 recipients were asked to delete the email from their inboxes, folders and deleted items.	2014-07-02	2014-07-02	Senior Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2014
P&RP	2014-07-16	2014-07-16	External	2015-01-02	Email breach. Records for 40 patients	The email was sent by a hospital to the Interim	2014-07-16	The Interim Manager, Systemic Treatment	2014-07-16	2014-07-16	Senior Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2014

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
					including the following data elements: facility number, health care number, disease site information, treatment regimen information.	Manager, Systemic Treatment Program. The Phi was sent by email rather than through a secure SSL port.		Program, emailed the sender and asked him to delete the email from his sent and deleted items folders. She then deleted the email from her inbox and deleted items folder.										
P&RP	2014-08-08	2014-08-08	External	2015-01-02	Email breach. PHI included medical record number, treating oncologist, appointment dates, diagnosis codes, case notes.	An email containing PHI was sent to the Project Coordinator, Systemic Treatment Program and the Acting Manager. An oncologist sent the email to determine why a patient's case was considered out of scope for the Systemic Treatment funding model.	2014-08-08	Project Coordinator contacted the Acting Manager and asked her to delete the email from her inbox and deleted items folder. Email was saved on CCO's secure H-drive so the program could respond. The Project Coordinator deleted the email from Outlook and contact the sender to ask him to delete the email from his sent and deleted items folders.	2014-08-08	2014-08-08	Senior Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2014
ATC	2014-08-08	2014-08-08	External	2015-01-02	Email breach. PHI included patient name, details of appointment	The MRI efficiency program receives data from hospitals through Tumbleweed	2014-08-08	The Senior Business Analyst, MRI Efficiency, deleted the email from her inbox and deleted	2014-08-08	2014-08-08	Senior Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2014

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
					s at the hospital.	. A hospital found and error in their data and the back-up coordinator send the corrected data to CCO via email rather than Tumbleweed.		items folder. She then requested the hospital resubmit their data using Tumbleweed. She also reminded the coordinator at the hospital that submitting data to CCO via email is against CCO's privacy and security policies.										
ATC	2014-09-09	2014-09-09	External	2015-01-07	Email breach. PHI included patient name, details of appointments at the hospital.	The MRI efficiency program receives data from hospitals through Tumbleweed. The hospital's data coordinator sent the data by email rather than through Tumbleweed.	2014-09-09	The Senior Business Analyst, MRI Efficiency, deleted the email from her inbox and deleted items folder. She then requested the hospital resubmit their data using Tumbleweed. She also reminded the coordinator at the hospital that submitting data to CCO via email is against CCO's privacy and security policies.	2014-09-09	2014-09-09	Senior Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	2014-09-09	See "Containment Measure".	2014

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
CPQI	2014-12-11	2014-12-11	External	2015-01-16	Email breach. Email contained patient's name, DOB, and HIN.	PHI data was included in an email to a Reimbursement Associate at CCO from a Pharmacist at Healthcare Service Provider. The email was sent in an effort to request a prior approval for a patient.	2014-12-11	Reimbursement Associate has: • Deleted the email from her inbox and delete items folder • Emailed the sender, informed them that the email they had sent contained PHI, and instructed them to delete the email from their sent items and deleted items folders ...Reimbursement Associate emailed the pharmacist to inform that all communication pertaining to patients should be sent through eClaims and that the original email they sent contained PHI and they should delete the email from their sent items and deleted items folder	2014-12-11	2014-12-11	Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	2014-12-11	See "Containment Measure".	2014
ATC	2014-12-11	2014-12-11	External	2015-01-19	Email breach. Email included patient ID for	Patient Care Manager from a site emailed CCO with a	2014-12-11	Delete email from all folders and instruct the sender of	2014-12-11	2014-12-11	Program Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2014

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
					waitlist ALC, date of death.	query on WTIS with PHI in the email. Though the PHI elements are not identifiable together, this is a breach of policy whereby external sites should not communicate any PHI over email to CCO.		the same as well as notify them of the breach.										
CPQI	2014-12-12	2014-12-15	External	2015-01-21	Email breach. Email contained patient's initials and DOB.	PHI data was included in an email to a Reimbursement Associate at CCO from a Pharmacist at Healthcare Service Provider.. The email was sent in an effort to request a prior approval for a patient from the PDRP.	2014-12-15	The Reimbursement Associate: • Deleted the email from her inbox and delete items folder • Emailed the sender, informed them that the email they had sent contained PHI, and instructed them to delete the email from their sent items and deleted items folders	2014-12-15	2014-12-15	Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	2014-12-15	See "Containment Measure".	2014
CPQI	2014-12-15	2014-12-15	External	2015-01-21	Email breach. Email contained patient's initials and HIN.	PHI data was included in an email to a Reimbursement Associate at CCO from a Pharmacy Technician	2014-12-15	Reimbursement Associate has: • Deleted the email from her inbox and delete items folder	2014-12-15	2014-12-15	Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	2014-12-15	See "Containment Measure".	2014

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						at Healthcare Service Provider.. The email was sent in an effort to request for a prior approval for a patient.		Emailed the sender, informed them that the email they had sent contained PHI, and instructed them to delete the email from their sent items and deleted items folders										
CPQI	2014-12-16	2014-12-16	External	2015-01-27	Email breach. Email contained patient's chart number.	PHI data was included in an email to [Reimbursement Associate, PDRP] from [name omitted], Pharmacist at Healthcare Service Provider.. The email was sent in an effort to request for a prior approval for a patient.	2014-12-16	[Reimbursement associate] has: • Deleted the email from her inbox and delete items folder • Emailed the sender, informed them that the email they had sent contained PHI, and instructed them to delete the email from their sent items and deleted items folders	2014-12-16	2014-12-16	Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	2014-12-15	See "Containment Measure".	2014
ATC - SETP	2015-01-01	2015-01-01	External	2015-02-05	Case file upload breach. Breached data included account number and MRN.	Unencrypted Case file upload contained account number and MRN to the McKesson Performance Benchmark Site (agent for Cancer Care	N/A	McKesson site was instructed to delete the file ASAP and the SETP Administrator was instructed to replace it with a properly	N/A	N/A	Compliance Analyst, ATC & PO Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						Ontario)- Breach of Policy (Data Sharing Agreement which advises to encrypt, though not PHI, sensitive information).		encrypted file.										
ATC - SETP	2015-01-02	2015-01-02	External	2015-02-05	Case file upload breach. Breached data included account number and MRN.	Unencrypted Case file upload contained account number and MRN to the McKesson Performance Benchmark Site (agent for Cancer Care Ontario)- Breach of Policy (Data Sharing Agreement which advises to encrypt, though not PHI, sensitive information). Three policy breaches identified in February through an investigation.	N/A	McKesson site was instructed to delete the file ASAP and the SETP Administrator was instructed to replace it with a properly encrypted file.	N/A	N/A	Compliance Analyst, ATC & PO Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015
ATC - SETP	2015-01-02	2015-01-02	External	2015-02-09	Case file upload breach. Breached data included account number and MRN.	Unencrypted Case file upload contained account number and MRN to the McKesson Performance Benchmark Site (agent for Cancer Care Ontario)-	N/A	McKesson site was instructed to delete the file ASAP and the SETP Administrator was instructed to replace it with a properly	N/A	N/A	Compliance Analyst, ATC & PO Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						Breach of Policy (Data Sharing Agreement which advises to encrypt, though not PHI, sensitive information). Three policy breaches identified in February through an investigation.		encrypted file.										
ATC - SETP	2015-01-02	2015-01-02	External	2015-02-13	Case file upload breach. Breached data included account number and MRN.	Unencrypted Case file upload contained account number and MRN to the McKesson Performance Benchmark Site (agent for Cancer Care Ontario)- Breach of Policy (Data Sharing Agreement which advises to encrypt, though not PHI, sensitive information). Three policy breaches identified in February through an investigation.	N/A	McKesson site was instructed to delete the file ASAP and the SETP Administrator was instructed to replace it with a properly encrypted file.	N/A	N/A	Compliance Analyst, ATC & PO Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015
ATC - SETP	2015-01-02	2015-01-02	External	2015-02-18	Case file upload breach. Breached data included account	Unencrypted Case file upload contained account number and MRN to the McKesson	N/A	McKesson site was instructed to delete the file ASAP and the SETP Administrato	N/A	N/A	Compliance Analyst, ATC & PO Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
					number and MRN.	Performance Benchmark Site (agent for Cancer Care Ontario)- Breach of Policy (Data Sharing Agreement which advises to encrypt, though not PHI, sensitive information). Three policy breaches identified in February through an investigation.		r was instructed to replace it with a properly encrypted file.										
ATC - SETP	2015-01-02	2015-01-02	External	2015-02-24	Case file upload breach. Breached data included account number and MRN.	Unencrypted Case file upload contained account number and MRN to the McKesson Performance Benchmark Site (agent for Cancer Care Ontario)- Breach of Policy (Data Sharing Agreement which advises to encrypt, though not PHI, sensitive information). Three policy breaches identified in February through an investigation.	N/A	McKesson site was instructed to delete the file ASAP and the SETP Administrator was instructed to replace it with a properly encrypted file.	N/A	N/A	Compliance Analyst, ATC & PO Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
CTO	2015-01-07	2015-01-07	Internal	2015-02-24	Incorrect data upload in ISAAC. Believe this contains PHI but the historical record was unclear on data elements included.	From Analyst, Tech Services, Cancer Information Program: [Name omitted] of the Healthcare Service Provider. had issues uploading patients to ISAAC. He notified our team via email. ...[Analyst] with the assistance of Ops looked at the event logs and viewed the patient upload file to look for errors. ...The file was copied to the [H: drive] so that [the Analyst] could repair the errors in the upload file and upload to ISAAC. The file contained PHI... ...[The Analyst enrolled the 132 patients to the wrong site in the ISAAC application due to human error: the upload went to hospital	2015-01-08	[Immediate actions taken by the Analyst on 1/7/2015:] • Identified the mistakenly added records • Discharged the patients from the hospital site (so they are not visible in the UI by hospital staff and so that the patients themselves will not see any association to hospital. Users of the hospital should not be able to access the PHI and patients who existed in the system should not notice any impact of their use.) • Developed a database script to clean the leftover data • Test the script in the test environment with our QA • Had our DEV(?) review the script to ensure he had no concerns. • Notified [manager] of the situation	N/A - internal	2015-01-08	Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						instead of Healthcare Service Provider. Healthcare Service Provider. is a new site to the application and has not yet gone live.		[Manager recommended discharging the patients] • Setup a standard change [request] to clean up the data • Emailed ops to secure a resource To-Do • Confirm resource with Ops (today) • Email CAB for approval (today) • CAB approval (today or tomorrow) • Deploy clean up script (Monday)										
CPQI	2015-01-15	2015-01-16	External	2015-02-24	Email breach. Email contained patient's initials.	PHI data...were included in emails to [individuals in PDRP] on January 15, 2015, from [two individuals] in an effort to reconcile a request for information to confirm a patient's diagnosis.	2015-01-16	• [Breach reporter] has deleted the email from her inbox and deleted items folders. • [Breach reporter] has informed the senders that the original email contained PHI and instructed them to delete the email from their inbox, sent items, and deleted items folders.	2015-01-16	2015-01-16	Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
ATC	2015-01-19	2015-01-19	External	2015-03-01	Email breach. PHI included MRN, order received date and time, procedure code, actual service date and time, and wait time.	PHI was included in an email from [name omitted], MRI Efficiency Coordinator and WTIS Coordinator at Healthcare Service Provider.. The email was sent in an effort to provide details around MRI Priority 4 wait... The email was sent to atcsupport@cancercare.on.ca and then forwarded (without opening) to [Service Analyst, ATC] who identified PHI in the attachment.	2015-01-19	[Service Analyst] informed [Service Specialist*] that the email attachment contained a spreadsheet of PHI from Healthcare Service Provider. Analyst and Service Specialist] deleted the emails from the inbox (personal and atcsupport), sent box and deleted box. [Coordinator at Healthcare Service Provider.] was emailed at 1:49pm (1/19/2015) to inform her that the email sent contained PHI and instructed her to delete the email from their sent items and deleted items folders. [Coordinator] responded at 1:53pm that she has deleted the emails. ...Facilities confirmed by 1:54pm that the email sent had been deleted from	2015-01-19	2015-01-19	Senior Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
								their inbox, sent folder and deleted folder. ...Report sent to [name omitted], Senior Manager, SD&M. *Current title										
ORN	2015-01-21	2015-01-21	External	2015-03-01	Fax breach. PHI included patient name, address, DOB and contact number.	From submitter, Planning Analyst, ORN: PHI data was included on a fax that was lying by our printer. ...The fax received was a request for medical information (stool results) for a patient from [doctor's name omitted]'s office. The fax was addressed to Cancer Care Ontario.	2015-01-21	[Submitter immediately contacted Senior Privacy Specialist, who recommended that the fax be kept safely under lock and key. The form would be collected by someone from the LPO. The submitter was asked to fill out the breach report form.]	N/A	2015-01-21	Senior Privacy Specialist	Privacy breach	PE breach	See "containment measure". Privacy recommendations mirrored the actions of the business unit.	Business Unit & Privacy Specialist	N/A	See "recommendations".	2015
CPQI	2015-01-21	2015-01-21	External	2015-03-01	Email breach. Email contained patient's chart number.	PHI data...were included in an email to [formulary pharmacist, PDRP] on January 21, 2015, from [Dr.'s name omitted] in an effort to appeal a funding decision for a patient.	2015-01-21	• [Breach reporter] has deleted the email from her inbox and deleted items folders. • [Breach reporter] has informed the sender that the original email contained PHI and instructed	2015-01-21	2015-01-21	Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
								them to delete the email from their inbox, sent items, and deleted items folders.										
CPQI	2015-01-27	2015-01-27	External	2015-03-01	Email breach. The email contained patient's full name, chart number, and primary care physician details.	PHI data was included in an email to the Provincial Drug Reimbursement Associate from a Pharmacist at Healthcare Service Provider.. The email was sent in an effort to complete an application for reimbursement for the New Drug Funding Program.	2015-01-26	The Drug Reimbursement Associate emailed the Pharmacist and informed her that the email sent contained PHI, and instructed to delete the email from the sent items and deleted items folders. The Drug Reimbursement Associate and the Pharmacist both have now deleted the email from their inbox and purged it from the deleted items folder.	2015-01-26	2015-01-26	Privacy Specialist	Policy breach	PE breach	The sender and recipient both purge the email containing PHI from Outlook.	Business Unit	2015-01-26	N/A	2015
CPQI	2015-02-04	2015-02-05	External	2015-03-01	Email breach. Email contained patient's name and chart number.	PHI data...were included in an email to a Formulary Pharmacist at PDRP on February 4, 2015, from a Doctor in an effort to secure funding	2015-02-05	• Formulary Pharmacist at PDRP has deleted the email from her inbox and deleted items folders. • Pharmacist has informed the sender and	2015-02-05	2015-02-05	Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						approval for a patient.		all recipients that the original email contained PHI and instructed them to delete the email from their inbox, sent items, and deleted items folders.										
CPQI	2015-02-05	2015-02-05	External	2015-03-01	Email breach. Email contained patient's name, HIN and drug treatment information.	PHI data was included in an email to the PDRP Program Manager and Director from an Oncologist at hospital. The email was sent in an effort to obtain information regarding an application for reimbursement for the NDFP.	2015-02-05	PDRP Program Manager and Director have: • Deleted the email from their inbox and deleted items folder • Emailed the sender, informed them that the email sent contained PHI, and instructed to delete the email from the sent items and deleted items folders	2015-02-05	2015-02-05	Privacy Specialist	Policy breach	PE breach	PDRP staff to delete email from her inbox and deleted items folders. PDRP staff to contact the sender and instruct them to delete the email from their inbox and deleted items folders.	Business Unit	2015-02-05	N/A	2015
CPQI	2015-02-09	2015-02-09	External	2015-03-01	Email breach. Email contained patient's full name and HIN/chart number.	PHI data was included in an email to [Reimbursement Associate, PDRP] from [name omitted], a pharmacist at hospital.. The email was sent in an effort to follow up on	2015-02-09	[Reimbursement Associate has:] • Deleted the email from their inbox and deleted items folder • Emailed the sender through eClaims, informed them that the email	2015-02-09	2015-02-09	Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						a request for reimbursement for the NDFP.		they had sent contained PHI, and instructed them to delete the email from their sent items and deleted items folders										
ATC	2015-02-12	2015-02-13	External	2015-03-18	Email breach. Email contained patient's name and healthcare institution.	PHI Data was included in an email to the mail box designated to ATC program at CCO (atcsupport @cancercare.on.ca) – Compliance from an employee of hospital.on Thursday, February 12, 2015 at 1:33pm. The email was sent in an effort to request that Waitlist Entry be excluded from reporting.	2015-02-13	• Senior Business Analyst deleted the email and purged the deleted file • Senior Business Analyst sent an email to the employee at hospital advising her of the privacy incident and instructing her to delete the emails and purging them from the deleted folder. [Note: "Senior Business Analyst...asked to resubmit the request with only the Waitlist Entry ID"] • Senior Business Analyst informed the Program Senior Manager who notified the Privacy Specialist at LPO advising of	2015-02-13	2015-02-13	Privacy Specialist	Privacy breach	PE breach	ATC staff to delete and purge the email containing PHI from their system. ATC staff to advise the sender to delete and purge email containing PHI.	Business Unit	2015-02-13	N/A	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
								the privacy incident and that a report would follow.										
CTO	2015-02-18	2015-02-18	Internal	2015-03-25	Email breach. Email contained screenshot that included HIN, patient name, and DOB for one patient record.	On February 18th at around 3:15 PM in preparation for a WTIS-CCN application deployment a screen shot containing PHI for one (1) patient record within the WTIS-CCN application was emailed by a QA Analyst at CCO to two CCO employees including the Program Manager. The QA Analyst was, as part of his duties, validating the deployment of the latest WTIS-CCN product ensuring that it met quality standards as part of pre-deployment process called a “Dry Run Smoke Test”. A final test prior to deploying the system	2015-02-18	After receiving the email, Program Manager responded to the other employee and QA Analyst at CCO that all copies of the email should be deleted immediately from their CCO inbox and Sent Items folder. All employees involved have confirmed that the email has subsequently been deleted. The issue is contained and is limited to the three CCO employees documented above all who have PHI certification.	2015-02-18	2015-02-19	Privacy Specialist	Policy breach	PE breach	All email copies to be deleted from every recipient's outlook folders. Program Manager to review PHI correspondence standards with QA Analyst and reinforce that email is not a secured mechanism. Program Manager to review with staff the procedures for validating Dry Run issues that emerge during Dry Runs. [Not sure if this step was carried out] Program Manager has suggested that QA Analyst take the Annual PHI refresher training again. [Not sure if this step was carried out]	Business Unit & Privacy Specialist	2015-02-19	See "Recommendations".	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						to hospitals. The PHI containing in the screen shot was incidental as the screen shot was showcasing a possible error in the application which the QA Analyst was attempting to confirm.												
CPQI	2015-02-18	2015-02-24	External	2015-03-25	Email breach. Email contained patient's initials and chart number.	PHI data was included in an email to the Reimbursement Associate from a Pharmacist at hospital.. The email was sent in an effort to request for a prior approval for a patient.	2015-02-19	The Reimbursement Associate: • Deleted the email from her inbox and deleted items folder • Emailed the sender, informed them that the email they had sent contained PHI, and instructed them to delete the email from their sent items and deleted items folders ...Reimbursement Associate emailed Pharmacist to inform him that all communication pertaining to patients should be sent through eClaims...	2015-02-19	2015-02-19	Privacy Specialist	Policy breach	PE breach	All copies of email containing PHI to be deleted and purged.	Business Unit	2015-02-19	N/A	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
CPQI	2015-02-19	2015-02-24	External	2015-04-20	Email breach. Email included patient's HIN.	PHI data was included in an email to the Provincial Drug Reimbursement Associate from a Pharmacist at hospital.The email was sent in an effort to request for a prior approval for a patient.	2015-02-20	The Reimbursement Associate: • Deleted the email from her inbox and deleted items folder • Emailed the sender, informed them that the email they had sent contained PHI, and instructed them to delete the email from their sent items and deleted items folders ...Reimbursement Associate emailed Pharmacist to inform him that all communication pertaining to patients should be sent through eClaims...	2015-02-20	2015-02-20	Privacy Specialist	Policy breach	PE breach	All copies of emails containing PHI to be deleted and purged.	Business Unit	2015-02-20	N/A	2015
CTO	2015-02-24	2015-02-24	External	2015-04-20	Email breach. Email contained a screenshot with patient name, sex, DOB and chart, treatment information.	From submitter: PHI Data was included in an email to me from an individual at hospital.. The email was sent to ask a question regarding OPIS application. ...	2015-02-24	• [Associate Product Manager] emailed the sender (removing the screen shot), informed them that the email they had sent contained PHI. Original email was deleted from the inbox	2015-02-24	2015-02-24	Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						Who received the PHI? [Associate Product Manager, Technology Services] How was it sent? Email Why was it sent? Screen shot of patient chemo treatment screen and drug detail screen.		and Deleted folder. Advised original user of breach and to not send PHI data on an email to CCO.											
ATC - SETP	2015-03-01	2015-03-01	External	2015-04-22	Case file upload breach. Breached data included account number and MRN.	Unencrypted Case file upload contained account number and MRN- Breach of Policy (Data Sharing Agreement which advises to encrypt, though not PHI, sensitive information).	1-Mar-15	Delete data from McKesson Servers	15-Dec-15	15-Dec-15	Compliance Analyst, ATC & PO Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015
ATC - SETP	2015-03-01	2015-03-01	External	2015-04-22	Case file upload breach. Breached data included account number and MRN.	Unencrypted Case file upload contained account number and MRN- Breach of Policy (Data Sharing Agreement which advises to encrypt, though not PHI, sensitive information).	1-Mar-15	Delete data from McKesson Servers	15-Dec-15	15-Dec-15	Compliance Analyst, ATC & PO Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
ATC - SETP	2015-03-01	2015-03-01	External	2015-05-19	Case file upload breach. Breached data included account number and MRN.	Unencrypted Case file upload contained account number and MRN- Breach of Policy (Data Sharing Agreement which advises to encrypt, though not PHI, sensitive information).	1-Mar-15	Delete data from McKesson Servers	15-Dec-15	15-Dec-15	Compliance Analyst, ATC & PO Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015
ATC - SETP	2015-03-01	2015-03-01	External	2015-04-28	Case file upload breach. Breached data included account number and MRN.	Unencrypted Case file upload contained account number and MRN- Breach of Policy (Data Sharing Agreement which advises to encrypt, though not PHI, sensitive information).	1-Mar-15	Delete data from McKesson Servers	15-Dec-15	15-Dec-15	Compliance Analyst, ATC & PO Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015
ATC - SETP	2015-03-01	2015-03-01	External	2015-05-12	Case file upload breach. Breached data included account number and MRN.	Unencrypted Case file upload contained account number and MRN- Breach of Policy (Data Sharing Agreement which advises to encrypt, though not PHI, sensitive information).	1-Mar-15	Delete data from McKesson Servers	15-Dec-15	15-Dec-15	Compliance Analyst, ATC & PO Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015
ATC - SETP	2015-03-01	2015-03-01	External	2015-05-13	Case file upload breach. Breached	Unencrypted Case file upload contained	1-Mar-15	Delete data from McKesson Servers	15-Dec-15	15-Dec-15	Compliance Analyst, ATC & PO Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
					data included account number and MRN.	account number and MRN- Breach of Policy (Data Sharing Agreement which advises to encrypt, though not PHI, sensitive information).												
ATC - SETP	2015-03-01	2015-03-01	External	2015-05-22	Case file upload breach. Breached data included account number and MRN.	Unencrypted Case file upload contained account number and MRN- Breach of Policy (Data Sharing Agreement which advises to encrypt, though not PHI, sensitive information).	1-Mar-15	Delete data from McKesson Servers	15-Dec-15	15-Dec-15	Compliance Analyst, ATC & PO Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015
ORN	2015-03-18	2015-03-18	External	2015-05-22	Email breach. Attached screenshot contained PHI (name, HIN, dates of death and DOB of 1 patient).	PHI data was included in an email as an attachment with screenshots sent to ORRS Helpdesk mailbox. [The purpose of the email was to] report issues when attempting to add a death event for a patient in the January reporting period on	2015-03-18	[Actions taken by Associate Support Specialist*:] -Created a new service desk ticket with no PHI -Added the following to the body of the message: Please note that the following e-mail contained Personal Health Information (PHI). Please see the attached copy with	2015-03-18	2015-03-18	Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						the JHH(?) location. [Sender was from hospital..]		the PHI removed. We have removed the e-mail from our Inbox and Deleted Items. Please do the same in your mailbox's Sent Items. A separate support request has been created to address your original issue <insert request number>. If you deem it necessary, please resend the original information, without PHI. You may use Interface Message ID or Waitlist Entry ID to reference a patient. Please quote the request number above so we can append the information to the appropriate request. -Deleted the received email and emptied the deleted items *Current title										

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
ATC	2015-03-25	2015-03-25	Internal	2015-06-01	Email breach. PHI included HIN; also included age and gender for 26 records.	File that included 26 records that included PHI was sent via email within CCO from [Data Analyst, ATC reporting and Analytics] to [name omitted], Clinical Liaison, ATC. Copied on the email were [2 names omitted] from ATC Reporting and Analytics. Staff Involved: Data Analyst, ATC reporting and Analytics (Sender) Team Lead, ATC reporting and Analytics (Recipient) Sr. Data Analyst, ATC reporting and Analytics (Recipient) Clinical Liaison, ATC (Recipient) [Team Lead was also the submitter of the breach form.]	2015-03-26	[The Clinical Liaison was out of the office at the time of sending, and the Team Lead sent a separate email on 3/25/2015 advising not to open the email with PHI, and to delete the PHI right away. The Clinical Liaison then confirmed PHI deletion from her inbox and deleted items box on 3/26/2015.] Immediate actions taken by the Team Lead on 3/25/2015: 1. Instructed sender to delete email from sent box and deleted items box and he did. 2. Deleted email from all the 3 recipients...in the inbox and the deleted items box [Submitter also spoke to sender about the importance of privacy, and advised them to review	N/A - internal	2015-03-26	Group Manager, Privacy	Privacy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
								CCO's privacy training slides again.]										
CPQI	2015-03-25	2015-03-25	External	2015-06-03	Email breach. PHI included patient name, DOB, phone number, postal code, MRN, and HIN for 56 patients.	From submitter: On March 25th an email was sent from me [Policy Research Analyst, SSO] to [name omitted] (Research Nurse for [a pilot study] at hospital.) asking her to send the [pilot study] Database Form 00 to me. My intention was that [the Research Nurse] would send the database using the secure MFT that has been set up for the study... [the Research Nurse] responded to my email and sent me the Form 00 database as an attachment.	2015-03-25	From submitter: I have contacted [the Research Nurse] and the project manager [name omitted] to let them know about the breach. ...I asked [the Research Nurse] to resend the file to the MFT. I also so asked her to do the following: "delete the email you sent me from your 'sent' folder, then delete in your 'deleted' folder and then delete from your 'permanent delete' folder." [The Research Nurse] has emailed me to let me know she has done this. I have done this as well.	2015-03-25	2015-03-25	Group Manager, Privacy	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
ATC - SETP	2015-04-16	2015-04-20	External	2015-04-20	Case file upload breach. Data submission from hospital to McKesson contained 202 records with MRN and account numbers.	An unencrypted file containing PHI was uploaded to the McKesson Performance Benchmark (MPB) website as part of the March 2015 Surgical Efficiency Targets Program (SETP), by [name omitted] at hospital.. ...The monthly Data Quality Process has incorporated a routine check of all hospitals using an encryption software yielding a regular numeric pattern in the MRN and Account Number fields in an effort to detect potentially unencrypted files. hospital. data was highlighted as potentially unencrypted as part of this routine check. Members of the Analytics and	2015-04-20	• [Name omitted, Acting Group Manager, Compliance*] sent an email to [name omitted] requesting the deletion of the unencrypted file from the MPB site. • [Acting group manager] sent an email to [original uploader at Stevenson Memorial] advising her of the privacy incident and instructing her to encrypt the Case File. The new file will be uploaded to MPB once the unencrypted file has been deleted. *Current title.	2015-04-17	N/A	Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						Informatics team with access to the McKesson raw data cut are [2 names omitted.] [Name omitted], SETP Administrator for hospital., was contacted to confirm whether encryption software had been used to conceal PHI before submitting SETP data. She confirmed that this step was overlooked for the March 2015 data submission, resulting in the upload of 202 records with unencrypted MRN and account numbers.												
ATC - SETP	2015-04-20	2015-04-20	External	2015-06-12	Case file upload breach. Breached data included account number and MRN.	Unencrypted Case file upload contained account number and MRN to the McKesson Performance Benchmark Site (agent for Cancer Care	20-Apr-15	McKesson site was instructed to delete the file ASAP and the SETP Administrator was instructed to replace it with a properly	20-Apr-15	20-Apr-15	Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						Ontario)- Breach of Policy (Data Sharing Agreement which advises to encrypt, though not PHI, sensitive information).		encrypted file.										
ORN	2015-04-21	2015-04-22	External	2015-06-15	SharePoint breach. One HIN was included in the file uploaded.	PHI data was included in an ORRS Feedback Tool file from a Main Point of Contact (MPOC) at hospital.. This ORRS Feedback Tool file was uploaded to the Site to provide the ORN with feedback relating to their monthly Data Quality report. One HIN was included in this ORRS Feedback Tool file so that the HIN can be corrected in ORRS.	2015-04-22	• [Senior Analyst, Access to Care] deleted this ORRS Feedback Tool file from the Site (in a secure folder for hospital. use and ATC internal use only). • [Senior Analyst] emailed the sender, informed them that the ORRS Feedback Tool file they uploaded contained PHI, and instructed them to resubmit their ORRS Feedback Tool file without the PHI and to submit that PHI item through Tumbleweed [MFT].	2015-04-22	2015-04-22	Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015
ATC	2015-04-22	2015-04-22	External	2015-06-15	Email breach. The email contained a DOB and	PHI data was included in an email to the	2015-04-22	• [Senior Analyst, ATC Compliance] has deleted	2015-04-22	2015-04-22	Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
					MRN of one patient at the facility.	ATCSupport@cancercare.on.ca mailbox from a coordinator at hospital.. The email was sent in an effort to resolve an issue the sender was having with submitting data for WTIS.		the email from the inbox and deleted items folders. • [Senior Analyst] emailed the sender, informed them that the email they had sent contained PHI, and instructed them to delete the email from their sent items and deleted items folders										
ORN	2015-04-27	2015-05-19	Internal	2015-06-15	Shared drive breach, exacerbated by links to the PHI that were embedded in slide decks circulated via email. PHI included the following data elements: • Patient HIN • DOB • Physician CPSO number Also included clinical information associated with the patient (disease, dates associated with project	PHI was held on the P: drive with the Integrated Care folder. Two slide decks were created including bar graphs representing the aggregate data which linked to this dataset saved on the P; drive. The PHI data was embedded within the graphs and could only be accessed if right clicking and selecting “edit data,” in which case an Excel file	2015-05-19	All data was immediately removed from the P: drive (and kept in the appropriate folder in the H: drive). Slide decks with charts representing this data were removed and replaced with PDF versions or JPEG versions. All recipients of the slides were advised to delete these emails from their inbox and deleted items folders. [The submitter, Senior	N/A - internal	2015-05-19	Team Lead, Privacy	Privacy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
					specific activities)	opened with PHI in it. The slide deck was shared with members of the Integrated Care team, and select members of the Palliative Care team...via email. Only members who have access to the Integrated Care folder could open the embedded Excel files.		Analyst in Integrated Care] deleted all emails with the slides attached from sent messages.										
P&RP	2015-04-28	2015-04-28	External	2015-06-15	Email breach. Email contained ALR case ID, HIN, and treatment info.	Email with PHI mailed to a CCO employee by a Director at a site	2015-04-28	CCO employee requested deletion of emails from all folders and notified sender of the breach	2015-04-28	2015-04-28	Privacy Specialist	Privacy breach	PE breach	Request sites to not email PHI	Business Unit	N/A	See "recommendations".	2015
ATC	2015-05-12	2015-05-12	External	2015-06-15	Email breach. Excel attachment contained PHI - data elements unavailable.	From submitter: An outreach letter was sent to a paediatric surgeon regarding their wait times. A reply was sent for the perioperative coordinator within the facility which with an Excel spreadsheet attachment that	2015-05-12	From submitter: I deleted the message, I informed SD&M to delete messaging from the ATC communications box, email was sent to the surgeon to inform them of the PHI breach and privacy was notified, [name	2015-05-12	2015-05-12	Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						contained PHI and the ATC communications box was cc'd. The email was then forwarded to me [note: Clinical Liaison, ATC] and I opened the attachment where I discovered the breach.		omitted], via email.										
ATC - SETP	2015-05-13	2015-05-13	External	2015-06-15	Email breach. Email included account number and MRN.	Cancellation file containing less than 5 cases emailed to the SETP mailbox by a facility reporting on the Wait Times. The file was encrypted, breach of policy.	13-May-15	Delete the emails from all folders	13-May-15	13-May-15	Compliance Analyst, ATC & PO Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015
ATC	2015-05-22	2015-05-22	External	2015-06-23	Email breach. Unclear what PHI was included.	Email containing PHI was sent to the ORRS Support mailbox. Email was sent by ORRS End User at the hospital.. Individual sent email asking for assistance in adding patient to ORRS. [Email viewed by Specialist,	2015-05-22	Service Specialist deleted email containing PHI from mailbox and additionally from the 'Deleted' Folder. Service Specialist informed Senior Manager and Manager. Service Specialist emailed sender from the hospital.to	2015-05-22	2015-05-22	Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						Service - SD&M.]		advise PHI was received in communication to [CCO]. Asked client to refrain from sending PHI in future and to delete sent email from their 'Sent' folder.										
CTO	2015-05-22	2015-05-22	External	2015-06-19	Email breach. PHI included drug names and dates when the drugs were administered.	[PHI was included in an email to CCO's Helpdesk from an OPIS user at hospital.. The email was sent in an effort to resolve an issue the sender was having with submitting data for OPIS. However, the email contained screenshots with unredacted PHI.]	2015-05-22	[The service desk recipient of the PHI deleted the attachments from the service desk ticket created for the email, and deleted the email from their inbox and deleted items folder. The recipient then emailed the sender, informed them that the email they had sent contained PHI, and instructed them to delete the email from their sent items and deleted items folders. They also created a second ticket without PHI and assigned to	2015-05-22	2015-05-22	Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
								the appropriate Group. The recipient then closed the ticket without PHI in it.]										
P&CC	2015-06-01	2015-06-01	External	2015-06-24	Fax breach. Faxes included patient DOB, name, gender, and study eligibility.	Multiple Research response faxes to the wrong CCO number; intended for a secured fax line were instead fax to the mainline by the lab-notified	N/A	Program to contact lab to notify all labs to use the correct CCO Secured Fax line instead of main line	throughout	N/A	N/A	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015
CTO	2015-06-01	2015-06-03	Internal	2015-06-03	Website breach.	PHI was visible on the QA and OAT ICMS https://icmsqa.cancercare.on.ca or https://icmsqas.cancercare.on.ca.. That is because vendor had disabled the security feature as part of Iteration 1 and 2. 1. PHI was viewed by: Only 1 record was visible on the site that was viewed by the EISO team. 2. Site was published internally, and can be viewed by anyone with	N/A	1. OPS team was requested to disable the site, and IIS for both QA and OAT. 2. The sites are disabled. 3. Vendor has been asked to deploy the Security component (authentication/authorization) in DEV, before moving to QA. Also prior to QA deployment, as it has PHI- EISO has asked the following be in place prior to turning on IIS in QA a. Authenticati	N/A	N/A	Senior Privacy Specialist	N/A	Unclear	N/A	te	N/A	See "Containment Measure".	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						knowledge to the URL.		on is fully functional b. Authorization is in place c. Integration with ArcSight is fully operational and validated by EISO d. A Vulnerability Assessment is completed by EISO and no critical vulnerabilities are found From the submitter: "Unfortunately the logs are not conclusive and we can't tell for sure that a breach occurred. Since the link was not known to many people and the exposure was less than 2 weeks, we can probably affirm that internal employees are not actively looking for rogue links. All the people who had the link also had the clearance to view PHI in the context of										

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
								developing the new ICMS solution. Let me know if there is anything else I can help you."										
P&CC	2015-06-05	2015-06-05	External	2015-08-06	Email breach. PHI included first name, last name, and DOB.	PHI data was included in an email to datarequest @cancercare.on.ca from a genetic counsellor at the hospital.. The email was sent as a follow-up in regards to a request made for a pathology report and the information was enclosed to identify the patient of interest.	2015-06-05	[Associate Analyst, Evaluation and Performance Monitoring] immediately reached out to the requestor using a separate email chain, noting the sensitivity of the data and asking for them to delete the email from their inbox and deleted mail folder. The associate analyst also deleted the email from her inbox and deleted mail folder. [Requestor responded on the same day, noting that they had deleted the email.]	2015-06-05	2015-06-05	Senior Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015
P&RP	2015-06-12	2015-06-12	External	2015-07-13	Email breach. Attachment included PHI (patient	An email containing an attachment with PHI	2015-06-12	[Team Lead] emailed [sender] explaining the privacy	2015-06-12	2015-06-12	Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
					chart numbers, HINs); also included treatment information.	was emailed to [Team Lead, Funding, Regional Programs]. The email came from [name omitted], Data Quality Lead/Project Manager, [University Health Network].		breach and requesting that all emails be deleted from sent boxes and deleted items. [Team Lead] deleted all emails from inbox and deleted items.										
CPQI	2015-06-15	2015-06-15	Internal	2015-07-15	iPort breach. PHI included patient HIN, chart numbers, postal code; also included additional details such as treatment, hospital, visit dates etc.	PHI was made available to Sr. Specialist - Policy for CPQI program and the project coordinator through the SSO IS iPort. A request was made to make the reports transformable/manipulate-able in iPort. This would allow the program to create new reports using available data. System changes were made by Sr. Specialist at the CTO operations to allow for additional access to the program as requested. When the CPQI Sr.	2015-06-15	Once the breach was noted: 1) Sr. Specialist from CPQI informed Manager and Project Coordinator (she did not access data) 2) The Sr. Specialist informed Sr. Analyst (CTO) that unauthorized access to data was granted and asked that permission to see PHI attributes (including DOB, patient chart number, postal code and HIN) be removed. 3) CTO Sr. Analyst removed permission to see PHI attributes. ...Privacy to escalate breach investigation	N/A - internal	2015-06-15	Privacy Specialist	Privacy breach	PE breach	Privacy to ensure containment measures have been employed. Privacy to escalate breach investigation to EISO for access controls. Privacy and EISO to meet with program to discuss standard protocols for access controls with SSO IS iPort system. [UPDATE 7/7/2015: The following are the next steps to prevent any future unauthorized access of PHI via iPort: • EISO and CTO will determine a Data	Business Unit & Privacy Specialist	2015-06-17	See "Recommendations".	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						Specialist went to check permissions, it was noted that they were given permission to manipulate all data elements collected, including PHI. This resulted in unauthorized access granted to the Program Sr. Specialist and the coordinator to PHI elements.		to EISO for access controls [completed]. Privacy and EISO to meet with program to discuss standard protocols for access controls with SSO IS iPort system [not sure when/if completed].						Steward for iPort and inform Privacy as needed. • EISO and CTO will transition any requests for PHI access to CTO. CTO will require IDAR approval from the business manager and Data Steward. • In the meantime, any PHI access requests are to be escalated to [name omitted]. [Name omitted] will engage the business manager to confirm the request and ensure there's an access rationale for the request. • Privacy is available for any discussion and consultation at any points mentioned above. Reaffirmed that IDAR must be enforced at all times for request				

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
														dealing with PHI.]				
ATC - SETP	2015-06-15	2015-06-15	External	2015-07-15	Case file upload breach. Breached data included account number and MRN.	Unencrypted Case file upload contained account number and MRN- Breach of Policy (Data Sharing Agreement which advises to encrypt, though not PHI, sensitive information).	2015-06-15	Delete data from McKesson Servers	N/A	N/A	Compliance Analyst, ATC & PO Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015
ATC - SETP	2015-06-15	2015-06-15	External	2015-07-15	Case file upload breach. Breached data included account number and MRN.	Unencrypted Case file upload contained account number and MRN- Breach of Policy (Data Sharing Agreement which advises to encrypt, though not PHI, sensitive information).	2015-06-15	Delete data from McKesson Servers	N/A	N/A	Compliance Analyst, ATC & PO Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015
ATC - SETP	2015-06-15	2015-06-15	External	2015-07-15	Case file upload breach. Breached data included account number and MRN.	Unencrypted Case file upload contained account number and MRN- Breach of Policy (Data Sharing Agreement	2015-06-15	Delete data from McKesson Servers	N/A	N/A	Compliance Analyst, ATC & PO Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						which advises to encrypt, though not PHI, sensitive information).												
ATC - SETP	2015-06-15	2015-06-15	External	2015-07-15	Case file upload breach. Breached data included account number and MRN.	Unencrypted Case file upload contained account number and MRN- Breach of Policy (Data Sharing Agreement which advises to encrypt, though not PHI, sensitive information).	2015-06-15	Delete data from McKesson Servers	N/A	N/A	Compliance Analyst, ATC & PO Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015
ATC - SETP	2015-06-15	2015-06-15	External	2015-07-15	Case file upload breach. Breached data included account number and MRN.	Unencrypted Case file upload contained account number and MRN- Breach of Policy (Data Sharing Agreement which advises to encrypt, though not PHI, sensitive information).	2015-06-15	Delete data from McKesson Servers	N/A	N/A	Compliance Analyst, ATC & PO Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015
P&CC	2015-06-15	2015-06-23	External	2013-12-04	Email breach. PHI included MRN, DOB and HIN for 20 records.	Suspected PHI (MRNs for 20 records, with no other health info linked) was included as an excel attachment to an email sent Monday June 15th to datarequest @cancercar	2015-06-22	[Associate Analyst, Evaluation and Performance Monitoring] deleted the first and second email from their inbox and deleted items folders.	2015-06-22	2015-06-23	Senior Privacy Specialist	Policy breach	PE and PR breach	N/A	Business Unit	N/A	See "Containment Measure".	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						e.on.ca. The sender was a member of a research study team (at the University) and the object of the request was to ask CCO to link the records to cancer registry data. Before the associate analyst had an opportunity to assess the original file against the de-identification guidelines, a second email was sent Sunday June 21st to datarequest @cancercare.on.ca containing the same 20 records, but this time with definite identifiers (DOB and HIN).		The associate analyst notified the sender and all cc'd after the second email was sent, letting them know that the email they had sent contained personal identifiers, and instructed them to delete the email from their sent items and deleted items folders. To avoid confusion, the associate analyst also instructed that the first email (sent Monday) be deleted in the same manner. Copies of both original emails have been saved on the H: drive under H:\Informatics\DAC, as the files will still be required for eventual linkage, should the data request be approved by the DAC.										

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
P&CC	2015-06-18	2015-06-19	Internal	2015-06-19	Email breach. PHI included a name, health card version code and expiration date.	[PHI was sent to the Senior Policy Specialist, Population Health and Prevention from a dermatologist working with a CCO collaborating committee by email. The Senior Policy Specialist accidentally replied back with the original email in the reply.]	2016-06-19	[The Senior Policy Specialist asked the dermatologist to delete all emails from their inbox and sent folders and deleted items folder. The Senior Policy Specialist did the same with the email received by the dermatologist and her reply.]	2016-06-19	2016-06-19	Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015
CTO	2015-06-24	2015-06-24	External	2015-07-16	Email breach. PHI included MRN number and a screen shot which included the patient's name, DOB, and chart number.	PHI submitted in an email to helpdesk@cancercare.on.ca from [name omitted, Hospital personnel]. The email was regarding dose adjustments that needed to be made.	2015-06-24	[The Associate Support Specialist* took the following immediate actions:] -Deleted contents of the email that were PHI -Sent back an email to notify the sender of the breach -Deleted email and sent items *Current title	2015-06-24	2015-06-24	Group Manager, Privacy	Privacy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015
P&CC	2015-07-07	2015-08-06	External	2015-08-18	Email breach. Attachment was a fax that contained PHI (patient name, DOB).	PHI data was emailed to screening@cancercare.on.ca in an attached fax document (A Release Form For Previous	2015-08-06	• [Associate Analyst, P&CC/recipient] permanently deleted the email from the Screening inbox.	2015-08-06	2015-08-06	Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						Mammographic Image). This is a form that is not typically processed by CCO and only after figuring out how to go about processing it, PHI was noticed in the form. [On investigation, discovered that the recipient does have access to the ICMS database, which includes access to client names and DOBs.]		• [Associate Analyst] instructed the sender to permanently delete the email from their email account.										
CTO	2015-07-13	2015-07-13	External	2016-08-16	Email breach. Contents unknown.	[PHI appeared to have been emailed to CCO's helpdesk inbox from an external sender with a Kingston MRI email address. Original email contents were not available.]	2015-07-13	Associate support specialist replied to the sender, asking them to delete the email from their sent items and deleted items folders. The specialist also deleted the email from their inbox and deleted items. Message to sender: "Please note that your original e-mail contained Personal	2015-07-13	N/A	Privacy Specialist	Privacy breach	Unclear	N/A	Business Unit	N/A	See "Containment Measure".	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
								Health Information (PHI) and we have subsequently removed the PHI from the email body below. We have also permanently deleted the e-mail from our Inbox and Deleted Items. Please do the same in your mailbox's Sent Items and Deleted Items."										
ATC - SETP	2015-07-14	2015-07-15	External	2015-07-21	Case file upload breach. Breached data included account number and MRN.	Partner Facility: Unencrypted Case file upload contained account number and MRN- Breach of Policy (Data Sharing Agreement which advises to encrypt, though not PHI, sensitive information).	15-Jul-15	Delete data from McKesson Servers	15-Jul-15	7-Aug-15	Compliance Analyst, ATC & PO Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015
ATC - SETP	2015-07-14	2015-07-15	External	2015-07-22	Case file upload breach. Breached data included account number and MRN.	Unencrypted Case file upload contained account number and MRN- Breach of Policy (Data Sharing Agreement which advises to encrypt,	15-Jul-15	Delete data from McKesson Servers	15-Jul-15	7-Aug-15	Compliance Analyst, ATC & PO Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						though not PHI, sensitive information).												
ATC - SETP	2015-07-14	2015-07-15	External	2015-07-28	Case file upload breach. Breached data included account number and MRN.	Unencrypted Case file upload contained account number and MRN- Breach of Policy (Data Sharing Agreement which advises to encrypt, though not PHI, sensitive information).	15-Jul-15	Delete data from McKesson Servers	15-Jul-15	7-Aug-15	Compliance Analyst, ATC & PO Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015
ATC - SETP	2015-07-14	2015-07-15	External	2015-07-31	Case file upload breach. Breached data included account number and MRN.	Unencrypted Case file upload contained account number and MRN- Breach of Policy (Data Sharing Agreement which advises to encrypt, though not PHI, sensitive information).	15-Jul-15	Delete data from McKesson Servers	15-Jul-15	7-Aug-15	Compliance Analyst, ATC & PO Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015
ATC - SETP	2015-07-14	2015-07-15	External	2015-08-06	Case file upload breach. Breached data included account number and MRN.	Unencrypted Case file upload contained account number and MRN- Breach of Policy (Data Sharing Agreement which advises to encrypt, though not PHI, sensitive information).	15-Jul-15	Delete data from McKesson Servers	15-Jul-15	7-Aug-15	Compliance Analyst, ATC & PO Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
ATC - SETP	2015-07-14	2015-07-15	External	2015-08-14	Case file upload breach. Breached data included account number and MRN.	Unencrypted Case file upload contained account number and MRN- Breach of Policy (Data Sharing Agreement which advises to encrypt, though not PHI, sensitive information).	15-Jul-15	Delete data from McKesson Servers	15-Jul-15	7-Aug-15	Compliance Analyst, ATC & PO Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015
P&CC	2015-07-15	2015-07-15	External	2015-08-06	Email breach. 1) First email included a description of a patient's age and birth year that was originally sent by the registered nurse coordinator on Jul 14th, 4:46pm. 2) Second email also included physician's notes on the patient, and a description of the types of screening that the patient had undergone.	PHI was included in two emails, both sent to screeningevaluation@cancercare.on.ca (central intake for Evaluation and Performance Management team) and several CCO staff. The source was a Registered Nurse Coordinator at Hospital. The emails were sent in the course of a conversation around RNFS secure portal issues/eligibility criteria for a specific client... When the recipient of the data received the first email	2015-07-15	After the second email was sent by the requestor, the recipient [Associate Analyst, P&CC] immediately: 1) Contacted Privacy indicating that a breach had occurred and 2) Contacted another known recipient of the first email [Senior Analyst*, P&CC], indicating that a review of the situation was underway, and not to further the breach by forwarding the original email. [The Associate	2015-07-15	2015-07-15	Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						(containing only age and birth year), they made a note to follow up with Privacy to ascertain whether a breach had occurred. However, a second email with more information came through the same channel before the recipient had an opportunity to file a report.		Analyst] took the following steps to contain the breach: 1) Deleted the emails from her inbox and deleted mail folder 2) Instructed [the Senior Analyst] to do the same, and to pass on the instructions to anyone else who may have received the email [second recipient later emailed back verifying that all who were cc'd on the email had been informed] 3) Instructed the Registered Nurse from hospital.to do the same. Since the 2nd email containing PHI contained certain program-related concerns, the Registered Nurse was further instructed to contact [the Senior Analyst] via telephone to										

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
								resolve this issue. *Current title.										
CTO	2015-07-16	2015-07-16	External	2015-08-14	Email breach. PHI included patient name, HIN, and DOB.	[PHI was included in an email to CCO's helpdesk inbox from a WTIS coordinator at hospital., who was attempting to troubleshoot a technical issue with WTIS.]	2015-07-16	Associate support specialist replied to the sender, asking them to delete the email from their sent items and deleted items folders. The specialist also deleted the email from their inbox and deleted items. Message to sender: "Please note that your original e-mail contained Personal Health Information (PHI) and we have subsequently removed the PHI from the email body below. We have also permanently deleted the e-mail from our Inbox and Deleted Items. Please do	2015-07-16	N/A	Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
								the same in your mailbox's Sent Items and Deleted Items. ...If you deem it necessary, please resend the original information, without PHI. You may use Interface Message ID or Waitlist Entry ID to reference a patient. Please quote the support request number above so we can append the information to the appropriate request."										
ORN	2015-07-21	2015-07-21	External	2015-08-17	Fax breach. The fax contained 3 "outpatient nephrology referral forms" which contained identifying information such as patient name, address, DOB, and HIN.	On Tuesday, July 21st the receptionist at 620 University received a fax (3 "Outpatient Nephrology Referral Forms") with PHI at 1:30 PM. [Senior privacy specialist] retrieved these forms and ORN was notified of the breach. The referral form is a tool	2015-08-13	The privacy office retrieved these forms from the main reception at 620 University and contacted the ORN to identify the purpose for which they were received, and to advise to whom these should be directed.	N/A	2015-11-19	Senior Privacy Specialist	Policy breach	PE breach	See "containment measure". Privacy recommendations mirrored the actions of the business unit.	Business Unit & Privacy Specialist	N/A	See "recommendations".	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						developed by ORN for use by primary care providers when they are referring outpatients to a nephrologist in the hospital setting and/or in the community.		[Program manager] contacted the ORN clinical programs unit, Early Detection and Prevention Progression portfolio to confirm the purpose of the form, and inquire if there was a purpose for collection. The ORN confirmed with privacy office that there was no ORN purpose for the data and that the faxes should be destroyed. [Business strategist with clinical programs] retrieved the faxes from [a senior privacy specialist] and contacted the primary care provider senders to 1. Inform of the breach, 2. confirm the forms are to be sent to a local nephrologist 3. confirm future referral forms are										

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
								not to be sent to CCO/ORN. [The business strategist and program manager securely faxed the forms back to the originating sites that requested this to be done. Forms were destroyed on CCO's side as soon as confirmation was received that sender had received the forms back and appropriate follow up was in place.] ...Referral form was updated to include the following language: "Please send the completed referral form to a local nephrologist in your region. Do not forward this form to CCO/Ontario Renal Network. If you need to access contact information for a local										

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
								nephrologist, please visit http://www.cpso.on.ca/public-register/all-doctors-search?term"										
P&RP	2015-07-21	2015-07-22	External	2015-08-18	Email breach. Unclear what PHI was included.	A password protected excel document containing PHI was sent via email to [various individuals at CCO] and STFM@cancercare.on.ca. The email contained patient level data intended to help the facility clarify their funding allocation. The email was sent from [name omitted] in Sudbury.	2015-07-23	CCO individuals deleted the email from their inbox and their deleted items folder. [Director, Regional Program Development] also emailed all those on the email chain and asked that the email be deleted from sent folder/inbox, deleted from deleted items folder, and that an email be sent back to confirm these steps have been taken. [Director] instructed the facility to only post patient level data to the SSL folder in the future.	2015-07-23	2015-07-23	Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015
CTO	2015-07-27	2015-07-28	External	2016-08-23	Presumed email breach.	Screen shot contains patient name and DOB	2015-07-28	Deleted screen shot, reported breach ...Informed sender of breach	2015-07-28	2015-07-28	Group Manager, Privacy	Privacy breach	Unclear	N/A	Business Unit	N/A	See "Containment Measure".	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
CPQI	2015-07-31	2015-07-31	External	2015-08-18	Email breach. PHI included a clinic note with patient's full name, HIN, DOB, etc.	PHI Data was included in an attachment by email to [Reimbursement Associate, PDRP] from [name omitted] from Hospital.	2015-07-31	[The Reimbursement Associate has:] • Deleted the email from their inbox and deleted items folder • Emailed the sender, informed them that the email they had sent contained PHI, and instructed them to delete the email from their sent items and deleted items folders	2015-07-31	2015-07-31	Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015
CPQI	2015-08-04	2015-08-06	External	2015-08-26	Email breach. The attachment contained PHI (patient's full name, chart number, HIN, and date of treatment).	PHI data was included in an attachment in an email to [Group Manager, PDRP] from [name omitted] of the DRHC Pharmacy Department. The email was sent in an effort to obtain a price adjustment for a patient that received treatment for a drug from the NDFP.	2015-08-06	[Group Manager] has deleted the email from inbox and deleted items folder and emailed the sender, informed them that the email they had sent contained PHI, and instructed them to delete the email from their sent items and deleted items folders. [Group manager saved the attachment	2015-08-06	2015-08-06	Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
								to the H: drive.]										
P&CC	2015-08-05	2015-08-14	External	2015-09-09	Email breach. Note: aggregate small cells were sent, rather than individual records. The small cells relate to prevalence for individuals with cancer broken down by sex, age group, and geography.	An excel workbook containing at least 1 spreadsheet with multiple small cells <6 was sent by a provincial planner at the Ministry of Health and Long-Term Care to the datarequest@cancercare.on.ca inbox, as well as to the populationhealth@cancercare.on.ca and surveillanceunit@cancercare.on.ca inboxes. [The small cells were sent as a proposed template for the requestor's new request.]	2015-08-07	The monitor of the datarequest@cancercare.on.ca inbox deleted the email from their inbox and deleted mail box, and verified that the monitor of the surveillanceunit@cancercare.on.ca inbox had deleted the email attachment as well. (UPDATE Aug 14th: doubly confirming this via email, and confirming that populationhealth@cancercare.on.ca, which is managed by the same team as surveillance unit, has also been purged of the email.) The monitor of the datarequest inbox has not yet had an opportunity to email the sender asking them	2015-08-06	2015-08-14	Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
								to delete the original attachment. However, surveillance unit did message the sender on August 6th letting them know that there are cell counts less than 6 and that these cells would normally be suppressed at CCO. Still, it may be necessary to ask the requestor directly to delete the data from their server. [Note: Unclear whether further steps were taken.]										
CPQI	2015-08-06	2015-08-06	External	2015-08-31	Email breach. Attachment appeared to contain PHI (patient names) for about 25 patients seen for palliative care in May 2015.	PHI data was included in an Excel spreadsheet in an email to [Quality Lead, CPQI* from name omitted], Regional Palliative Care Lead for hospital.. The spreadsheet was sent to confirm the RCC's wait time performance for palliative care.	2015-08-06	[From submitter:] - I contacted Privacy immediately for assistance - I permanently deleted the file - I contacted [regional lead] informing her that email is not a secure method of transfer for PHI, that I am not authorized to receive	2015-08-06	2015-08-06	Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						*Current title.		that information, and asking her to delete the file from her sent box and anywhere else that it might be contained. I also asked her to instruct anyone else who received the file to do the same. I have received confirmation from her that this is being done.										
ATC	2015-08-14	2015-08-14	Internal and External	2015-09-11	Email breach. Attachment included PHI (patient names and hospital IDs) for 8 records.	PHI data was included in an email to [Team Lead]* at ATC from [name omitted] at LHIN. The email was sent in an effort to resolve an issue regarding cochlear implant wait times for a particular facility. The email was forwarded from [Team Lead] to [Clinical Liaison, Analytics and Informatics]. [Team Lead] did not open accompanying	2015-08-14	[Clinical Liaison] deleted the email from their inbox and deleted items folders. [Clinical Liaison] emailed the sender, informed them that the email they had send contained PHI, and instructed them to delete the email form their sent items and deleted items folders.	N/A	2015-08-14	Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						attachment which had the PHI. [Clinical Liaison] received the forwarded email, opened the attachment and noted the PHI data. *Current title.												
A&I	2015-08-14	2015-08-17	External	2015-09-16	Email breach. PHI included patient names and WTIS procedures for 8 records.	An email trail containing 8 patient records with first and last name and WTIS procedure was sent to the datarequest @cancercare.on.ca inbox and iPortaccess @cancercare.on.ca inbox as part of a new email request from a requestor at a LHIN.	2015-08-17	The monitor of the datarequest @cancercare.on.ca inbox deleted the email from their inbox and deleted mail box, and verified that the monitor of theiPortaccess@cancercare.on.ca inbox had deleted the email attachment as well. The monitor of the iPortaccess inbox has contacted the requestor to advise them to delete the email containing PHI.	2015-08-14	2015-08-17	Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
CPQI	2015-08-18	2015-08-18	External	2015-09-16	Email breach. The attachment contained PHI (patient's initials and HIN).	PHI data was included in an email to [Group Manager, PDRP] from [name omitted] of the hospital.Pharmacy Department. The email was sent in an effort to request reimbursement for a patient that received treatment for a drug from the New Drug Funding Program.	2015-08-18	[Group Manager] deleted the email from inbox and deleted items folder and emailed the sender, informed them that the email they had sent contained PHI, and instructed them to delete the email from their sent items and deleted items folders. [Group Manager] cut and paste the email content into a message through the eClaims secure communication so that the matter could be addressed using eClaims secure messenger function	2015-08-18	2015-08-18	Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015
ATC - SETP	2015-08-18	2015-08-18	External	2015-09-21	Case file upload breach. Breached data included account number and MRN.	Unencrypted Case file upload contained account number and MRN- Breach of Policy (Data Sharing Agreement which advises to	18-Aug-15	Delete data from McKesson Servers	18-Aug-15	18-Aug-15	Compliance Analyst, ATC & PO Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						encrypt, though not PHI, sensitive information).												
ATC - SETP	2015-08-18	2015-08-18	External	2015-09-24	Case file upload breach. Breached data included account number and MRN.	Unencrypted Case file upload contained account number and MRN- Breach of Policy (Data Sharing Agreement which advises to encrypt, though not PHI, sensitive information).	18-Aug-15	Delete data from McKesson Servers	18-Aug-15	18-Aug-15	Compliance Analyst, ATC & PO Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015
CPQI	2015-08-26	2015-08-26	External	2015-09-30	Fax breach. Fax included patient's DOB, name, and eligibility criteria.	Patient eligibility form was faxed by a patient/provider to the main line instead of the secure fax for the program.	2015-08-26	Privacy retrieved the fax from the receptionist and handed it over to the program.	N/A	N/A	Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015
CPQI	2015-08-31	2015-08-31	External	2015-10-08	Email breach. PHI included patient initials and MRN.	PHI data was included in the body of an email to [Reimbursement Associate, PDRP] from [name omitted] from Ottawa Regional Cancer Centre.	2015-08-31	[Reimbursement Associate has:] • Deleted the email from their inbox and deleted items folder • Emailed the sender, informed them that the email they had sent contained PHI, and instructed them to delete the email from their sent items and	2015-08-31	2015-08-31	Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
								deleted items folders										
CPQI	2015-09-09	2015-09-09	External	2015-10-16	Fax breach. Faxed referral form contained PHI (patient name, address, DOB, HIN). Patient history details and consultations.	On Thursday, October 22nd CCO main reception at 620 received a fax with PHI. The intended recipient (CCO's Case by Case Review Program) has a dedicated secured fax line for their incoming requests. However, the sender sent it to CCO's main fax number in error.	2015-09-09	Main line deleted the fax and handed over a printed copy to Privacy Specialist which was delivered to the program contact directly. Re: controls in place, the program has stated: "The CCO CBCRP website encourages applicants to upload documents using our secured upload tool and our program email is listed if they have any questions related to the application process: https://www.cancercare.on.ca/cms/One.aspx?portalId=1377&pageId=118921"	N/A	N/A	Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015
A&I	2015-09-10	2015-09-11	Internal	2015-10-13	Email breach. Unclear what PHI was included.	PHI was included in an internal e-mail from [Senior Analyst, Analytics & Informatics].	2015-09-11	From submitter: I deleted the e-mail and asked [the sender] to delete the e-mail as well all folders in	N/A - internal	2015-09-11	Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						[The email included an Excel spreadsheet attachment, which contained PHI. Email recipient was the Team Lead, Activity Level Reporting Program, Analytics & Informatics, who also submitted the breach.]		our inbox. As well I asked CCO Helpdesk to delete the copy that was in their mailbox. I informed [the sender] and she is aware that this was a miss on her part, she understands that PHI is not be sent via email.										
ATC - SETP	2015-09-16	2015-09-16	External	2015-10-16	Case file upload breach. Breached data included account number and MRN.	Unencrypted Case file upload contained account number and MRN- Breach of Policy (Data Sharing Agreement which advises to encrypt, though not PHI, sensitive information).	16-Sep-15	Delete data from McKesson Servers	16-Sep-15	23-Sep-15	Compliance Analyst, ATC & PO Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015
ATC - SETP	2015-09-16	2015-09-16	External	2015-10-16	Case file upload breach. Breached data included account number and MRN.	Unencrypted Case file upload contained account number and MRN- Breach of Policy (Data Sharing Agreement which advises to encrypt, though not PHI, sensitive information).	16-Sep-15	Delete data from McKesson Servers	16-Sep-15	17-Sep-15	Compliance Analyst, ATC & PO Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
CTO	2015-09-21	2015-09-21	External	2015-10-22	Email breach. Unclear what PHI was included.	[A decision support analyst at hospital.emailed CCO's helpdesk and ATC inboxes to inquire about a technical issue in the WTIS. This email contained a screenshot that included PHI.]	2015-09-21	[The associate support specialist deleted the email containing PHI from their inbox and deleted items folder. They sent an email to the original sender instructing them to delete the email from their sent items and deleted items folder.] Message to sender: "Please note that the following e-mail contained Personal Health Information (PHI). Please see the attached copy with the PHI removed. We have removed the e-mail from our Inbox and Deleted Items. Please do the same in your mailbox's Sent Items. A separate support request has been created to address your original issue .	2015-09-21	N/A	Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
								If you deem it necessary, please resend the original information, without PHI. You may use Interface Message ID or Waitlist Entry ID to reference a patient... "											
CPQI	2015-09-24	2015-09-24	Internal	2015-10-22	Email breach. Email attachment included patient name. The data source was clinical documentation sent to the program by the physician applicant.	PHI data was included in an attachment and unknowingly forwarded to several people. Original email was sent from [name omitted] (CCO) to 3 external reviewers and to [Program Manager, CPQI*] (CCO). [Program Manager] forwarded the request with the attachment to [Reimbursement Associate, PDRP] where the breach was identified. ...For the PET Access program, the Reimbursement Associate	2015-09-24	All parties were notified to delete the original email from their inbox and deleted folder. [The Reimbursement Associate has:] • Deleted the email from their inbox and deleted items folder • Emailed the sender, informed them that the email they had sent contained PHI, and instructed them to delete the email from their sent items and deleted items folders	2015-09-24	2015-09-24	Senior Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						normally sends out a redacted package to the clinical expert reviewers of the application and the relevant clinical documents (e.g., clinic notes, other imaging reports, pathology report, etc.). One instance of the patient name was missed. *Current title.												
CTO	2015-09-30	2015-09-30	External	2015-10-22	Email breach. Embedded screenshot included PHI (patient name, DOB and chart, and treatment information), plus sex information.	PHI data was included in an email by a user to STIP@cancercare.on.ca from hospital. It was regarding an outstanding Helpdesk ticket opened with STIP@cancercare.on.ca. ... Who received the PHI? STIP@cancercare.on.ca. How was it sent? Email Why was it sent? In reference to an open	2015-09-30	[Product Manager, Product Management, Cancer Services] emailed the sender (removing the screen shot), informed them that the email they had sent contained PHI. Original email was deleted from the inbox and deleted folder. Advised original user of breach and to not send PHI data on an email to CCO.	2015-09-30	2015-09-30	Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						ticket IR259583. What was the extent of PHI sent? Screenshot.												
CPQI	2015-10-08	2015-10-08	External	2015-10-13	Email breach. Data elements unavailable.	PHI was sent via email. [Group manager, SSO] was added to an email string involving a number of hospital participants. Several emails were received in this string over a short period of time before the PHI breach was identified. [Additional info from submitter]: The source of the PHI came from an external hospital who was asking questions about the OOC [out of country?] process for a patient. Someone looped [Group Manager, SSO] into the email thread.	2015-10-08	[Group Manager, SSO] notified the participants on the string and requested to be removed from the distribution list. The emails were deleted and then deleted from the deleted box in Outlook. [Additional info from submitter]: [Group Manager, SSO] noticed that there was PHI in it and replied all to request that they remove her from the thread as there is PHI in it that she is not authorized to see. She has deleted the emails (from her sent/deleted folders as well).	2015-10-08	2015-10-08	Senior Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015
ATC - SETP	2015-10-08	2015-10-16	External	2015-10-16	MRN and Account Number	Unencrypted Case File Uploaded to MPB by SETP facility	2015-10-18	Delete data from McKesson Servers	2015-10-19	2015-10-16	Compliance Analyst, ATC & PO Specialist	Policy breach	PE breach	No further recommendations possible. SETP escalates	Business Unit	2015-10-19	As per protocol in place by Privacy and Business Unit	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
														such breaches to the sites and management to ensure future mistakes are minimized while uploading files to CCO's service provider. Procedures are already in place. This breach is a breach of agreement which requires MRN to be encrypted however CCO doesn't have access to any databases with MRN.				
CPQI	2015-10-13	2015-10-13	External	2015-10-20	Email breach. The email included patient initials and chart numbers for 3 people.	PHI data was included in the body of an email to [reimbursement associate, Clinical Programs] from [name omitted] from Hospital.	N/A	[Reimbursement associate] has: • Deleted the email from their inbox and deleted items folder • Emailed the sender, informed them that the email they had sent contained PHI, and instructed them to delete the email from their sent items and deleted items folders	10/13/2015 Notified sender (their data).	2015-10-13	Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
ATC - SETP	2015-10-13	2015-10-16	External	2015-10-16	MRN and Account Number	Unencrypted Case File Uploaded to MPB by SETP facility	2015-10-18	Delete data from McKesson Servers	2015-10-19	2015-10-16	Compliance Analyst, ATC & PO Specialist	Policy breach	PE breach	No further recommendations possible. SETP escalates such breaches to the sites and management to ensure future mistakes are minimized while uploading files to CCO's service provider. Procedures are already in place. This breach is a breach of agreement which requires MRN to be encrypted however CCO doesn't have access to any databases with MRN.	Business Unit	2015-10-19	As per protocol in place by Privacy and Business Unit	2015
ATC - SETP	2015-10-13	2015-10-16	External	2015-10-16	MRN and Account Number	Unencrypted Case File Uploaded to MPB by SETP facility	2015-10-18	Delete data from McKesson Servers	2015-10-19	2015-10-16	Compliance Analyst, ATC & PO Specialist	Policy breach	PE breach	No further recommendations possible. SETP escalates such breaches to the sites and management to ensure future mistakes are minimized while uploading files to CCO's service provider. Procedures are already	Business Unit	2015-10-19	As per protocol in place by Privacy and Business Unit	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
														in place. This breach is a breach of agreement which requires MRN to be encrypted however CCO doesn't have access to any databases with MRN.				
CPQI	2015-10-22	2015-10-22	External	2015-10-27	Emailed data elements unavailable. [On further investigation: Patient name and demographic info as well as the fact that the patient was part of the Out of Country Cancer process (PHI)]	[Group manager, CPQI] received PHI via email from a physician at one of the cancer centres. The nature of the email was to request follow-up on the progress of an out-of-country request.	2015-10-22	The email was deleted from the Outlook. Follow up with the physician requested that PHI not be sent via email in future. [On follow-up, found out that data was deleted from both inbox and deleted folders.]	2015-10-22	2015-10-22	Senior Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015
CPQI	2015-10-22	2015-10-22	External	2015-10-27	Email breach. Data elements unavailable. [On further investigation: Patient name and demographic info as well as the fact that the patient was part of the Out of Country Cancer process (PHI)]	[Group manager, CPQI] received PHI via email from a physician at one of the cancer centres. The nature of the email was to request follow-up on the progress of an out-of-country request.	2015-10-22	The email was deleted from the Outlook. Follow up with the physician requested that PHI not be sent via email in future. [On follow-up, found out that data was deleted from both inbox and deleted folders. From staff:	2015-10-22	2015-10-22	Senior Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
								Physician was advised not to send us PHI.]										
ORN	2015-10-22	2015-10-22	External	2015-10-27	Fax breach. Faxed referral form contained PHI (patient name, address, DOB, HIN).	On Thursday, October 22nd CCO main reception at 620 received a fax (1 Outpatient Nephrology Referral Form) with PHI. The referral form is a tool developed by ORN for use by primary care providers when they are referring outpatients to a nephrologist in the hospital setting and/or in the community. On Monday November 2nd, the privacy office retrieved these form from the main reception at 620 University and contacted the [program manager, ORN] from the data and analytics team on November 3rd to re-direct the	11/16/2015 (Note: an electronic copy was deleted from H: drive on 11/8/2016.)	On November 16th [the business strategist] retrieved the fax from [the program manager] and contacted the primary care provider sender to 1) Inform of the breach, 2) confirm the forms are to be sent to a local nephrologist 3) confirm future referral forms are not to be sent to CCO/ORN. The form will be securely destroyed. A follow up fax was sent back to the sender reiterating the above steps, and the contact information for a local nephrologist. .. After communication with the sender, the form was securely destroyed. [Nov 16th]	11/16/2015 Notified sender via fax (their data).	2015-11-16	Senior Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						form to the appropriate ORN contact. [Program manager] retrieved the form from [senior privacy specialist, Legal and Privacy Office] on November 3rd. ...Business Strategist from the Early Detection and Prevention of Progression portfolio...confirmed that there was no ORN purpose for the data and that the faxes should be destroyed.		The ORN will also be modifying the form to include a disclaimer such as "do not fax/email this form to CCO/ORN" An electronic copy was deleted from H: drive on 11/8/2016.										
A&I	2015-10-30	2015-10-30	External	2015-11-03	Email breach. Data elements unavailable. [More information from ALR: From the looks of the attachments (before I deleted them) they had PHI containing Patient Chart Number, HIN (with Facility Number, and other non-direct	PHI was included in an e-mail to Informatics mailbox and [analyst, Data Assets] of CCO. The e-mail was sent to resolve a data submission issue [name omitted] that PMH was having while submitting PMH's ALR data to CCO. The e-mail was received by	2015-10-30	From submitter: We deleted the PHI content immediately we realized it was PHI from all CCO e-mails and advised the sender [name omitted] of PMH to delete at her end, the sender acknowledged that she deleted the PHI attachments.	2015-10-30	2015-10-30	Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
					PHI data elements).]	[analyst] and the informatics mailbox and forwarded to the ALR Team. The PHI was sent as an e-mail attachment.		[On follow-up, confirmed that the emails were deleted from both inboxes and deleted email folders.]										
PSC	2015-10-30	2015-10-30	External	2015-11-03	Email breach. The email contained a single patient name. [Note: on further investigation, it appears that the email referenced the patient's transplant, as well as patient sex and name of treatment facility.]	PHI data was included in an email to [business analyst, Strategy] and [group manager, health service provider] from [name omitted] at the Ministry of Health Out-of-Country office. The email was sent in an effort to communicate an urgent issue being experienced by stakeholders.	2015-10-30	• [Business analyst, Strategy] and [group manager, Regional Systemic Treatment Program] deleted the email from their inboxes and deleted item folders. • [Business analyst] called the sender, informed them that the email they had sent contained PHI, and instructed them to delete the email from their sent items and deleted items folders. • Sender is now aware to NOT send any emails with PHI to anyone at CCO	10/30/2015 Notified sender (their data).	2015-10-30	Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
PSC	2015-10-30	2015-10-30	External	2015-11-03	Email breach. The email contained a single patient name. [Note: on further investigation, it appears that the email referenced the patient's transplant, as well as patient sex and name of treatment facility.]	PHI data was included in an email to [business analyst, Strategy] and [group manager, health services provider] from [name omitted] at Hospital. The email was sent in an effort to communicate an urgent issue being experienced by stakeholders.	2015-10-30	• [Business analyst, Strategy] and [group manager, health services provider] deleted the email from their inboxes and deleted item folders. • [Business analyst] called the sender, informed them that the email they had sent contained PHI, and instructed them to delete the email from their sent items and deleted items folders. • Sender is now aware to NOT send any emails with PHI to anyone at CCO	10/30/2015 Notified sender (their data).	2015-10-30	Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015
CPQI	2015-10-30	2015-11-03	Internal	2015-11-10	Email breach. One patient first name was left unredacted.	[Reimbursement Associate, PDRP sent PHI to the PET reviewer panel of three individuals. It seems all PHI in the package was redacted except for the patient's	2015-11-02	[Reimbursement Associate deleted the email from their sent box, inbox, and deleted items box.] Email was sent to all the recipients of the original email to delete it from both	2015-11-02	2015-11-03	Senior Privacy Specialist	Privacy breach	PE breach	Privacy to connect with PDRP in early 2016 once CCO's proposed de-identification tool has been tested, to determine whether it will help reduce the rate of manual error	Business Unit & Privacy Specialist	N/A	See "Recommendations".	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						first name in one instance. A reviewer brought the omission to the Reimbursement Associate's attention.]		the inbox and deleted items as well. [1 reviewer confirmed deletion.]						in redactions.				
ATC - SETP	2015-11-05	2015-11-17	External	2015-11-17	MRN and Account Number	Unencrypted Cancellation File Uploaded to MPB by SETP Facility	2015-11-17	Delete data from McKesson Servers	2015-11-17	2015-11-17	Compliance Analyst, ATC & PO Specialist	Policy breach	PE breach	No further recommendations possible. SETP escalates such breaches to the sites and management to ensure future mistakes are minimized while uploading files to CCO's service provider. Procedures are already in place. This breach is a breach of agreement which requires MRN to be encrypted however CCO doesn't have access to any databases with MRN.	Business Unit	2015-11-17	As per protocol in place by Privacy and Business Unit	2015
ATC	2015-11-06	2015-11-06	External	2015-11-10	Email breach. Email contained MRN identifier for a patient.	PHI was included in an email chain between [service specialist, SD&M] and [hospital coordinator]	2015-11-06	Informed facility contact [hospital coordinator, name omitted] to delete the email from all email	11/6/2015 Notified sender (their data).	2015-11-16	Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						at hospital.. The email was received at 9am Friday, November 6, 2015 and was in relation to a call that took place the day before regarding the ALC designation of a patient. The coordinator at the hospital ([name omitted, email omitted]) sent in a follow-up email asking [service specialist] to review the patients wait list entry and included the MRN as the identifier rather than the waitlist entry ID for the patient. Service Specialist noticed the email had been placed in a sub-folder by another SS. When auctioning the email notice the PHI and directly went to Team Lead.		folders. This included the sent, inbox and deleted folders. Also deleted these from ATCSupport@cancercare.on.ca mailbox (all folders). Informed the Privacy Representative for the department as soon as the breach was noticed. ...A separate email was receive back from the facility confirming they had deleting the chain email. ...Confirmation email was provided to Privacy Rep.										

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
ORN	2015-11-06	2015-11-16	External	2015-11-17	Fax breach. The shipment notification form that was faxed to the main CCO reception line included study participant's study ID (letters and numbers) and a DOB as a secondary identifier. It also was attached to a lab requisition.	From submitter: A fax was sent by lab to the general fax line at 620 University (416-971-6888) instead of to the analytical laboratory. The fax was a shipment notification form... The purpose of the shipment notification form is to track study samples that are sent from lab collection centers to main laboratory for analysis as we cover the cost of this shipment through our research grant. The instructions on the shipment notification form clearly indicate that the fax should be sent to the lab fax line... We do not receive laboratory results via e-mail or fax from lab. They are mailed to us or	2015-11-17	[CCO reception informed a privacy specialist of the nature of the fax and handed the fax to her. The original fax was securely destroyed by placing it in one of CCO's secure shredding bins. The submitter, a research associate with the ORN, was summarily apprised.] [The research associate contacted a program manager at lab on 11/17/2015 to request that they remind lab staff not to send forms containing "identifiers such as birthdate" to the CCO main line. The correct fax number was attached to this communication, which was circulated via email to all patient collection	11/17/2015 Notified Gamma Dynacare (their tracking form).	2015-11-17	Senior Privacy Specialist	Policy breach	PE breach	See "containment measure". Privacy recommendations mirrored the actions of the business unit.	Business Unit & Privacy Specialist	2015-11-17	See "Recommendations".	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						downloaded via the secure eResults portal (?) in HL7 format.		centres on 11/18/2015.] Per submitter: We have communicated with lab several times in the past and asked that they only send faxes related to the study to our study fax line (1-855-222-8625).										
ATC - SETP	2015-11-09	2015-11-17	External	2015-11-17	MRN and Account Number	Unencrypted Cancellation File Uploaded to MPB by SETP Facility	2015-11-17	Delete data from McKesson Servers - CIO informed of recurring poor submission	2015-11-17	2015-11-17	Compliance Analyst, ATC & PO Specialist	Policy breach	PE breach	No further recommendations possible. SETP escalates such breaches to the sites and management to ensure future mistakes are minimized while uploading files to CCO's service provider. Procedures are already in place. This breach is a breach of agreement which requires MRN to be encrytpted however CCO doesn't have access to any databases with MRN.	Business Unit	2015-11-17	As per protocol in place by Privacy and Business Unit	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
A&I	2015-11-13	2015-11-13	External	2015-11-17	Email breach. Attachment contained HIN numbers.	PHI was included in an e-mail to Informatics mailbox of CCO. The e-mail was sent to inquire about the availability of reports for their August and September data for the ALR program. The e-mail was received by [Associate Analyst, Data Assets] through the informatics mailbox. The PHI was sent as an e-mail attachment and the data contained HINs.	2015-11-13	From submitter: We deleted the PHI content immediately we realized it was PHI from the CCO e-mail and advised the sender [name omitted] of Hospital to delete at her end, the sender acknowledged that she deleted the PHI attachments.	11/13/2015 Notified sender (their data).	2015-11-13	Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015
ATC	2015-11-24	2015-11-24	External	2015-12-01	Email breach. The email contained the patient's name, specified medical exam and other information pertaining to the patient.	[An email containing PHI was sent by an individual at Hospital to the CCO, ATC inbox, in order to resolve an issue with the WTIS application.]	2015-11-24	[IT analyst deleted the email from inbox and all other email folders, and notified the sender about the breach and how to purge their email. Contents of the notification: "Please note that the following e-mail contained Personal Health	11/24/2015 Notified sender (their data).	2015-11-25	Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
								Information (PHI). Please see the attached copy with the PHI removed. We have removed the e-mail from our Inbox and Deleted Items. Please do the same in your mailbox's Sent Items. A support request has been created to address your original issue < IR276069 >. If you deem it necessary, please resend the original information, without PHI. You may use Interface Message ID or Waitlist Entry ID to reference a patient. Please quote the subsequent request number so we can append the information to the appropriate request."]										

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
CTO	2015-12-03	2016-01-18	External	2016-03-02	Email breach. Email attachments included PHI - MRN numbers were included in the file names. The recipient saw 3 files with MRN in the names. The files were not opened to further verify the contents.	[PHI data was sent by hospital. to the ISAAC mailbox (isaac@cancercare.on.ca) in order to resolve an existing issue on December 3rd. The issue was that the sender was getting duplicate patient error while trying to enroll patients in November.] [Altogether 3 individuals manage the ISAAC mailbox and 1 other external contact was cc'd on the email, making 5 individuals who would have had access to the PHI that was breached. However, all individuals had permissions to view the PHI.]	2016-12-06	The email was deleted right away, and the user informed to do so as well from their inbox and deleted box. The user was informed of the PHI disclosure process at CCO and communicating it. The privacy specialist was emailed on January 18th. The delay in reporting resulted from confusion regarding the breach management process and who to contact within the Privacy team; this has since been resolved.	12/6/2016 Notified sender (their data).	2016-03-08	Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "containment measure".	2016
A&I	2015-12-04	2015-12-04	Internal	2015-12-08	SharePoint breach. Spreadsheet contained PHI such as name, DOB, HIN, address, phone number and test/case	[Data consisted of] data profiling performed on Cytology, Symptom Management and Person information. Spreadsheet was placed	2015-12-04	Notified the CCO lead [name omitted] immediately to confirm with [consultant] staff if the file contained	N/A	N/A	Group Manager, Privacy	Policy breach	PE and PR breach	N/A	Business Unit	N/A	See "Containment Measure".	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
					dates. Potentially two values of PHI for each sensitive attribute across the various tables. Not significant volume and not complete records. i.e. the Phone number would not be for the associated HIN and not for the associated name, so difficult to recombine.	on CCO's external SharePoint site with access only by CCO and [consultant] staff associated with the [Data Strategy Roadmap] project The file was only on the site for only a couple of hours before being removed. Was also on a CCO Laptop before being moved to CCO H: drive. File was opened by [Data Architect, Analytics and Informatics] using a CCO Laptop and the file was not saved. [Data included EDW, Wait Times and Screening data.]		real information or dummy values. The file was immediately removed from SharePoint while this was being assessed. It was confirmed as PHI. Confirmed copies of the file were only on the SharePoint site (removed) and CCO Laptop used by consultant. File moved from laptop to designated H drive. [Team lead, Privacy] notified of potential breach.										

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
ORN	2015-12-04	2015-12-04	External	2015-12-08	Fax breach. Form included PHI such as patient name, address, DOB, and HIN.	On December 4th 2015 CCO main reception at 620 received a fax (1 Outpatient Nephrology Referral Form) with PHI. The referral form is a tool developed by ORN for use by primary care providers when they are referring outpatients to a nephrologist in the hospital setting and/or in the community.	2015-12-22	On December 4th, the privacy office retrieved these forms from the main reception at 620 University and contacted...the Business Strategist from the Early Detection and Prevention of Progression portfolio of the ORN. The ORN confirmed that there was no ORN purpose for the data and that the faxes should be destroyed. ORN to identify the purpose for which they were received, and to advise to whom these should be directed. On December 7th, 2015 [Business Strategist, ORN] retrieved the fax from [name omitted], the Senior	12/18/2015 Notified sender (their data).	2015-12-04	Senior Privacy Specialist	Policy breach	PE breach	From the LPO 12/4/2015: "...Ensure that the faxes are re-directed appropriately and the sender's reminded that the forms are not to be faxed to the ORN. I would also welcome any suggestions as to how to further mitigate this risk. I understand that we have changed the wording on the form and asked the leadership to cascade down communications indicating the importance of using the updated form. Can we reiterate this? Is there another option we haven't tried?"	Business Unit & Privacy Specialist	N/A	See "Recommendations".	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
								Privacy Analyst and provided the form to [Senior Specialist] from the ORN team on December 17th to contact the referring physician's office and confirm next steps. On December 18th [the Senior Specialist] contacted the primary care provider sender to 1) Inform of the breach, 2) confirm the forms are to be sent to a local nephrologist 3) confirm future referral forms are not to be sent to CCO/ORN. The form will be securely destroyed. A follow up fax was sent back to the sender reiterating the above steps, and the contact information for a local nephrologist.										

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
								[Follow up phone call and e-mail with provider's office to confirm that referral package can be destroyed took place Dec 22nd.] The ORN has modified the form in the future to include a disclaimer such as "do not fax/email this form to CCO/ORN"										
ORN	2015-12-04	2015-12-04	External	2015-12-08	Fax breach. Form included PHI such as patient name, address, DOB, and HIN.	On December 4th 2015 CCO main reception at 620 received a fax (1 Outpatient Nephrology Referral Form) with PHI. The referral form is a tool developed by ORN for use by primary care providers when they are referring outpatients to a nephrologist in the hospital setting and/or in the community.	2015-12-22	On December 4th, the privacy office retrieved these forms from the main reception at 620 University and contacted...the Business Strategist from the Early Detection and Prevention of Progression portfolio of the ORN. The ORN confirmed that there was no ORN purpose for the data and that the faxes should	12/18/2015 Notified sender (their data).	2015-12-04	Senior Privacy Specialist	Policy breach	PE breach	From the LPO 12/4/2015: "...Ensure that the faxes are re-directed appropriately and the sender's reminded that the forms are not to be faxed to the ORN. I would also welcome any suggestions as to how to further mitigate this risk. I understand that we have changed the wording on the form and asked the leadership to cascade down communicati	Business Unit & Privacy Specialist	N/A	See "Recommendations".	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
								be destroyed. ORN to identify the purpose for which they were received, and to advise to whom these should be directed. On December 7th, 2015 [Business Strategist, ORN] retrieved the fax from [name omitted], the Senior Privacy Analyst and provided the form to [Senior Specialist] from the ORN team on December 17th to contact the referring physician's office and confirm next steps. On December 18th [the Senior Specialist] contacted the primary care provider sender to 1) Inform of the breach, 2) confirm the forms are to be sent to a local						ons indicating the importance of using the updated form. Can we reiterate this? Is there another option we haven't tried?"				

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
								nephrologist 3) confirm future referral forms are not to be sent to CCO/ORN. The form will be securely destroyed. A follow up fax was sent back to the sender reiterating the above steps, and the contact information for a local nephrologist. [Follow up phone call and e-mail with provider's office to confirm that referral package can be destroyed took place Dec 22nd.] The ORN has modified the form in the future to include a disclaimer such as "do not fax/email this form to CCO/ORN"										
CPQI	2015-12-08	2015-12-08	External	2016-01-08	Email breach. The email included patient initials and chart number.	PHI data was included in the body of an email to [Reimbursement Associate, CPQI] from [name	2015-12-08	[The Reimbursement Associate has:] • Deleted the email from their inbox and deleted items folder	12/8/2015 Notified sender (their data).	2015-12-09	Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						omitted] from The Scarborough Hospital. [The email was sent as a reference to a claim in eClaims.]		• Emailed the sender, informed them that the email they had sent contained PHI, and instructed them to delete the email from their sent items and deleted items folders										
ATC - SETP	2015-12-09	2015-12-15	External	2015-12-15	MRN and Account Number	Unencrypted Cancellation File Uploaded to MPB by SETP Facility	2015-12-15	Delete data from McKesson Servers	2015-12-15	2015-12-15	Compliance Analyst, ATC & PO Specialist	Policy breach	PE breach	No further recommendations possible. SETP escalates such breaches to the sites and management to ensure future mistakes are minimized while uploading files to CCO's service provider. Procedures are already in place. This breach is a breach of agreement which requires MRN to be encrypted however CCO doesn't have access to any databases with MRN.	Business Unit	2015-12-15	As per protocol in place by Privacy and Business Unit	2015
ATC - SETP	2015-12-09	2015-12-15	External	2015-12-15	MRN and Account Number	Unencrypted Cancellation File	2015-12-15	Delete data from	2015-12-15	2015-12-15	Compliance Analyst,	Policy breach	PE breach	No further recommendations	Business Unit	2015-12-15	As per protocol in place by	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						Uploaded to MPB by SETP Facility		McKesson Servers			ATC & PO Specialist			possible. SETP escalates such breaches to the sites and management to ensure future mistakes are minimized while uploading files to CCO's service provider. Procedures are already in place. This breach is a breach of agreement which requires MRN to be encrytpted however CCO doesn't have access to any databases with MRN.			Privacy and Business Unit	
CPQI	2015-12-15	2015-12-15	Internal	2016-01-08	Email breach. The report included patient names and HINs for 3 patients.	PHI data was included in an attachment from [Reimbursement Associate, PDRP] to [another reimbursement associate and a program manager in PDRP]. ...The report was a summary of CCO NDFP audit findings.	2015-12-15	[The Reimbursement Associate has:] • Deleted the email from their inbox and deleted items folder • Skyped [the two recipients], and instructed them to delete the email from their inbox and deleted items folders	N/A	2015-12-15	Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
P&CC	2015-12-29	2015-12-29	Internal	2016-01-08	Shared drive breach. The report contained PHI such as DOB, patient ID number; also included sex and age of the patient and the dictating physician.	PHI data was not redacted from one patient's cancer imaging report before being sent for assessment. The report was pulled by [Cancer Screening] analysts, and only part of the report was redacted of PHI and stored on the H: drive. [Program Analyst, Cancer Imaging Program] pulled the report from the H: did not realize there was PHI still visible, and assigned it to [Student Analyst]. The report was put on the P: for [Student Analyst] to access.	2015-12-29	[Student Analyst] emailed [Program Analyst] on December 29, 2015 and informed her that he could see PHI on one report. [Program Analyst] went into the P: where the report was, and redacted it completely of the PHI, and saved the report over the original one. An email was then sent to [Team Lead, Privacy].	N/A	2015-12-29	Group Manager, Privacy	Policy breach	PE and PR breach	The CCO analyst...was reminded to be careful in ensuring PHI has been removed from the cancer staging cases before making them available to the CCO auditor for analysis.	Business Unit	2016-01-18	N/A	2015
A&I	2015-12-31	2016-04-13	Internal and External	2016-04-13	Email breach. Attachment contained PHI (HINs, postal codes, DOB attached to lung cancer information) for 13,151 individuals from the	[PHI was provided by a member of Analytics & Business Intelligence in an Excel report to the DAP in P&RP. The report was a DAP vs non-DAP lung	2016-04-19	[4/11/2016 - 4/19/2016: All 9 individuals deleted the email.] Team Lead, Analytics & Business Intelligence reviewed other reports	N/A (internal)	2016-05-03	Senior Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "containment measure".	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
					DAP and 21,847 non-DAP individuals.	cancer analysis that was requested by the DAP, and was intended to contain aggregate data only. Although the original analyst who created the report deleted the PHI data from the report, clicking on one of the pivot tables still revealed PHI. The DAP later emailed the Excel document within their team, as did Analytics & Business Intelligence within their team. Altogether 4 individuals in P&RP and 5 individuals from the CTO had the PHI in their emails (same version of the PHI). The file did not go to external recipients from either the Analytics & Business Intelligence teams or the DAP team.]		from the team (mostly aggregate) and ensured that the error made was not also applied to other reports. The Team Lead advised other members of the team not to use PHI as the data source for pivot tables. Thereafter, other team members checked their own files for this issue, and did not raise any new concerns.									

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						The Excel file was saved in the P: drive from December 27, 2015 until April 13, 2016.												
ATC - SETP	2016-01-08	2016-01-15	External	2016-01-18	MRN and Account Number	Unencrypted Cancellation File Uploaded to MPB	2016-01-18	Delete data from McKesson Servers (CCO's service provider)	2016-01-18	2016-01-18	Compliance Analyst, ATC & PO Specialist	Policy breach	PE breach	No further recommendations possible. SETP escalates such breaches to the sites and management to ensure future mistakes are minimized while uploading files to CCO's service provider. Procedures are already in place. This breach is a breach of agreement which requires MRN to be encrypted however CCO doesn't have access to any databases with MRN.	Business Unit	2016-01-18	As per protocol in place by Privacy and Business Unit	2016
A&I	2016-01-13	2016-01-15	External	2016-01-26	Email breach. Email attachment included PHI (patient DOB; "pathkey ID", not sure if PHI), plus gender and other fields,	RE: Data Disclosure Request...PHI was sent via email from [name omitted] from University. The excel file containing patients	2016-01-15	From submitter, Associate Analyst, Data Disclosure: I deleted the email from my inbox and deleted items box. I called the sender and	1/15/2016 Notified sender.	2016-01-18	Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
					for 40 records.	DOB...was included as an attachment. The sender was seeking more information about the missing fields in the excel file. [On investigation: Originally CCO disclosed 519 records to the requestor in 2012. The requestor's file contains 40 of those 519 records. It was not University's own cohort, but a data request CCO provided.]		advised them to delete the email from their sent box and deleted items folder.										
P&CC	2016-01-14	2016-01-14	External	2016-01-14	Unclear. Pathology report contained PHI.	PHI was sent to CCO - method unclear. Form missing.	N/A	N/A	N/A	N/A	Privacy Specialist	N/A	Unclear	N/A	Business Unit	N/A	See "Containment Measure".	2016
ATC	2016-01-25	2016-01-26	Internal and External	2016-02-02	iPort Access breach.	[From submitter, Group Manager, Business Intelligence:] In our internal review of user access on iPort Access (MicroStrategy tool hosting ATC reports), we observed that four external	2016-01-26	[From submitter:] 1) Access to iPort Access was revoked for the four external users. [Non-containment follow-up:] We did further analysis and confirmed that no breach happened.	N/A Suspected breach.	2016-03-16	Privacy Specialist	Policy breach	PE breach	Final recommendations for all iPort and iPort Access suspected privacy breaches that took place between Dec 2015 and Jan 2016 were sent on Mar 16, 2016 to key internal stakeholders.	Business Unit & Privacy Specialist	N/A	See "Recommendations".	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						users had access to certain reports with PHI data for all facilities. (Three users under ER iPort Access project...and one user...under WTIS iPort Access project.) The users would have to log into iPort Access (MicroStrategy tool hosting ATC reports) to access these reports. [Although no internal CCO users of iPort Access appeared to have received unauthorized access to PHI, internal process gaps contributed to the incidents.]		a. We collected and analyzed user report execution statistics from iPort Access (MicroStrategy platform). b. From that the statistics, we confirmed that the users in question did not execute [i.e. access] any reports with PHI data. A detailed description of this breach has been submitted to LPO senior management.						Resolutions: 1) • BI to validate all user profiles involved in iPort Access breaches, as well as all CCAC profiles. • ATC program to advise BI development team when to re-enable user access. • Clinical Manager, ALC & MHA to confirm that profiles for CCAC users do not include access to PHI. • BI to consult with other programs using iPort and iPort Access to validate users. 2) • Revisit the resolutions from the June 2015 breach and determine whether they or a comparable alternative can be implemented. • Review the process of request submission and approval for both iPort				

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
														and iPort Access; consult with Enterprise Information Security Office to ensure the process is secure and consistent with CCO's policies for accessing PHI. The review and approval processes for iPort and iPort Access are currently being documented through the "OneID Process Redesign" initiative; this may provide an opportunity for improvement."				
ATC	2016-01-26	2016-01-26	Internal and External	2016-02-02	iPort Access breach.	On Tuesday, January 26, 2016 8:41 AM, ...(Director of Decision Support) at HNHB CCAC sent an email to ATC Support & ...(Group Manager, MH & ALC) requesting access for her staff to iPort Access with PHI. [The director] mentioned	2016-01-26	...(Lead, Business Intelligence) was engaged and he liaised with the BI development team...to disable the user accounts of [the two individuals] until the investigation was completed. These accounts were confirmed to be disabled	N/A Suspected breach.	2016-03-16	Privacy Specialist	Policy breach	PE breach	Final recommendations for all iPort and iPort Access suspected privacy breaches that took place between Dec 2015 and Jan 2016 were sent on Mar 16, 2016 to key internal stakeholders. Resolutions: 1) • BI to validate all	Business Unit & Privacy Specialist	N/A	See "Recommendations".	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						"Two current users - [names omitted] have had access to patient level data for ALC for several years." ...There was no PHI included in the email, just the statement that they said they had access to PHI. CCAC user profiles do not have PHI access or RSA tokens, therefore an investigation was requested by [the group manager]. [Although no internal CCO users of iPort Access appeared to have received unauthorized access to PHI, internal process gaps contributed to the incidents.]		by Tue 1/26/2016 3:37 PM by...(technical specialist, IT Ops). A detailed description of this breach has been submitted to LPO senior management.						user profiles involved in iPort Access breaches, as well as all CCAC profiles. • ATC program to advise BI development team when to re-enable user access. • Clinical Manager, ALC & MHA to confirm that profiles for CCAC users do not include access to PHI. • BI to consult with other programs using iPort and iPort Access to validate users. 2) • Revisit the resolutions from the June 2015 breach and determine whether they or a comparable alternative can be implemented. • Review the process of request submission and approval for both iPort and iPort Access; consult with Enterprise Information				

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
														Security Office to ensure the process is secure and consistent with CCO's policies for accessing PHI. The review and approval processes for iPort and iPort Access are currently being documented through the "OneID Process Redesign" initiative; this may provide an opportunity for improvement."				
CTO	2016-02-01	2016-02-08	External	2016-02-09	Email breach. The PHI involved was a single patient's DOB, HIN, and chart number.	PHI Data was included in an email to helpdesk@cancercare.on.ca from [name and description omitted] of the Hospital. The email was sent in an effort to resolve an issue the sender was having with WTIS Duplicate Patient issue.	2016-02-08	[The recipient, helpdesk]: Deleted attachment from ticket Deleted email from ticket Informed the sender of the PHI data that was sent... Message sent to the original PHI sender: "Please note that the following e-mail contained Personal Health Information	2/8/2016 Notified sender (their data).	2016-02-09	Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
								(PHI). Please see the attached copy with the PHI removed. We have removed the e-mail from our Inbox and Deleted Items. Please do the same in your mailbox's Sent Items. A support request has been created to address your original issue [ID omitted]. If you deem it necessary, please resend the original information, without PHI. You may use Interface Message ID or Waitlist Entry ID to reference a patient. Please quote the subsequent request number so we can append the information to the appropriate request. "										
PSC	2016-02-03	2016-02-04	External	2016-02-09	Email breach. The PHI involved was a single patient name.	PHI data was included in an email to [4 CCO staff members from across	2016-02-04	• [The 4 CCO recipients] deleted the email from their inboxes	2/4/2016 Notified sender (their data).	2016-01-18	Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						People, Strategy and Communications and CPQI] from [name omitted] at the Hospital. The email was sent in an effort to provide an update on the timing of information flow, and patient information was included inadvertently.		and deleted item folders. • [The submitter (Specialist, People, Strategy and Communications)] contacted the sender, informed them that the email they had sent contained PHI, and instructed them to delete the email from their sent items and deleted items folders. • Sender is now aware to NOT send any emails with PHI to anyone at CCO.										
CTO	2016-02-08	2016-02-08	External	2016-03-02	Email breach. The email contained 1 patient name.	[A user at a physician's office sent an inquiry to the ATC inbox asking after a patient's information that was entered incorrectly into the ATC wait times information system. The email contained not only the permissible wait time number related to	2016-02-08	[The recipient created a helpdesk ticket without the patient's name, attached the email to the ticket with the patient's name being omitted, and sent an email to the submitter in regards to the privacy breach. The original email was	2/8/2016 Notified sender (their data).	2016-03-04	Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						the patient, but also the patient's name.]		deleted and purged.] Message sent to the original PHI sender: "Please note that the following e-mail contained Personal Health Information (PHI). Please see the attached copy with the PHI removed. We have removed the e-mail from our Inbox and Deleted Items. Please do the same in your mailbox's Sent Items. ... If you deem it necessary, please resend the original information, without PHI. You may use Interface Message ID or Waitlist Entry ID to reference a patient. Please quote the subsequent request number so we can append the information to the appropriate request."										

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
ATC - SETP	2016-02-10	2016-02-12	External	2016-02-17	MRN and Account Number	Unencrypted Case & Cancellation Files Uploaded to MPB	2016-02-17	Delete data from McKesson Servers	2016-02-17	2016-02-17	Compliance Analyst, ATC & PO Specialist	Policy breach	PE breach	No further recommendations possible. SETP escalates such breaches to the sites and management to ensure future mistakes are minimized while uploading files to CCO's service provider. Procedures are already in place. This breach is a breach of agreement which requires MRN to be encrypted however CCO doesn't have access to any databases with MRN.	Business Unit	2016-02-17	As per protocol in place by Privacy and Business Unit	2016
ATC - SETP	2016-02-10	2016-02-12	External	2016-02-17	MRN and Account Number	Unencrypted Case & Cancellation Files Uploaded to MPB	2016-02-17	Delete data from McKesson Servers	2016-02-17	2016-02-17	Compliance Analyst, ATC & PO Specialist	Policy breach	PE breach	No further recommendations possible. SETP escalates such breaches to the sites and managemen	Business Unit	2016-02-17	As per protocol in place by Privacy and Business Unit	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
														t to ensure future mistakes are minimized while uploading files to CCO's service provider. Procedures are already in place. This breach is a breach of agreement which requires MRN to be encrypted however CCO doesn't have access to any databases with MRN.				
ATC - SETP	2016-02-10	2016-02-29	External	2016-02-29	MRN and Account Number	Unencrypted patient numbers captured in the Procedure Code mapping table	2016-02-29	Delete data from McKesson Servers - mapping table. Work scheduled for Monday March 14/16.	2016-02-29	2016-02-29	Senior Business Analyst(SETP) & McKesson	Policy breach	PE breach	No further recommendations possible. SETP escalates such breaches to the sites and management to ensure future mistakes are minimized while uploading files to CCO's service provider. Procedures are already in place. This breach is a breach of agreement which requires MRN to be encrypted however	Business Unit	2016-02-29	As per protocol in place by Privacy and Business Unit	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
														CCO doesn't have access to any databases with MRN.				
CPQI	2016-02-24	2016-02-24	External	2016-03-07	Email breach. The document attached to the email contained the name and HIN of the patient for which a genetic testing application was denied through the Out of Country Program.	[From submitter, Manager, Pathology and Laboratory Medicine Program:] PHI was included in an email that I received from a pathologist at Hospital. . The email was sent to highlight the consequences of recent Ministry policy decisions impacting access to genetic testing for patient. The document was a copy of a letter from the Ministry indicating that a request for genetic testing is being denied through the Out of Country Program as testing is available in Ontario.	2016-02-24	[From the submitter:] • I deleted the email from their inbox and deleted items folders. •I emailed the sender, informed them that the email they had sent contained PHI, and instructed them to delete the email from their sent items and deleted items folders.	2/24/2016 Notified sender (their data).	2016-02-24	Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
CTO	2016-02-24	2016-02-29	External	2016-03-02	Email breach. The email attachment contained 1 chart number.	[A user at Hospital sent an inquiry to the CCO helpdesk inbox as they were having difficulty opening data in OPIS. The email contained 2 screenshots attachments; when the email first arrived in the helpdesk inbox, the first attachment was viewed and the request was deemed to be a question for the STIP (Systemic Treatment Information Program) Department. The email went to the STIP inbox, where the second attachment was opened - this second attachment contained a patient chart number. Consequently, the email was forwarded back to helpdesk, where it was treated as a privacy breach.]	2016-02-29	[The email was deleted and a ticket routed to SCM (?) admin for purging. A new ticket was created without PHI data. The user who sent the email was notified via email of the breach.] Message sent to the original PHI sender: "Please note that the following e-mail contained Personal Health Information (PHI). Please see the attached copy with the PHI removed. We have removed the e-mail from our Inbox and Deleted Items. Please do the same in your mailbox's Sent Items. ... If you deem it necessary, please resend the original information, without PHI. Please quote the subsequent request	2/29/2016 Notified sender (their data).	2016-03-04	Privacy Specialist	Privacy breach	PE breach	Verified that the STIP inbox did not receive an email with the PHI.	Business Unit	N/A	N/A	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
								number so we can append the information to the appropriate request."										
CTO	2016-02-25	2016-02-25	External	2016-03-02	Email breach. Email does not contain any direct patient identifiers, but does include the name of the patient's spouse and payment information for the patient.	[PHI was sent from an acquaintance of the patient. Email requested guidance on recouping costs associated with hospital stay. The email address of the user and his signature are clearly visible. The content of the email contains no reference to patient name, hospital or treatment.]	N/A	[No actions taken.]	N/A	2016-02-26	Privacy Specialist	Privacy breach	PE breach	Privacy specialist provided the following email back to the submitter: "Given that the email in question contains only identifiers for the sender and not the patient, and that the inquiry itself is unclear, here are my recommendations from a Privacy perspective: 1. Prior to responding to the sender, double check that you are definitely not the correct line of business/do not have a contact for inquiries regarding payment eligibility. Unfortunately this is something that Privacy cannot advise on, but your	Business Unit & Privacy Specialist	N/A	See "Recommendations".	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
														program area may have more information. 2. Once the above has been confirmed, respond to the sender in a new thread, letting them know that their original email will be treated as a breach of privacy for the patient involved, and advising them that email is not a secure method of transferring personal health information. Recommend to the requestor that they delete the email from their inbox and deleted emails folder. Please add that, given the limited information provided, we are unable to advise on the appropriate contact for their original inquiry, and will be closing this request without opening a ticket.				

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
														You may BCC the LPO inbox on this exchange for our records. 3. Delete the email from the ATC inbox and deleted emails folder immediately following step 2 and let me know once this is done. I would not recommend printing a physical copy of the email, but if you must do this for business reasons per 1), let me know before executing 3) and we can discuss further. This is a fairly conservative approach, as there is no direct identifying information for the patient within the email, but we do acknowledge that other information in the email may make the patient more identifiable under the				

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
														circumstances..." Update 3/16/2016: The submitter confirmed that the original sender has been redirected to the Contact Centre,				
CTO	2016-03-02	2016-03-18	Internal	2016-03-23	Email breach. Submitter believes the emails contained approx. 10 MRNs, and no other patient identifiers.	[PHI data was sent by IT Operations via email to 2 internal recipients, on two separate occasions. The data were requested by the Product Management team to decipher error messages for Hospital in the ISAAC exception database. The error messages contained an account number, which Product Management assumed was a site-specific account number. However upon investigation, it was revealed that the site had	2016-03-15	[Product manager asked all staff involved in sending and receiving the emailed PHI to delete it from their inboxes, deleted emails, and cache. The staff confirmed that the emails had been deleted.]	N/A - internal	2016-03-17	Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						embedded MRN in their error message, not the site number. A product manager in CTO - one of the recipients - eventually identified the breach and notified Privacy.]												
CTO	2016-03-07	2016-03-07	Internal	2016-03-07	Shared drive breach. PHI was found in P:\Informatics\NACRS. The PHI was NACRS data only and included 61 files in a combination of .txt, .xls, and .csv formats. The files contained approximately 440,000 records. Difficult to ascertain data elements as columns are not clearly labelled; however "OHIP billing number" is included in some files.	[On Mar 7th, during regular work, Senior Data Architect noticed that there was PHI on the P: drive in P:\Informatics\NACRS. Storing PHI on the P: drive contravenes CCO policy.]	2016-04-20	Mar 7th: Director of Technology Services informed the Senior Data Architect that the H: drive should be the only file share used for PHI. Director of Technology Services will share the information with the PHI Access Working Group for discussion. Director of Technology Services also informed the Director of Data Assets, whose team worked with IT Service Desk to remove the PHI from the P: drive. All files were deleted from the P: drive by the end of the date	N/A Suspected breach.	2016-04-20	Privacy Specialist	Policy breach	PE breach	Recommendations for all March shared drive breaches were shared with stakeholders 4/4/2016. 1) Data Assets will delete the "NACRS" and "NACRS_OCR" folder contents from the H: drive, and delete the "MYF" folder contents from the P: drive. 2) The EISO will ensure that any PHI that may have been backed up and sent to offsite storage is permanently deleted. 3) Analytics and Informatics will remind CCO staff who have access to	Business Unit & Privacy Specialist	N/A	See "Recommendations".	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
								of discovery, and a copy of the files is now being maintained in H:\Informatics\CIHI Unfiltered File\NACRS files. Due to H: drive permissions issues, the files first had to be moved to a P: drive location restricted to Data Assets team members (P:\Informatics\Data Management\Data Operations\20. Data Assets Operations Manual and Contact List\For Annum) before they could be deleted from the P: drive. The relocated files were deleted from the H: drive as of Apr 20th, 2016 after an investigation revealed that they were not being used.						the P:\Informatics folder to engage the LPO if they suspect that there may be PHI on the P: drive, and to double check that there is no PHI in the P:\Informatics subfolders that they can access.				

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
ATC - SETP	2016-03-08	2016-03-10	External	2016-03-10	MRN and Account Number unencrypted and full data set sent via email	Data submission file was sent via email to help answer questions about reporting	2016-03-10	Email recipients were advised to delete attachment and empty recycling bin on their computer	2016-03-10	2016-03-10	Senior Business Analyst(SETP) & McKesson	Policy breach	PE breach	No further recommendations possible. SETP escalates such breaches to the sites and management to ensure future mistakes are minimized while uploading files to CCO's service provider. Procedures are already in place. This breach is a breach of agreement which requires MRN to be encrypted however CCO doesn't have access to any databases with MRN.	Business Unit	2016-03-10	As per protocol in place by Privacy and Business Unit	2016
A&I	2016-03-09	2016-03-10	Internal	2016-03-10	Shared drive breach. PHI was found in P:\Informatics\NACRS_OCR. The two types of file are Excel and SAS dat files. In the Group Manager's opinion, SAS files are likely to be duplicates with Excel files. There are 102 files	[On March 9, the Group Manager, Cancer Registry was informed about files with PHI under P:\Informatics\NACRS. When she attempted to review the files, she noticed another directory just below it P:\Informatics\NACRS_OCR, which	2016-04-07	[The Group Manager moved all files except one to her personal directory on H: drive - could not move this last file as it requires administrator privileges, so it was deleted directly from the P:\Informatics location instead. The group	N/A Suspected breach.	2016-04-07	Privacy Specialist	Policy breach	PE breach	Recommendations for all March shared drive breaches were shared with stakeholders 4/4/2016. 1) Data Assets will delete the “NACRS” and “NACRS_OCR” folder contents from the H: drive, and delete the “MYF” folder	Business Unit & Privacy Specialist	N/A	See "Recommendations".	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
					and 2 subfolders (Group Manager declined to look into the folders in detail). Group Manager declined to look into the files to ascertain the number of records. However, she is reasonably certain that "a couple of the excel files have PHI in them", and since the "dat" files are believed to be redundant, they likely also contain PHI. In addition to these files, one Excel file still in P:\Informatics\NACRS was encrypted - could not identify contents - and was consequently deleted. At least in some files, the data appears to contain HIN, diagnosis date, and type of cancer. The files were	contained additional PHI. She contacted the Data Assets Team Lead, who followed up with a privacy specialist. Storing PHI on the P: drive contravenes CCO policy.]		manager then deleted the relocated files from her H: drive directory on Apr 7th, 2016.]							contents from the P: drive. 2) The EISO will ensure that any PHI that may have been backed up and sent to offsite storage is permanently deleted. 3) Analytics and Informatics will remind CCO staff who have access to the P:\Informatics folder to engage the LPO if they suspect that there may be PHI on the P: drive, and to double check that there is no PHI in the P:\Informatics subfolders that they can access.				

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
					last modified 2007-2009 for the most part.													
ATC - SETP	2016-03-09	2016-03-10	External	2016-03-10	Error report for data submission was sent via email and this contained a complete SETP data set, MRN and Account Numbers were encrypted	Error report for data submission was sent via email and this contained a complete SETP data set, MRN and Account Numbers were encrypted	2016-03-10	Email recipients were advised to delete attachment and empty recycling bin on their computer	2016-03-10	2016-03-10	Senior Business Analyst(SETP) & McKesson	Policy breach	PE breach	No further recommendations possible. SETP escalates such breaches to the sites and management to ensure future mistakes are minimized while uploading files to CCO's service provider. Procedures are already in place. This breach is a breach of agreement which requires MRN to be encrypted however CCO doesn't have access to any databases with MRN.	Business Unit	2016-03-10	As per protocol in place by Privacy and Business Unit	2016
CTO	2016-03-10	2016-03-10	External	2016-03-10	Email breach. Email included PHI - patient's full name, DOB and chart number. Submitter	[PHI data was included in an email to helpdesk from an applications analyst at hospital.The sender	2016-03-10	[From submitter:] I have deleted the screen shots that contain the PHI, have forwarded incident to	3/10/2016 Notified sender (their data).	2016-03-22	Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
					could not recall whether health information was attached.	provided screen shots for clear description of issue (question re: drug information in OPIS). Picture contained patient's full name, date of birth and chart number.]		appropriate support group. Also notified sender that they should delete the screen shots from their sent mail. [Message to sender: "Please note that your original e-mail contained Personal Health Information (PHI) and we have subsequently removed the PHI from the email body below. We have also permanently deleted the e-mail from our Inbox and Deleted Items. Please do the same in your mailbox's Sent Items and Deleted Items. ...If you deem it necessary, please resend the original information, without PHI. Please quote the support request number above so we can append the information										

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
								to the appropriate request."]										
CTO	2016-03-14	2016-03-14	Internal and External	2016-03-16	Email breach. Email contained an unredacted DOB for one patient. Update 3/15/2016: Subsequent emails in the discussion with Privacy also contained PHI. Update 3/23/2016: In addition to the unredacted DOB, there were a number of suspicious looking names and dates in the email. Privacy was able to confirm with the original sender that the HL7 data does not constitute personal health information or patient information. The names enclosed may be the names of persons who	[The inboxes ATC@cancercare.on.ca and ATCSupport@cancercare.on.ca received an email from a patient care information coordinator at Hospital. The email contained a screen shot detailing an issue with the Wait Times Information System. Within one of the screen shots the DOB of the patient was not blacked out.] Update 3/15/2016: After multiple follow-up emails, it came to the Privacy Specialist's attention that the PHI was not appropriately redacted and can still be seen in the follow-up emails between	2016-03-15	[Associate Support Specialist monitoring the ATC inbox deleted the screen shot from the email and sent notification to the sender of the breach. Ticket was created and assigned to appropriate support group. The same individual also notified ATCSupport personnel so that the email could be deleted from their side.] Email message: "Please note that your original e-mail contained Personal Health Information (PHI) and we have subsequently removed the PHI from the email body below.	3/15/2016 Notified sender (their data).	2016-03-15	Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
					entered the info into WTIS.	herself, the Associate Support Specialist responsible for monitoring the ATC inbox, and the original sender.		We have also permanently deleted the e-mail from our Inbox and Deleted Items. Please do the same in your mailbox's Sent Items and Deleted Items. ...If you deem it necessary, please resend the original information, without PHI. You may use Interface Message ID or Waitlist Entry ID to reference a patient. Please quote the support request number above so we can append the information to the appropriate request." Update 3/15/2016: in regards to the fact that the PHI was not properly redacted during containment, the Privacy Specialist contacted the Associate Support										

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
								Specialist and notified him of the fact, and provided additional containment measures. These included: 1. Resending the original email notification to the sender, with the PHI properly redacted. 2. Asking the sender to delete all emails containing the PHI from her sent box, inbox, and deleted emails folder. If the email was forwarded to anyone else (e.g., to inquire about the definition of PHI), the sender will be asked to pass the same message to them. 3. Double checking their own inbox and the ATC inbox, and deleting from their sent box, inbox and deleted emails folder any emails										

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
								containing the screenshot exposing PHI.										
CTO	2016-03-18	2016-03-21	Internal	2016-03-23	Email breach. PHI included name, HIN, gender, and DOB for one person. The PHI is a sample record used by the Freedom of Information (FOI) project. It is normally saved as a PDF on the secure H: drive. The project team is developing SQL queries based on this sample record.	[The submitter, a developer on the FOI project, was attempting to clarify a technical requirement about how to develop SQL queries. In the process, the developer sent an email to CCO's Enterprise Data Warehouse team - 6 recipients - and accidentally enclosed PHI. The email containing PHI was discovered immediately after it was sent.] [All those who received the PHI were authorized to view the PHI; they are either ETL developers	2016-03-18	[The EDW team was requested to delete this email from their inbox, sent items, and deleted items folders. All members from CCO EDW team deleted the email.]	N/A - internal	2016-03-21	Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						or data architects.]												
CTO	2016-03-22	2016-03-22	External	2016-03-29	Email breach. PHI contained patient name, the medical service they received, the hospital in which they received the procedure, and the name of the doctor who performed the procedure.	[The ATC inbox received and email that contained a screen shot containing PHI. The email was sent by an OR (?) booking clerk from hospital.in an attempt to trouble shoot an issue she was facing.]	2016-03-22	[The Associate Support Specialist for the ATC inbox deleted the screenshot from the email and notified the user of the breach.] Message to sender: "Please note that your original e-mail contained Personal Health Information (PHI) and we have subsequently removed the PHI from the email body below. We have also permanently deleted the e-mail from our Inbox and Deleted Items. Please do the same in your mailbox's Sent Items and Deleted Items. ...If you deem it necessary, please resend the original information, without PHI.	3/22/2016 Notified sender (their data).	2016-03-22	Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
								You may use Interface Message ID or Waitlist Entry ID to reference a patient. Please quote the support request number above so we can append the information to the appropriate request."										
A&I	2016-03-23	2016-03-23	Internal	2016-03-23	Shared drive breach. Multiple file types are involved, and some were restricted. However, files that could be opened contained the following columns: Center, Fiscal Year, "MRN", Visit Date, NHPIP Codes, Description, New Act Code, New Description, New Unit, AC, Completion Flag, Completion Comment, Assigned Course, Decision Rule, Course ID, Course Span, Start	[On March 23rd, the team lead, Cancer Registry found PHI in P:\Informatics\MYF. Storing PHI on the P: drive contravenes CCO policy.]	2016-04-20	[The team lead notified the group manager, Cancer Registry and the appropriate privacy specialist. Privacy specialist first recommended relocation of the files to the H: drive, then amended the recommendation to deletion of the files. All files associated with P:\Informatics\MYF were deleted as of Apr 20th, 2016.]	N/A Suspected breach.	2016-04-20	Privacy Specialist	Policy breach	PE breach	Recommendations for all March shared drive breaches were shared with stakeholders 4/4/2016. 1) Data Assets will delete the "NACRS" and "NACRS_OCR" folder contents from the H: drive, and delete the "MYF" folder contents from the P: drive. 2) The EISO will ensure that any PHI that may have been backed up and sent to offsite storage is permanently deleted.	Business Unit & Privacy Specialist	N/A	See "Recommendations".	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
					Date, Finish Date, RxSite [believe this is treatment site], Category, ICD9, Description, Age, Gender, Laterality, TxIntent [believe this is treatment intent], Diagnosis Type, Distant Mets, “Oncologist” for over 400,000 records.									3) Analytics and Informatics will remind CCO staff who have access to the P:\Informatics folder to engage the LPO if they suspect that there may be PHI on the P: drive, and to double check that there is no PHI in the P:\Informatics subfolders that they can access.				
CPQI	2016-03-30	2016-04-01	Internal and External	2016-04-06	Email breach. PHI included 1 HIN.	[PHI was included in an email to a reimbursement analyst, PDRP from a pharmacist at hospital.. The email was sent in an effort to request deletion of an enrolment. A second reimbursement analyst also received the email. The first analyst then wrote a reply to the two others in the chain, propagating the breach. The second analyst then detected the breach and	2016-03-31	[The analysts deleted the email from their inbox, sent box and deleted items folder as applicable. The first analyst then emailed the original sender, informed them that the email they had sent contained PHI, and instructed them to delete the email from their sent items and deleted items folders as well as delete the	3/31/2016 Notified sender (their data).	2016-04-01	Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "containment measure".	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						initiated containment processes.]		email from her Inbox and the deleted folder. The original sender replied that they would do so. The Group Manager, Drug Reimbursement was also notified of the breach.]										
CPQI	2016-04-05	2016-04-05	External	2016-04-13	Email breach. PHI included patient's initials and HIN.	PHI was included in an email to [reimbursement analyst, PDRP] from [name omitted], Pharmacist at hospital.. The email was sent in an effort to request for a prior approval for a patient.	2016-04-05	[Reimbursement analyst has: • Deleted the email from her inbox and delete items folder • Emailed the sender, informed them that the email they had sent contained PHI, and that all communication pertaining to patients should be sent through eClaims Reimbursement analyst later added that they would advise the site to delete the email from their sent and deleted mail folders]	4/5/2016 Notified sender (their data).	2016-04-05	Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "containment measure".	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
CTO	2016-04-06	2016-04-06	External	2016-04-13	Email breach. PHI included the patient's first name and case number. Note: case number is not considered PHI.	PHI was included in an email to helpdesk@cancercare.on.ca from...the Hospital. The email was sent in an effort to resolve an issue the sender was having with WTIS Patient name change. This item was not forwarded to the ATC inbox as a ticket, since PHI was discovered by helpdesk.	2016-04-06	[The service desk analyst deleted the attachment from the service desk ticket, deleted the email containing PHI from the inbox and deleted items folder in the helpdesk inbox, and informed the sender of the PHI data that was sent to CCO. The sender and anyone else who may have been cc'd on the PHI was asked to delete the PHI from their inboxes, sent boxes, and deleted items folders.]	4/6/2016 Notified sender (their data).	2016-04-11	Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "containment measure".	2016
ATC	2016-04-13	2016-04-14	External	2016-04-21	WTIS conformance environment breach. PHI included name, DOB, and HIN for 14 records.	[hospital. Sent an email to the ATC inbox on Apr 13th notifying that they had sent PHI to the WTIS conformance environment. The discoverer of the breach at hospital. ran an interface message report within	2016-04-14	[Access to Care identified the number of messages with PHI and confirmed it was 14 waitlist entries. They opened a ticket with eHealth to remove the entries from eHealth's Provincial Client Registry	N/A	2016-04-26	Privacy Specialist	Policy breach	PE breach	Privacy's recommendation to the program: "...if you could please remind hospitals not to upload PHI in the conformance environment, that would be greatly appreciated. Let us know if you have any questions."	Business Unit & Privacy Specialist	N/A	See "recommendations". No response from the business to date.	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						the Conformance environment and discovered that there were approximately 14 messages with a status of success. A few contained open waitlist entries.] [Per submitting team, all those who viewed the PHI were authorized to do so.]		(PCR) conformance environment. They took down CCO's conformance environment to clean out the PHI. eHealth responded that the PHI was successfully removed from their system. CCO's conformance environment was brought back online.]										
ATC	2016-04-19	2016-04-20	External	2016-04-21	WTIS conformance environment breach. PHI included name, DOB, and HIN for 9 records.	[ATC was gathering information from a suspected privacy breach involving hospital.and the WTIS conformance environment, when it found additional PHI from a secondary site - Mackenzie Richmond Hill, which uses the same interface. 9 waitlist entries were involved.] [Per submitting team, all those who	2016-04-20	[Access to Care identified the number of messages with PHI and confirmed it was 9 waitlist entries. They opened a ticket with eHealth to remove the entries from eHealth's Provincial Client Registry (PCR) conformance environment. They took down CCO's conformance environment to clean out the PHI. eHealth responded	N/A	2016-04-26	Privacy Specialist	Policy breach	PE breach	Privacy's recommendation to the program: "...if you could please remind hospitals not to upload PHI in the conformance environment, that would be greatly appreciated. Let us know if you have any questions."	Business Unit & Privacy Specialist	N/A	See "recommendations". No response from the business to date.	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						viewed the PHI were authorized to do so.]		that the PHI was successfully removed from their system. CCO's conformance environment was brought back online.]										
ATC	2016-05-03	2016-05-03	External	2016-05-04	Email breach. Attachment contained various WTIS data elements including patient name, HIN, postal code, and MRN, relating to 881 MRI and Computed Tomography wait list entries from scans performed in March 2016.	[PHI was forwarded to the inbox of a clinical liaison in ATC. The email contained a WTIS Extract of Open and Closed cases from a individual at the hospital.. The data was sent by the facility to ask for a similar report to be pulled from the WTIS. Altogether 5 people had the PHI in their inboxes. Out of these 5, 1 was the original sender, and 4 were internal staff who had access to the wait times PHI through WTIS.]	2016-05-03	[The clinical liaison deleted the email from his inbox and deleted items folders and advised the other 3 internal staff to do the same. Additionally the clinical liaison issued this notice to the others: "According to the privacy regulations at Cancer Care Ontario, record level data is not to be sent via email. We have set up all DI Efficiency Program sites with access to 'Tumbleweed' so that files containing personal health information can be transferred securely. As per our	5/3/2016 Notified sender (their data).	2016-05-05	Privacy Specialist	Policy breach	PE breach	Double checked that all staff involved in the breach had confirmed deletion of the file. No further recommendations.	Business Unit & Privacy Specialist	N/A	The submitter confirmed that all had deleted the file.	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
								processes, I have deleted your email from my inbox, and then deleted it again from the deleted folder. Please let me know when you done the same on your end (deleting from 'sent' folder, and again from your 'deleted' folder). From our end, incidents where record level data has been sent by email, our privacy office needs to be notified – and I will keep you up to date if further actions are required. In future, please ensure that personal health information is not included in any attached files sent via email. Please send another separate email without personal health information outlining the									

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
								original tasks and upload the Excel file to Tumbleweed folder for us to review. Thank you." Of the internal staff, one Team Lead forwarded the above notice to the original sender, and requested her to delete the email from her sent box and deleted items folders.]										
CTO	2016-05-03	2016-05-05	External	2016-05-18	Email breach. Email included DOB and chart number for one patient.	[PHI was included in an email to ITservicedesk@cancercare.on.ca from hospital.. The email was sent in an effort to resolve an issue the sender was having with DAP-electronic pathway solution. The breach was discovered 2 days later by the associate support specialist monitoring the inbox.]	2016-05-05	[The associate support specialist: Deleted the attachment from the service desk ticket Deleted the email from the ticket Informed the sender of the PHI data that was sent to us. Response to the original sender: "...Please note that the following e-mail contained Personal Health Information (PHI). Please see the email with the PHI	5/5/2016 Notified sender (their data).	2016-05-05	Privacy Specialist	Privacy breach	PE breach	The privacy specialist issued a recommendation to the associate support specialist: "For the notification back to the sender, we should let them know that the email should be deleted from both their sent and deleted folders. Essentially we are recommending that they completely purge the PHI from their email system. If you could please let me know	Business Unit & Privacy Specialist	N/A	Associate support specialist had advised the original sender: "Please note that the following e-mail contained Personal Health Information (PHI). Please see the email with the PHI removed. We have removed the e-mail from our Inbox and Deleted Items. Please do the same in your mailbox's Sent Items. If you deem it necessary, please	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
								removed. We have removed the e-mail from our Inbox and Deleted Items. Please do the same in your mailbox's Sent Items. If you deem it necessary, please resend the original information, without PHI. You may use Interface Message ID or Waitlist Entry ID to reference a patient..."]						once they have been advised of this, that would be greatly appreciated. "			resend the original information, without PHI. You may use Interface Message ID or Waitlist Entry ID to reference a patient. Please quote the subsequent request number so we can append the information to the appropriate request."	
ATC	2016-05-10	2016-05-10	External	2016-05-18	Email breach. PHI included computed tomography (CT) scheduling data (including MRN), information about CT scans that had been performed (including MRN), and operating hour operation (no PHI). In the file that was emailed, there were 3,682 records for scheduled CT scans	[PHI was sent to the ATCsupport @cancercare.on.ca inbox (April CT Efficiency data submission files) from a coordinator at the Bluewater – Sarnia site hospital. This was discovered by a senior business analyst within the ATC.] [Update from the senior business analyst: At no point was	2016-05-10	[The Senior Business Analyst: • deleted the email from her inbox and deleted items folders. • instructed the sender over the phone to delete the email from their sent folder and again from their deleted folder; ensured that the sender provided verbal confirmation that it had been done. The senior business analyst	5/10/2016 Notified sender (their data).	2016-05-13	Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "containment measure".	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
					(with MRN as PHI), and 1,388 records for performed CT scans (with MRN as PHI).	there any issue with the coordinator's ability to upload files to MFT, she had uploaded MRI files earlier in the day. Included in the data submission template to prepare the files - there is the link for MFT, and the contact information for the CCO Helpdesk in case they have any issues. The senior business analyst had also included that information in the email trail with Bluewater on which the coordinator in question was copied.]		advised the sender to upload the file in question to Tumbleweed for their review, and reminded the sender to only use Tumbleweed for sending PHI.]										
A&I	2016-05-17	2016-05-17	External	2016-05-18	Email breach. There were 3 patient chart numbers cited.	[PHI - patient chart numbers pertaining to Activity Level Reporting (ALR) data - was included in an external email sent from hospital.to a Senior Analyst in Data Assets. The email	2016-05-17	[The Senior Analyst deleted the e-mail and asked the original sender and all recipients of the original email - 2 external, and 2 internal not including the Senior Analyst - to delete the e-	5/17/2016 Notified sender (their data).	2016-05-17	Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "containment measure".	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						was sent because the Senior Analyst had originally contacted hospital.to let them know that one of their ALR metric volume counts was inflated.]		mail from all folders in their inbox. She informed the original sender that the PHI is not be sent via email and to use the secure Gateway Portal for any PHI data exchange. The Senior Analyst has also deleted the email permanently from all folders of their inbox.] [Aside: The "Gateway" Portal, is what is used by ALR sites to access the ALR Submission Tool, as well as the SSL portal where they can go to get files that contain PHI (ie. QA reports from ALR submissions, PHI file exchange between CCO and the site).] [All internal viewers had authorization to view PHI, but unsure about external viewers.]									

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
A&I	2016-05-17	2016-05-17	External	2016-05-18	Email breach. PHI included one patient chart, chemotherapy drug names, and treatment date.	[PHI Data was included in an email by a user to STIP@cancercare.on.ca from Hospital, where it was discovered by the Product Manager, Product Management. The email was regarding an outstanding Helpdesk ticket opened with the same mailbox.] [Updated: The Product Manager is authorized to view the PHI.]	2016-05-17	[The Product Manager emailed the sender and informed them that they had sent email containing PHI. Original email was deleted from the inbox and Deleted folder. Advised original user of breach and to not send PHI data on an email to CCO. CCO notified the original sender that they should also delete the email from their sent and deleted items folders.]	5/17/2016 Notified sender (their data).	2016-05-18	Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "containment measure".	2016
CPQI - SSO	2016-05-17	2016-05-17	Internal	2016-05-18	Email breach. Attachment contained PHI for one individual including HIN.	[PHI (HIN) was included in a file that a cancer analytics analyst sent to the functional lead, SSO and stored on the H: drive.]	2016-05-17	Upon recognizing that the file contained PHI, the functional lead contacted the analyst to remind her that the lead was not allowed to view PHI, and asked her to delete the file from H drive or remove the HCNs from the file.	N/A (internal)	2016-05-17	Senior Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "containment measure".	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
CPQI - SSO	2016-05-17	2016-05-17	Internal	2016-05-18	Email breach. PHI included a list of patient names and information for those patients engaged in out of country services.	PHI was sent in error in an email attachment from a coordinator in SSO to the group manager, SSO and a director in P&RP. All parties are allowed to see the data.	2016-05-17	• The coordinator contacted the recipients, informed them that the email they had received contained PHI, and instructed them to delete the email. • All recipients and sender deleted the email from their inboxes and deleted item folders.	N/A (internal)	2016-05-19	Senior Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "containment measure".	2016
CPQI - SSO	2016-05-17	2016-06-03	External	2016-06-07	Email breach. PHI included two patient names and information about diagnosis.	PHI was sent to the Coordinator, SSO by a contact in the Hospital. All parties were authorized to view the data.	2016-05-17	The Coordinator, SSO contacted the sender and informed her that the email she had sent contained PHI, and not to send this in the future. The Coordinator then deleted the email from his inbox and deleted item folders.	5/17/2016 Notified sender (their data).	2016-06-10	Senior Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "containment measure".	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
CPQI	2016-05-17	2016-06-06	Internal and External	2016-06-07	Email breach. The email related to a patient case.	[PHI was included in an internal email between a hospital.sender and recipient. The email was copied to the Policy Research Analyst, Pathology and Laboratory Medicine Program at CCO. The email was sent regarding a patient case, and CCO was copied in error - it appears that the sender had meant to copy his assistant.] [The Policy Research Analyst subsequently forwarded the email to their manager, resulting in a privacy breach. The Manager notified the Policy Research Analyst that the email contained PHI.]	2016-05-19	[The Policy Research Analyst asked their manager to delete the forwarded email containing PHI from her inbox and deleted items; the Manager has confirmed that this was done.] [The Policy Research Analyst deleted all copies of the email from her sent folder, inbox, and deleted items folder.] [The Policy Research Analyst emailed the sender and receiver of the email, informing them that the email they had sent and copied her on contained PHI, that she had deleted the email from her inbox and deleted items folders, and that they should delete this email from their sent folder and deleted	5/19/2016 Notified sender (their data).	2016-06-10	Manager, Privacy	Privacy breach	PE breach	N/A	Business Unit	N/A	See "containment measure".	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
								items folders as well.]										
CTO	2016-05-18	2016-05-18	External	2016-05-25	Email breach. PHI included health records and chart numbers for multiple patients.	[PHI was sent by a booking clerk to ATC@cancercare.on.ca to correct an error in data entry in the WTIS.]	2016-05-18	[The support specialist deleted the PHI from the email, created a ticket and responded to the user per data breach procedures. Email to the original sender:"Please note that your original e-mail contained Personal Health Information (PHI) and we have subsequently removed the PHI from the email body below. We have also permanently deleted the e-mail from our Inbox and Deleted Items. Please do the same in your mailbox's Sent Items and Deleted Items. ...If you deem it necessary, please resend the	5/18/2016 Notified sender (their data).	2016-05-19	Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "containment measure".	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
								original information, without PHI. You may use Interface Message ID or Waitlist Entry ID to reference a patient..."]										
A&I	2016-05-18	2016-05-18	External	2016-05-25	Email breach. PHI included pathology reports - approx. 40 pages' worth.	[PHI was faxed to the OCR team. hospital. faxes the paper pathology reports to the OCR team on a quarterly basis. On May 18th the sender informed the OCR team that they wanted to fax over the pathology reports for the months of January-March 2016. There were a total of four batches of pathology reports to be faxed over via the secure fax line that is routed to pimspathologyfax@cancercare.on.ca . The Part 1 of 4 was faxed successfully to the PIMSPathologyFax inbox. However,	2016-05-18	[The team lead: • Immediately emailed the sender, informed them that the Part 2 was send as an attachment in an email instead of via the secure fax line, and instructed them to delete the email. • Immediately deleted the email from their inbox and deleted items folders. • Reported the incident to the Legal and Privacy Office.]	5/18/2016 Notified sender (their data).	2016-05-19	Privacy Specialist	Policy breach	PE breach	From privacy specialist to team lead, OCR: "Would it be possible to please ensure that the original sender has hard deleted the email containing PHI from both their sent and deleted items folders, and to ensure that they are aware of the rationale for deletion (that PHI must not be sent through email to CCO, as it is not considered a secure method of transfer)?"	Business Unit & Privacy Specialist	N/A	The team lead carried out the recommendations.	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						part 2 was send as an attachment in an email to the team lead, OCR instead of via the secure fax line. The team lead was authorized to view the PHI.] [Update: All 4 parts successfully came through the secure fax line on May 18, 2016.]												
P&CC	2016-05-18	2016-05-24	External	2016-05-25	Fax breach. The PHI appeared to be a large patient record for a single patient (28 pages) including HIN, DOB, medical history, etc.	[PHI was included in an electronic fax from a physician's office at hospital. The fax was intended to be sent to PET Scans Ontario to book a patient for a PET scan, but the fax number was incorrect and it ended up in CCO's Provincial Implementations mailbox. It was received by [omitted 2 names] who monitor the fax email box.]	2016-05-24	[One of the two recipients of fax followed up with PET Scans Ontario and confirmed that the request was intended to be sent to CCO, just to the wrong fax number. The request was faxed to the appropriate program and the reimbursement associate monitoring the fax confirmed receipt. Faxes that pass through the PET Scans Ontario fax line come to	N/A - sender could not be reached.	2016-05-30	Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "containment measure".	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
								a direct PET fax inbox and the reimbursement associate would ordinarily save them into the appropriate patient folders. All electronic copies of the PHI have been deleted, and all printed copies have been disposed of. The sender could not be successfully contacted to be informed of their error. However, the fax number for PET Scans Ontario is on the PET Scans Ontario website as well as the actual form submitted. Therefore, Privacy has no further recommendations.]										
ORN	2016-05-19	2016-05-19	External	2016-05-25	Fax breach. PHI included patient name, address, DOB, HIN, and other information.	PHI was received by CCO's main fax line, and forwarded to the Legal and Privacy Office, then later to the ORN for	2016-05-24	[The ORN confirmed that there was no ORN purpose for the data and that the faxes should be destroyed. ORN was to	5/24/2016 Notified sender (their data).	2016-05-24	Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "containment measure".	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						investigation. The referral form is a tool developed by ORN for use by primary care providers when they are referring outpatients to a nephrologist in the hospital setting and/or in the community.		identify the purpose for which they were received, and advised whom these forms should be directed to. [On May 24, 2016 [ORN] contacted the primary care provider (aka. the original sender) to 1) Inform them of the breach, 2) confirm the forms are to be sent to a local nephrologist, 3) confirm future referral forms are not to be sent to CCO/ORN, and 4) advised that the form will be securely destroyed. [A follow up fax was sent back to the sender reiterating the above steps, and the contact information for a local nephrologist. [The ORN has modified the form in the future to include a disclaimer										

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
								such as "do not fax/email this form to CCO/ORN".]										
CPQI	2016-05-19	2016-05-19	External	2016-05-25	Email breach. PHI included patient initials and chart number.	PHI was included in an email from [name omitted] at Hospital to [a reimbursement associate].	2016-05-19	[The reimbursement associate] has: • Deleted the email from their inbox and deleted items folder • Sent new email to [the sender], and instructed her to delete the email from their inbox and deleted items folders	5/19/2016 Notified sender (their data).	2016-05-19	Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "containment measure".	2016
P&RP	2016-05-24	2016-05-24	Internal and External	2016-05-25	Email breach. PHI included the patient's treatment (drug name), their last name, and a bit of the patient's disease history.	[PHI pertaining to a patient was sent from a patient's family member to STFM@cancercare.on.ca. It was a question about whether or not a patient could receive funding for a drug. This is not a drug that is funded by CCO but rather by the MOHLTC. The email was then	2016-05-24	[Group Manager, Drug Reimbursement instructed everyone on the email chain to delete the email from inbox, sent items and deleted items. All PHI confirmed deleted by 5/26/2016.]	2016-05-26	2016-05-26	Privacy Specialist	Privacy breach	PE breach	Privacy specialist instructed the Group Manager to also let the original sender know that email is not a secure method of transfer for personal health information.	Business Unit	N/A	The Group Manager acknowledged the recommendations and passed them on to the group that would be responding to the original sender.	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						sent internally by the Group Manager, Funding Implementation, to 6 CCO staff members to identify next steps/who should respond. One of the staff members flagged the email as containing PHI. Only 2 of the staff members were authorized to view the PHI.]												
P&RP	2016-05-31	2016-05-31	External	2016-06-01	Email breach. PHI included 7 HINs.	[PHI was included in an email to a Senior Specialist, Contract Management from the Manager of Radiation Therapy at hospital. The email was sent in an effort to resolve an issue the sender was having with C1R volume reconciliation.	2016-05-31	Senior Specialist deleted the email from his email boxes. He then emailed the sender, informing them that the email contained PHI and instructing them to delete the email from their email.	N/A	2016-05-31	Senior Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "containment measure".	2016
LPO	2016-06-07	2016-06-07	Internal	2016-06-07	Hardcopy PHI breach. PHI included a patient's name, health insurance number, patient ID	The Privacy Specialist printed out a 1-pg document containing PHI, that had initially come in as a	2016-06-07	The Privacy Specialist removed the paper copy of the PHI from the printing area and put it	N/A - internal	2016-06-07	Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "containment measure".	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
					number (likely hospital-specific), date of birth, sex, and phone number, as well as the name of their physician and a description of their medical condition.	fax to the CCO main fax line, for the purpose of further investigation. The PHI was accidentally left in the printer when the rest of the print job was picked up, and was later discovered by the Senior Board Coordinator, Legal and Privacy Office. Given the short amount of time that elapsed between printing and discovery, it is unlikely that anyone else had viewed the PHI.		into a locked cabinet. The electronic copy of the PHI had previously been purged from CCO's systems.									
CPQI	2016-06-07	2016-06-07	External	2016-06-22	Fax breach. The fax included information about the patient such as their health insurance number, the identity of their provider, and a description of their health condition.	PHI was faxed by a healthcare provider to the CCO main reception line, and the main reception desk subsequently brought it to the attention of a Privacy Specialist within the Legal and Privacy Office. The	N/A	The Privacy Specialist printed a copy of the fax, then hard deleted the electronic version of the fax from CCO's systems. She transferred the printed copy of the fax to the PDRP. Within the PDRP, the	N/A	N/A	Senior Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "containment measure".	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						Privacy Specialist then alerted the Provincial Drug Reimbursement Program (PDRP). The PHI was faxed in an effort to facilitate a drug reimbursement request; however, based on established policy, all such requests should either be coming through a secure fax line dedicated to the program, or through eClaims.		intended recipient program was identified, and the appropriate Reimbursement Analyst agreed to add the fax to their case file in eClaims. The Reimbursement Analyst agreed to follow up with the healthcare provider's office to let them know that they can submit their request securely online. [Note: need to confirm that this took place, and when]										
CPQI	2016-06-08	2016-06-09	External	2016-06-15	Email breach. Information included a patient's full name.	[PHI was included in an email to two members of PDRP from a Pharmacist at Hospital. The email was sent in an effort to request review of a supplemental form in eClaims. The two members of PDRP included the former site reimbursem	2016-06-08	[The current site reimbursement associate notified the former site reimbursement associate and the original sender to delete the email from their Outlook inbox/sent folder, as well as the deleted items folder. Both have confirmed	6/8/2016 Notified sender (their data).	2016-06-09	Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "containment measure".	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						ent associate and the current site reimbursement associate for Hospital. Wanting to ensure that a supplemental form was being reviewed appropriately, the sender emailed both recipients.] [Reimbursement associates are permitted to view PHI for the purpose of their day-to-day work.]		deletion either verbally or via email.] [In her communication, the current site reimbursement associate informed the original sender that the email she had sent contained PHI, and reminded her of the process to prevent future privacy breaches.] [The current site reimbursement associate also deleted the original email containing PHI from her own Outlook inbox and deleted items folders, and informed her manager of the incident.]										
CPQI	2016-06-14	2016-06-15	External	2016-06-22	Mail breach. The letter included information about the patient such as their health insurance number, the identity of their provider, and a	PHI was sent by a healthcare provider to CCO, and the recipient (main reception desk) subsequently brought it to the attention of a Privacy	2016-06-21	The Privacy Specialist transferred the hardcopy PHI to the PDRP, advising the program to follow up with the original sender directly and	6/21/2016 Notified sender (their data).	N/A	Senior Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "containment measure".	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
					description of their health condition.	Specialist within the Legal and Privacy Office. The Privacy Specialist then alerted the Provincial Drug Reimbursement Program (PDRP). The PHI was sent in an effort to facilitate a drug reimbursement request; however, based on established policy, all such requests should either be coming through a secure fax line dedicated to the program, or through eClaims. The letter included information about the patient such as their health insurance number, the identity of their provider, and a description of their health condition.		to let them know the appropriate secure procedure for transferring the PHI. The program then followed up with the sender.										

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
CTO	2016-06-20	2016-06-20	External	2016-06-22	Email breach. PHI included patient's name, birth date, chart number, and HIN.	[PHI was included in an email to ATC@cancercare.on.ca from an Office Receptionist at Hospital. The email was sent in an effort to resolve an issue the sender was having with WTIS; surgery was unable to modify the patient wait time. The breach was discovered by a Service Desk Analyst.]	2016-06-20	[The Service Desk Analyst deleted the email from the ATC ticket and informed the sender of the PHI data that was sent. Text of email: "Please note that your original e-mail contained Personal Health Information (PHI) and we have subsequently removed the PHI from the email body below. We have also permanently deleted the e-mail from our Inbox and Deleted Items. Please delete the same email from your mailbox's Sent Items and Deleted Items, and relay these deletion instructions to all individuals who may have been copied on the email containing PHI. ...If you deem it necessary, please resend the	6/20/2016 Notified sender (their data).	2016-06-21	Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "containment measure".	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
								original information, without PHI. You may use Interface Message ID or Waitlist Entry ID to reference a patient..."]										
CTO	2016-06-21	2016-06-21	External	2016-06-22	Email breach. Email contained patient HIN.	PHI was included in an email from Hospital to a Technical Support Associate at CCO, in an attempt to troubleshoot an issue for a health care provider.	2016-06-21	[The Technical Support Associate informed the sender of the PHI that was sent. Text of the email: "Please note that the following e-mail contained Personal Health Information (PHI). Please see below with the PHI removed. We have removed the e-mail from our Inbox and Deleted Items. Please do the same in your mailbox's Sent Items. ... If you deem it necessary, please resend the original information, without PHI..."]	6/21/2016 Notified sender (their data).	2016-06-23	Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "containment measure".	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
CTO	2016-06-21	2016-06-21	External	2016-06-22	Email breach. Email contained patient ID and birth date.	PHI was included in an email to ORRSHelpdesk@cancercare.on.ca from an Administrative Assistant at the hospital The email was sent in an effort to resolve an issue the sender was having with ORRS. The breach was discovered by a Service Desk Analyst.]	2016-06-22	[The Service Desk Analyst deleted the attachment from the WTIS ticket, deleted the email from the WTIS ticket, and informed the sender of the PHI that was sent. Text of email: "Please note that your original e-mail contained Personal Health Information (PHI) and we have subsequently removed the PHI from the email body below. We have also permanently deleted the e-mail from our Inbox and Deleted Items. Please delete the same email from your mailbox's Sent Items and Deleted Items, and relay these deletion instructions to all individuals who may have been copied on the email containing PHI. ...	6/21/2016 Notified sender (their data).	2016-06-22	Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "containment measure".	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
								If you deem it necessary, please resend the original information, without PHI. You may use Interface Message ID or Waitlist Entry ID to reference a patient..."]											
A&I	2016-06-23	2016-06-23	External	2016-06-29	Email breach. PHI included patient chart number, name, and DOB.	[PHI was included in an email sent by William Osler Health Services to the Senior Analyst, Data Assets. The sender was trying to show the Senior Analyst what she wanted to extract from the OPIS application (used for drug administration) by putting a screen shot of the Patient Index.]	2016-06-23	[The Senior Analyst replied to notify the original sender of the breach, and asked the original sender to delete the e-mail from all folders in their inbox including sent and deleted folders. She informed the sender that PHI was not be sent via email and to use the secure Gateway Portal for any PHI data exchange. The Senior Analyst then deleted the email permanently from all folders of her own inbox.]	6/23/2016 Notified sender.	2016-06-23	Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "containment measure".	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
CTO	2016-07-05	2016-07-05	External	2016-07-13	Email breach. PHI related to a single patient.	[PHI was included in an email to ATC@cancercare.on.ca from Hospital. The email was sent in an effort to resolve an issue the sender was having re: a question from a surgeon's office.]	2016-07-05	[The Service Desk Analyst at CCO deleted the attachment from the ticket, deleted the email from the ticket, and informed the sender of the PHI. Email to sender: "Please note that your original e-mail contained Personal Health Information (PHI) and we have subsequently removed the PHI from the email body below. We have also permanently deleted the e-mail from our Inbox and Deleted Items. Please delete the same email from your mailbox's Sent Items and Deleted Items, and relay these deletion instructions to all individuals who may have been copied on the email	7/5/2016 Notified sender (their data).	2016-07-07	Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "containment measure".	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
								containing PHI. ... If you deem it necessary, please resend the original information, without PHI. You may use Interface Message ID or Waitlist Entry ID to reference a patient..."										
ORN	2016-07-05	2016-07-05	External	2016-07-13	Fax breach. PHI included the patient's name, address, telephone number, HIN, date of birth, and laboratory results.	PHI was included in a faxed Ontario Renal Network (ORN) Outpatient Nephrology Referral Form, sent through CCO's main fax line. The fax was brought to the attention of a privacy specialist.	2016-07-13	[The Privacy Specialist notified a program contact at the ORN of the breach. She purged the electronic copy of the fax from the Legal and Privacy Office mailbox and saved a copy in the secure H: drive for further investigations. She transferred a hardcopy of the fax to the Senior Specialist, ORN 2 days later. No clinic phone number was provided on the referral form and could not be located online. A phone number was	7/5/2016 Notified sender (their data).	2016-07-18	Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "containment measure".	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
								was eventually found. The Senior Specialist, ORN contacted the primary care provider's office to inform them of the breach and provide next steps. There is a fax record of this communication which outlines that the forms should be sent to a local nephrologist in the future. The referral package containing PHI, which had been locked up throughout, was put into a shredder box to be securely destroyed.]										
CTO	2016-07-06	2016-07-06	External	2016-07-13	Email breach. PHI related to a single patient (name, date of birth). Some non-redacted letters and numbers were also enclosed in the copy of the email that went to	[PHI was included in an email to ATC@cancercare.on.ca from Hospital. The email was sent in an effort to resolve an issue the sender was having in WTIS.]	2016-07-06	[The Service Desk Analyst at CCO deleted the attachment from the ticket, deleted the email from the ticket, and informed the sender of the PHI.	7/6/2016 Notified sender (their data).	2016-07-18	Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "containment measure".	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
					the Privacy Specialist; confirmed with the Service Desk Analyst that these were non-identifying.			Email to sender: "Please note that your original e-mail contained Personal Health Information (PHI) and we have subsequently removed the PHI from the email body below. We have also permanently deleted the e-mail from our Inbox and Deleted Items. Please delete the same email from your mailbox's Sent Items and Deleted Items, and relay these deletion instructions to all individuals who may have been copied on the email containing PHI. ... If you deem it necessary, please resend the original information, without PHI. You may use Interface Message ID or Waitlist Entry ID to reference a patient..."										

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
CTO	2016-07-21	2016-08-04	External	2016-08-10	Email breach. Email contained a list of patients with Adverse Effects which have to be corrected within OPIS. PHI included patient names, HCNs, drugs. Number of records unknown as the file was deleted prior to notification of Privacy, by a member of the Service Desk who is no longer at CCO.	[PHI was included in an email to STIP in July from an OPIS user at the Hospital. The email was sent in an effort to resolve an issue the sender was having with list of patients with Adverse Effects which have to be corrected. STIP noticed the PHI in August and informed the Service Desk.] [STIP clarified that the user had emailed helpdesk with the PHI, not STIP@cancercare.on.ca. The PHI information was not stored or captured on STIP side.]	2016-08-04	• CCO, Service Desk deleted the email from their inbox and deleted items folders. • CCO, Service Desk mailed the sender, informed them that the email they had sent contained PHI, and instructed them to delete the email from their sent items and deleted items folders. • CCO, Service Desk Modified ticket with PHI by deleting any evidence of PHI attached, and assigned to the appropriate Group. [Service Desk's messaging: "Please note that the following e-mail contained Personal Health Information (PHI). Please see the content	2016-08-04	2016-08-10	Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "containment measure".	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
								of the email with the PHI removed. We have removed the e-mail from our Inbox and Deleted Items. Please do the same in your mailbox's Sent Items. ... If you deem it necessary, please resend the original information, without PHI."]										
A&I	2016-05-17	2016-07-28	Internal and External	2016-08-03	iPort Access breach. PHI included patient name, health insurance number (HIN), another patient number, patient type (e.g., outpatient vs inpatient), as well as postal code, plus service start dates, wait dates, and other clinical information.	• A user of iPort Access reported that they were seeing personal health information (PHI) belonging to other facilities in the Wait Times Information System (WTIS) report "XMC110 Patient Detail Report – MRI/CT Closed Scans". • Upon further investigation, it was found that multiple sites were experiencing	2016-07-29	• This privacy breach has been contained. • The report was disabled, i.e., hidden from iPort Access users while the issue was being investigated. This means that it was restricted to internal viewers, and only CCO's system administrator and developer could see the report, and not via the web portal. • A root cause was identified.	N/A	2016-09-26	Privacy Specialist	Privacy breach	PE breach	The following resolutions were issued: 1) A&BI to double check other iPort Access reports containing PHI, to ensure that the same error has not occurred elsewhere. Where incorrect access permissions are found in other reports, A&BI will work with the appropriate business units to contain the suspected breach as soon as	Business Unit & Privacy Specialist	Ongoing. 1) was completed Aug 22, 2016.	See "recommendations". 1) All 72 other PHI reports in iPort Access have been checked. Of these, one other PHI report with incorrect access permissions was found. However, through a review of the report execution log, it was confirmed that no privacy breach had occurred. The privacy risk was confirmed resolved as of Aug 22nd, after a	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						the same technical issue. • Normally when presented with the report, users can choose their own facility, another facility, or leave the field blank. In this case, PHI was exposed when users did not select their own facility while running the report. A detailed list of users and the data they accessed in an unauthorized manner is available. Incorrect access permissions were in place since May 2016.		The issue was caused by metrics, which are components of the report. During deployment, there are several objects or codes that need to be deployed together, including metrics. However, metrics were not deployed for this report as a result of human error. Therefore, incorrect access permissions have been in place for this report since early May. • Normally a test plan would be put in place in order to reduce the risk of incorrect deployment. This plan would commonly include the names of those approving access for the report, what changes were being made, and other information. In this case, the report was						possible, and notify Privacy of each incident. 2) A&BI to double check whether it is possible to identify which patients' PHI were exposed during the breach; if possible, Privacy will discuss whether notification is required. 3) Privacy to follow up with A&BI later in the year, to ensure that documentation detailing testing procedures for iPort Access reports is made available, and reflects adequate privacy controls, including but not necessarily limited to double checking any access controls in place.			technical solution was deployed and access settings were corrected.	

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
								deployed through a master release, i.e., all fixes were packaged and deployed together. For these types of deployments, less than usual testing was performed. However, Analytics and Business Intelligence (A&BI) will now be performing the same amount of testing whether the report is a master release or not. Documentation for this process will be made available later this year. • To correct the error, the metrics update was deployed and tested. Then, the report was re-enabled (unhidden) so that those who had appropriate permissions could view it again. • No detailed explanation for the										

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
								change was issued to affected users; during the containment process, the following notice was posted to the iPort Access website: 7/28/2016 Resolved: Issue with XMC110 MRI/CT Closed Scan Extract Report UPDATE: This issue has been resolved as of July 29. There is currently an issue with the following Diagnostic Imaging iPort™ Access report: XMC110 Patient Detail Report - MRI/CT Closed Scans Our technical team is investigating the root cause of the issue and this will be resolved as soon as possible. Until further notice, the report is hidden and not available									

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
								for use in iPort™ Access. If you have any questions or concerns, please contact iPort™ Access Support at iportaccess @cancercare.on.ca.											
CTO	2016-08-03	2016-08-04	External	2016-08-10	Email breach. Email included OPIS data - patient charts / Drugs / Allergies - for approximately 25 records, including some duplicate records.	[PHI was included in a file attached to email by technical support at hospital) to STIP@cancercare.on.ca, regarding a helpdesk ticket. The original ticket was to help the site make corrections to Adverse Effects records that were affected by an OPIS bug. A script was run at the site to identify those records – local technical support were supposed to give the file to the user but included STIP as well. The PHI came to the	2016-08-03	[The analyst emailed the sender and informed them that they had sent email containing PHI. Original email was deleted from the inbox and Deleted folder. The analyst advised the sender of the breach and to not send PHI data on an email to CCO.]	2016-08-03	2016-08-09	Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "containment measure".	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						attention of the Analyst, Technical Support who was overseeing the inbox. Only the members of STIP that support OPIS have access to OPIS at the sites via the secure VPN portal, including the analyst who viewed the PHI.Access to OPIS is administered by the STIP team and the individual OPIS sites. The OPIS sites agreed to CCO's access.]												
ORN	2016-08-09	2016-08-09	External	2016-08-03	Email breach contained Patient name and health status.	PHI was included in an email to CPQI team from [omitted]. The email was sent in an effort to communicate an issue being experienced by stakeholders.	2016-08-09	Recipient deleted email form inbox and deleted folder, contacted sender to inform them of the breach and requested not to send emails with PHI to CCO.	2016-08-09	2016-08-09	Senior Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "containment measure".	2016
P&RP	2016-08-10	2016-08-03	External	2016-08-10	Email breach contained Patient name and health status.	PHI was included in an email to SSO team, and [name omitted] at Hospital sent by [Dr's name	2016-08-10	Recipient deleted email from inbox and deleted folder, contacted sender to inform them	8/10/2016 Notified sender (their data).	2016-08-11	Senior Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "containment measure".	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						omitted] in Ottawa. The email was sent in an effort to communicate an update on a patient issue that had been brought to CCO's attention yesterday.		of the breach and requested not to send emails with PHI to CCO.										
CTO	2016-08-11	2016-08-12	External	2016-08-15	Email breach. Email contained 2 patient names, in the context of talking about their enrolment in eClaims.	[PHI Data was included in an email to IT Service Desk from a Administrative Coordinator, Nuclear Medicine and Molecular Imaging at hospital. The email was sent in an effort to resolve an issue the sender was having with eClaims.]	2016-08-12	[The Technical Support Associate, Service Desk deleted the email from the inbox and deleted items folders. He emailed the sender on Aug 12, informed them that the email they had sent contained PHI, and instructed them to delete the email from their sent items and deleted items folders. He also created a second ticket without PHI and assigned to the appropriate Group. He then closed the ticket with PHI in it.]	2016-08-12	2016-08-15	Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "containment measure".	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
								[Service Desk's messaging: "Please note that the following e-mail contained Personal Health Information (PHI). Please see the attached copy with the PHI removed. We have removed the e-mail from our Inbox and Deleted Items. Please do the same in your mailbox's Sent Items. ... If you deem it necessary, please resend the original information, without PHI. You may use Interface Message ID or Waitlist Entry ID to reference a patient..."]											
A&I	2016-08-15	2016-08-16	Internal	2016-08-23	No breach occurred - suspected breach only. However, the report in question contained patient-level information such as DOB, gender, HIN, patient	[Business Intelligence Team Lead in Analytics and Informatics found that an iPort Access WTIS report, "ALC-DTR002 Daily ALC Volumes by	2016-08-16	[The report was disabled (hidden) for iPort Access users. The root cause was identified and a fix was deployed. The issue was due to	N/A - internal	N/A	Privacy Specialist	Suspected breach	Unclear	N/A	Business Unit	N/A	See "containment measure".	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
					name, patient postal code, and last ALC discontinuation reason.	Discharge Destination", was incorrectly configured. If users drilling down in this report did not select their own facility, the drilldown template "ALC-EXT001 ALC Patient Detail Report" would display PHI data from all facilities.]		an attribute for the report, which should have been a security attribute but was a common attribute instead. The report update was deployed and tested. Then, the report was re-enabled (unhidden). After investigating the report execution log, A&I found no evidence for a real breach (i.e., no one had executed the report successfully).]										
CPQI	2016-08-16	2016-08-16	External	2016-08-17	Email breach contained Patient last name and first initial with diagnosis	[PHI was included in an email that 2 CCO employees were copied on. The emails were sent in an effort to communicate an update on a continuing patient issue that had been brought to CCO's attention.]	2016-08-17	Recipient deleted email from inbox and deleted folder, contacted sender to inform them of the breach and requested not to send emails with PHI to CCO.	8/17/2016 Notified sender (their data).	2016-08-17	Senior Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "containment measure".	2016
CTO	2016-08-19	2016-08-23	External	2016-08-23	Email Breach. 2 attachments contained PHI. The	[A user of OPIS at Trillium Health Partners	2016-08-23	[The email with PHI has been permanently deleted from	8/23/2016 (Notified sender - their data.)	2016-08-23	Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "containment measure".	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
					screenshot file contains MRN, diagnosis, admin start date, and drug information. The report file contains MRN, admin start date, and drug information in the regimen name.	experienced account setup issues and emailed helpdesk@cancercare.on.ca to request assistance. This user included PHI in the attachment while trying to describe the issue to CCO's IT Service Desk. The breach was discovered by an Associate, Technical Support.]		helpdesk's Inbox and Deleted Items. The attachments with PHI has been deleted from the IT Service Desk's ticketing system. The Associate, Technical Support emailed the sender, informing them of the privacy breach and instructing them to delete the email from their sent items and deleted items folder.]										
CPQI - SSO	2016-08-23	2016-08-23	External	2016-08-23	Email breach containing PHI (name and diagnosis)	[PHI was included in an email to CCO employee received from hospital. The email was sent in an effort to communicate an issue being experienced by hospital . The PHI involved was a single patient name and diagnosis.]	2016-08-23	Recipient deleted email from inbox and deleted folder, contacted sender to inform them of the breach and requested not to send emails with PHI to CCO.	8/23/2016 Notified sender (their data).	2016-08-23	Senior Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "containment measure".	2016
ORN	2016-08-30	2016-08-30	External	2016-09-07	Fax breach. The form includes such	PHI was included in a faxed ORN Outpatient	2016-09-07	8/30/2016: The Privacy Specialist notified the	9/7/2016 Notified sender (their data).	2016-09-08	Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "containment measure".	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
					information as the patient's name, address, telephone number, HIN, and date of birth.	Nephrology Referral Form, sent through CCO's main fax line. The fax was brought to the attention of a privacy specialist.		Senior Specialist, ORN of the breach. She purged the electronic copy of the fax from the Legal and Privacy Office mailbox and will transfer a hardcopy of the fax to the Senior Specialist. 9/6/2016 – Hard copy of fax transferred to the Senior Specialist. 9/7/2016 - Senior Specialist, ORN contacted primary care provider's office to inform of breach and provide next steps and referral package was put into a shredder box to be securely destroyed. A follow-up fax was sent to the primary care providers office to confirm next steps.										
CPQI - SSO	2016-09-09	2016-09-13	Internal	2016-09-13	Email breach containing picture and patient identifiers	Email with PHI sent in error to internal SSO team.	2016-09-13	All recipients were notified that the email contained PHI and	9/13/2016 Notified sender (their data).	2016-09-13	Senior Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "containment measure".	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
								deleted the email from their inbox and deleted folder.										
CPQI	2016-09-12	2016-09-12	Internal	N/A	Fax breach. Unclear about details.	[Privacy specialist received a fax containing PHI related to the NDFP and transferred this to the appropriate senior privacy specialist for triage. This is a policy breach because the form that was faxed should have been completed electronically using eClaims. The NDFP must collect the PHI that was included in the fax to administer the program.]	N/A	N/A	N/A	N/A	Senior Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	N/A	2016
CTO	2016-09-13	2016-09-13	External	2016-09-20	Email breach. PHI included patient names, DOBs and HINs for 3 individuals.	[PHI was included in an email to ATC@cancercare.on.ca from a dental clinic. The email was sent in an effort to resolve an issue the sender was having with the WTIS system. The email was discovered	2016-09-13	[The Associate, Technical support deleted the attachment from the helpdesk ticket, deleted the email from the ticket, and informed the sender of the PHI data.	9/13/2016 Notified sender (their data).	2016-09-14	Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "containment measure".	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						by the Associate, Technical Support supporting this inbox.]		Note: the copy of the email with redacted PHI that was sent to the privacy specialist contained only addresses where treatment was received, not actual direct patient identifiers. Thus, it does not constitute a second breach. The response to the sender: "Please note that your original e-mail contained Personal Health Information (PHI) and we have subsequently removed the PHI from the email body below. We have also permanently deleted the e-mail from our Inbox and Deleted Items. Please delete the same email from your mailbox's Sent Items and Deleted Items, and relay these										

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
								deletion instructions to all individuals who may have been copied on the email containing PHI... If you deem it necessary, please resend the original information, without PHI...]											
ORN	2016-09-14	2016-09-15	Internal and External	2016-09-15	Email breach. Email contained ORRS Patient ID and patient journey data (last treatment status and status date) for 33 records.	[PHI was sent via email to 3 individuals at CCO (Group Manager, Funding Policy & Operations; Team Lead, Data Management; Group Manager, ORN IM/IT & Implementation) by an Information Team Lead at the hospital. The email was subsequently forwarded to 3 other individuals at CCO (Senior Analyst, Policy; Senior Analyst, ORN Informatics; Team Lead, ORN Informatics). The email was sent in order to get	2016-09-29	[The Team Lead, ORN Informatics had deleted the email from all folders in their Outlook, and advised her colleagues to do so as well. All CCO recipients of the PHI have confirmed deletion including the Team Lead, Data Management, who was away at the time of the breach. Group Manager, Funding Policy & Operations advised the sender on the 15th of the incident. Sender expressed that ORRS	9/15/2016 Notified sender (their data).	2016-10-05	Privacy Specialist	Policy breach	PE breach	Privacy supported the response of the Businss Unit to the sender.	Business Unit & Privacy Specialist	N/A	See "recommendations".	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						clarification on the eligibility status of the referenced patients, based on the revised pre-dialysis eligibility criteria that were implemented on April 1st and the new supporting report first released to CKD programs in June.]		PID is not PHI.										
ORN	2016-09-19	2016-09-20	Internal	2016-09-21	Email breach. Email contained 9 records with HINs.	[PHI was included in an email to a Team Lead and Sr. Specialist (1) from a Sr. Specialist (2), all within CCO. The email was sent in an effort to resolve an issue the sender was having with submitting data for GI Endo project. The sender and two recipients were each authoritzed to view the source data holding.]	2016-09-20	[The sender deleted the email from their inbox, sent and deleted items folders. The Sr. Specialist (1) emailed the sender to let him know that the email he had sent contained PHI, and instructed everyone on email chain to delete the email from their inbox, sent items and deleted items folders. All recipients have confirmed deletion of the email.]	N/A - internal	2016-09-21	Privacy Specialist	Policy breach	PE breach	Privacy added: "From a privacy perspective, we would recommend ensuring that the original sender is aware that email is not a secure method of transferring PHI. For more information regarding secure methods of transfer, please see CCO's Secure Transfer of PHI Standard. Please let me know if you have any questions."	Business Unit & Privacy Specialist	N/A	See "recommendations". On 9/21/2016 the Team Lead who submitted the breach agreed that they would carry out the recommendation.	2016
ORN	2016-09-20	2016-09-20	External	2016-09-21	Fax breach. PHI included the patient's	PHI was included in a faxed	2016-09-26	[9/20/2016: The Privacy Specialist	9/26/2016	2016-09-30	Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "containment measure".	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
					name, address, telephone number, HIN, and date of birth.	Ontario Renal Network (ORN) Outpatient Nephrology Referral Form, sent through CCO's main fax line. The fax was brought to the attention of a privacy specialist.		notified the Senior Specialist, ORN of the breach. She purged the electronic copy of the fax from the Legal and Privacy Office mailbox and will transfer a hardcopy of the fax to the Senior Specialist. 9/20/2016: Hard copy of fax transferred to the Senior Specialis, ORN. 9/26/2016: After 2 unsuccessful attempts, Senior Specialist, ORN successfully contacted referring primary care provider's office to inform them of the breach and provide next steps. Referral package was put into a shredder box to be securely destroyed. A follow-up fax was sent to the primary care provider's office	Notified sender (their data).									

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
								confirming next steps.]										
P&RP	2016-09-21	2016-09-21	Internal and External	2016-09-27	Email breach. Email contained HIN and treatment information for 7 patients.	PHI was included in an email from hospital to the Group Manager, Funding Implementation & Operations in error. The Group Manager then forwarded the email to the Director, Funding Unit and the Director, Regional Program Development.	2016-09-21	The Group Manager sent an email to both Directors and the original sender, requesting that everyone delete the emails from their inboxes, sent items and deleted items folders. All have confirm that the above action was taken. The Group Manager also did the same.	9/21/2016 Notified sender (their data).	2016-09-30	Senior Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "containment measure".	2016
P&CC	2016-09-22	2016-09-22	Internal	2016-09-22	Fax breach. Other info N/A.	PHI was faxed to CCO. The form that was faxed should have been completed electronically using eClaims. The NDFP must collect the PHI that was included in the fax to administer the program.	N/A	N/A	N/A	N/A	Senior Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	N/A	2016
ORN	2016-09-26	2016-09-26	External	2016-09-28	Fax breach. PHI included the patient's name, address, telephone number, HIN, and date of birth.	PHI was included in a faxed Ontario Renal Network (ORN) Outpatient Nephrology	2016-09-29	[9/28/2016: The Privacy Specialist notified the Analyst, ORN of the breach. She purged the electronic	9/29/2016 Notified sender (their data).	2016-10-03	Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "containment measure".	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						Referral Form, sent through CCO's main fax line. The fax was brought to the attention of a privacy specialist.		copy of the fax from the Legal and Privacy Office mailbox and will transfer a hardcopy of the fax to the Analyst. 9/28/2016: Hard copy of fax transferred to the Analyst, ORN. 9/29/2016: Analyst, ORN successfully contacted referring primary care provider's office to inform of breach and provide next steps. The referral package was put into a shredder box to be securely destroyed. A follow-up fax was sent to the primary care provider's office to confirm next steps.]										
LPO	2016-09-28	2016-09-28	External	2016-10-04	Fax breach. Fax contained patient reports. Details unclear.	PHI was faxed to CCO via CCO's main fax line by hospital. The fax later came to the attention of the Privacy Specialist,	2016-09-28	Privacy specialist contacted hospital regarding the fax. The Manager of Health Records at Sunnybrook determined	9/28/2016 Notified sender (their data).	2016-09-28	Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "containment measure".	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						LPO. The purpose of the fax was unclear. The Privacy Specialist saved a copy of the fax to the H: drive to facilitate investigation.		that the fax was intended for a health care provider and said that their office would contact the provider's office to obtain the correct fax number. The Privacy Specialist communicated that the fax would be destroyed at CCO and deleted the copy from the H: drive.										
CTO	2016-09-29	2016-09-30	External	2016-10-05	Email breach. Unclear what contents were there.	[PHI was included in an email from hospital to the Technical Support Associate at CCO.The email was sent in an effort to resolve an issue the sender was having while sending HL7 message to OPIS but failed to process. On the bottom it said no PHI info but PHI was there.]	2016-09-30	[Technical Support Associate deleted the email from their inbox and deleted items folders. They emailed the sender, informed them that the email they had sent contained PHI, and instructed them to delete the email from their sent items and deleted items folders. They also created a second ticket without PHI and	9/30/2016 Notified sender (their data).	2016-10-07	Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "containment measure".	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
								assigned to the appropriate Group. They then closed the ticket with PHI in it.] [Email to sender: "Please note that your original e-mail contained Personal Health Information (PHI) and we have subsequently removed the PHI from the email body below. We have also permanently deleted the e-mail from our Inbox and Deleted Items. Please do the same in your mailbox's Sent Items and Deleted Items....If you deem it necessary, please resend the original information, without PHI. You may use Interface Message ID or Waitlist Entry ID to reference a patient..."]											

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
LPO	2016-10-04	2016-10-04	External	2016-10-11	Faxed report. PHI included patient name, DOB, and MRN.	PHI was faxed by the hospital to the CCO main fax line, and was brought to the attention of the Privacy Specialist.	2016-10-27	Privacy Specialist retained an electronic copy of the fax on the H: drive. She contacted hospital and left a voicemail requesting the reason for the fax being sent. After multiple attempts to contact hospital Health Records without being able to reach anyone, she contacted their Privacy office and was able to coordinate an in-person transfer of PHI. Privacy at hospital is now aware of the PHI and noted that they would further investigate what led to the breach. The Privacy Specialist deleted the electronic copy of the fax from CCO systems on 10/27/2016.	10/4/2016 Notified sender.	2016-10-27	Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "containment measure".	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
ORN	2016-10-05	2016-10-11	External	2016-10-21	Fax breach. PHI included the patient's name, address, telephone number, HIN, and date of birth.	PHI was included in a faxed Ontario Renal Network (ORN) Outpatient Nephrology Referral Form, sent through CCO's main fax line. The fax was brought to the attention of a privacy specialist.	2016-10-18	10/11/2016: The Privacy Specialist notified the Senior Specialist, ORN of the breach. She purged the electronic copy of the fax from the Legal and Privacy Office mailbox and will transfer a hardcopy of the fax to the Senior Specialist. 10/12/2016: Hard copy of fax transferred to the Senior Specialist, ORN. 10/18/2016 - Senior Specialist, ORN successfully contacted referring primary care provider's office to inform of breach and provide next steps and referral package was put into a shredder box to be securely destroyed. A follow-up fax was sent to the primary care providers office to confirm next steps.	10/18/2016 Notified sender.	2016-10-24	Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "containment measure".	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
CTO	2016-10-12	2016-10-13	External	2016-10-21	Email breach. Email included patient's MRN.	[PHI was included in an email sent to ITServicedesk@cancercare.on.ca email in reference to OPIS printing problem for labels.	2016-10-13	[Associate created a second support request using the appropriate template to address the customer's issue, without PHI. The Privacy & Access office was informed of the incident via email. The sender was sent the following message: "Please note that the following e-mail contained Personal Health Information (PHI). Please see the attached copy with the PHI removed. We have removed the e-mail from our Inbox and Deleted Items. Please do the same in your mailbox's Sent Items. A separate support	10/13/2016 Notified sender.	2016-10-17	Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "containment measure".	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
								request has been created to address your original issue... If you deem it necessary, please resend the original information, without PHI. You may use Interface Message ID or Waitlist Entry ID to reference a patient..."]										
ORN	2016-10-13	2016-10-13	External	2016-10-21	Fax breach. PHI included the patient's name, address, telephone number, HIN, and date of birth.	PHI was included in a faxed Ontario Renal Network (ORN) Outpatient Nephrology Referral Form, sent through CCO's main fax line. The fax was brought to the attention of a privacy specialist.	2016-10-19	10/13/2016: The Privacy Specialist notified the Senior Specialist, ORN of the breach. She purged the electronic copy of the fax from the Legal and Privacy Office mailbox and will transfer a hardcopy of the fax to the Senior Specialist. 10/18/2016: Hard copy of fax transferred to the Senior Specialist, ORN 10/19/2016 - Senior Specialist, ORN successfully contacted referring primary care	10/19/2016 Notified sender.	2016-10-20	Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "containment measure".	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
								provider's office to inform of breach and provide next steps and referral package was put into a shredder box to be securely destroyed. A follow-up fax was sent to the primary care providers office to confirm next steps.										
CPQI	2016-10-13	2016-10-13	Internal	2016-10-21	Email breach. Email included patient name and clinical info. (Stem Cell program)	PHI was included in an email from CCO employee to several other CCO employees in the SSO program. Email was sent to follow up on patient case status.	2016-10-14	Recipient deleted email from inbox and deleted folder, contacted sender and others to inform them of the breach and requested not to send emails with PHI .	10/14/2016 recipient notified sender and others copied on theemail.	2016-10-14	Senior Privacy Specialist	Policy breach	PE breach	N/A	N/A	N/A	N/A	2016
A&I	2016-10-18	2016-10-19	External	2016-10-21	Email breach. PHI included patient chart number and drug information.	[PHI was included & sent back in an email by a Pharmacist at hospital o STIP@cancercare.on.ca regarding a CCO helpdesk ticket.]	2016-10-19	[Recipient (Analyst Technical Support, OPIS) emailed the sender, and informed them that they had sent email containing PHI. Original email response was deleted from the inbox and deleted folder.	10/19/2016 Notified sender.	2016-10-27	Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "containment measure".	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
								Advised original user of breach and to not send PHI data on an email to CCO.]										
CPQI	2016-10-21	2016-10-21	External	2016-11-02	Email containing patient initials and health card number.	An email was sent by a hospital to a reimbursement analyst containing patient initials and a health card number.	2016-10-21	The reimbursement analyst hard deleted the email from outlook and notified the hospital of the breach. The hospital was instructed to hard delete the email from Outlook and was reminded to not send PHI to CCO via email.	2016-10-21	2016-10-21	Senior Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	N/A	2016
ORN	2016-10-25	2016-10-26	External	2016-11-02	Fax breach. PHI included the patient's full name, date of birth, name of the referring physician, and clinical information.	PHI was included in a faxed Ontario Renal Network (ORN) Outpatient Nephrology Referral Form, sent through CCO's main fax line.	2016-10-27	10/26/2016: The Privacy Specialist notified the Senior Specialist, ORN of the breach. She purged the electronic copy of the fax from the Legal and Privacy Office mailbox and will transfer a hardcopy of the fax to the Senior Specialist. 10/26/2016: Hard copy of fax transferred to the Senior Specialist, ORN	10/27/2016 Notified sender.	2016-11-14	Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "containment measure".	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
								10/27/2016 - Senior Specialist, ORN successfully contacted referring primary care provider's office to inform of breach and provide next steps and referral package was put into a shredder box to be securely destroyed. A follow-up fax was sent to the primary care providers office to confirm next steps.										
ORN	2016-10-26	2016-10-27	External	2016-11-02	Fax breach. PHI included the patient's full name, date of birth, HIN, address, name of the referring physician, and clinical information.	PHI was included in a faxed Ontario Renal Network (ORN) Outpatient Nephrology Referral Form, sent through CCO's main fax line.	2016-10-27	10/27/2016: The Privacy Specialist notified the Senior Specialist, ORN of the breach. She purged the electronic copy of the fax from the Legal and Privacy Office mailbox and will transfer a hardcopy of the fax to the Senior Specialist. 10/27/2016: Hard copy of fax transferred to the Senior Specialist, ORN	10/27/2016 Notified sender.	2016-11-14	Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "containment measure".	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
								10/27/2016 - Senior Specialist, ORN successfully contacted referring primary care provider's office to inform of breach and provide next steps and referral package was put into a shredder box to be securely destroyed. A follow-up fax was sent to the primary care providers office to confirm next steps.										
CPQI	2016-10-28	2016-10-31	External	2016-11-09	Fax breach. Fax contains PHI including patient's name, HIN, MRN, DOB, sex, admitted date, clinic date, and clinical notes.	Fax sent from hospital containing PHI. Privacy was made aware 10/31/2016.	2016-11-11	Privacy Specialist attempted to call hospital Privacy Office on October 31st, and left a message. She later received a call back requesting that the PHI be sent back to the PHI. PHI was sent back by courier. On Nov 8th the Privacy Specialist received a call back from hospital Privacy Analyst	10/31/2016 Notified sender.	2016-11-29	Privacy Specialist	Policy breach	PE breach	N/A	Privacy Specialist	N/A	See "containment measure".	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
								advising that they had received the couriered PHI. On closer review they concluded that it was intended for a CCO program (specifically NDFP), making it a breach of procedure/policy breach. The Privacy Analyst verified that they had 1) communicated the error with the internal sender, 2) resent the file through the correct method (an online portal) and 3) will ensure that the same error is not made in the future. The Privacy Specialist, who had saved a copy of the PHI to the H: drive for investigation purposes, deleted this file from the H: drive on Nov 11th.										
ATC	2016-10-31	2016-10-31	External	2016-11-09	Fax breach. Fax contained clinical	A fax containing PHI was accidentially	2016-11-01	The fax was hard deleted from Outlook. The	2016-11-01	2016-11-01	Senior Privacy Specialist	Privacy breach	PE breach	N/A	Privacy Specialist	N/A	N/A	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
					records that included medication history and diagnosis, as well as OR scheduling information for 16 patients.	sent to CCO. The Physician was trying to send the records from their practice at one hospital to another facility where they also practice.		Privacy Specialist phoned the physician to notify them of the breach. The hard copy printout of the fax was securely shredded.										
Office of the President	N/A	2013-11-30	External	2014-01-14	Fax breach. PHI contained name and description of diagnosis.	PHI was faxed to the Executive Assistant of the Office of the President [by whom?], requesting a certain drug to be covered by the Province on basis of compassionate review policy.	2013-10-31	The EISO confirmed that the PHI was saved in a P: drive location accessible to six employees, and it is unlikely the file was accessed. Nonetheless the file was transferred from the P: drive to the new LPO H: drive location.	2013-10-31	2013-11-04	Senior Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	2013-11-04	See "Containment Measure".	2013
ATC	N/A	2014-01-08	External	2014-05-09	Email breach. Data files contained MRN and hospital account number.	MRI program data was due to be submitted via MFT, However, the Coordinator at Hospital could not access MFT. Instead, she emailed the MRI data submission template containing record-level data for several patients.	2014-01-08	ATC asked all recipients of the email with PHI to delete the email from their mailboxes. ATC also asked the recipients not to email PHI to CCO. Finally, ATC reached out to the sender to confirm which staff at the facility are registered MFT users,	N/A	2014-01-08	Senior Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2014

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
								to avoid future breaches. The hospital Coordinator confirmed that they deleted the email on their side.										
ORN	N/A	2014-01-30	External	2014-07-16	Email breach. PHI included patient name and DOB.	An email containing PHI was sent to CCO [by whom?], to troubleshoot a technical issue that occurred when the sender tried to edit patient DOBs in the ORRS.	2014-01-30	A service analyst noticed the PHI and deleted the email from all mail folders on CCO's end. They advised the sender to not send PHI via email to CCO. A reminder notice [was posted?] in the weekly bulletin to all Ontario Renal Reporting System users to not submit PHI in emails.	N/A	2014-01-30	Senior Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2014
ATC	N/A	2014-02-07	External	2014-08-08	Email breach. Data files contained MRN and hospital account number.	Hospital submitted MRI program data to CCO via MFT. ATC contacted the hospital to correct this [unclear - perhaps it was the wrong data?]. The hospital then sent an email to	2014-02-07	ATC asked all recipients of the email to delete the email from their mailboxes. ATC also asked the recipients not to email PHI to CCO. The hospital Coordinator confirmed that they deleted the	N/A	2014-02-07	Senior Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2014

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						CCO with attached monthly data files containing PHI.		email on their side.										
ATC	N/A	2014-02-13	External	2014-08-08	Email breach. PHI included MRN and hospital number.	Hospital added an MRI at a new site and were having trouble separating the data from each MRI site for their data submission to CCO. CCO asked to review a copy of the hospital's raw data, in order to help resolve the issue. The hospital Coordinator then sent an email to another staff member, asking them to upload the raw data file; the email contained record-level data and a Senior Business Analyst (at CCO?) was also copied.	2014-02-13	The sender was notified of the breach [by whom?], and was asked to remove the thread from his inbox and deleted items folder. The sender was cautioned not to send PHI via email.	N/A	2014-02-13	Senior Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2014
ATC	N/A	2014-02-21	External	2014-09-09	Email breach. PHI included patient name, HINs, types of procedures, and procedure date.	A hospital emailed unencrypted PHI to the ATC support desk. The support desk then sent it to the ATC Senior Team Lead. [In the ticket there	2014-02-21	The Senior Team Lead will ensure that the email containing PHI is removed from the ATC Service Desk ticket, and [unclear	N/A	2014-02-21	Senior Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2014

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						is also mention of the PHI being saved to an unencrypted USB key.]		- think they intended to contact the sender to ensure that they will no longer send PHI via email.] The Senior Team Lead deleted the file from the unencrypted USB key.										
CPQI	N/A	2014-03-06	Unclear	2014-12-11	Email breach. PHI included patient name, chart number and appointment date.	An email containing PHI was sent to CCO [by whom?], to troubleshoot a technical issue that occurred when trying to upload CSV files [to which database?]. A CCO project manager received the email with the PHI.	2014-03-06	The project manager asked the sender to delete the email from all folders, and reported the suspected breach to the LPO. The sender was cautioned not to send PHI via email.	N/A	2014-03-06	Senior Privacy Specialist	Privacy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2014
CPQI	N/A	2015-11-20	External	2015-11-24	Email breach. Attachment contained PHI. [On further investigation: Information included in the clean password protected data file included responses to the anonymous survey (response rate 557).	From submitter, Lead of Patient Experience Measurement: Through review of project report we realized that there was outstanding deliverables. When we went back to previously sent deliverables we identified a privacy	2015-11-20	• Flagged immediately for [name omitted] Director, Person-Centred Care. •[Recipient - Lead, Person-Centred Care] deleted email from inbox. [From submitter: the email has been	11/20/2015 Notified vendor. PHI was for CCO's own pilot.	2015-11-25	Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2015

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
					NOTE the information is de-identified. The survey consists of 28 questions (18 core questions; 2 open-ended responses; 8 demographic questions). The demographic questions included gender, age range, education, born in Canada, how long lived in Canada and FNIM.] [A copy of the questionnaire is available.]	breach. ...As part of the validation study for ePREMs, the vendor sent a clean data file with all responses from validation pilot by email. [On further investigation: recipient of the data was authorized to view the data. From submitter: the responses were on [cloud software as a service] however once the survey closed it was not accessible. In addition, the vendor had to share the clean data as part of their agreement.] [As the actual breach took place prior to 11/20/2015, exact date unavailable.]		deleted from my inbox and mail folder in my inbox.] [Also: an email has been sent to the vendor notifying them and requesting a plan for secure transfer of raw data for future analytics purpose.]									
P&RP	N/A	2016-03-07	External	2016-03-16	Email breach. The PHI consisted of 1 HIN, plus disease &	[In late Feb 2016, an email containing PHI was emailed to Manager,	2016-03-07	[The manager emailed the original sender, explaining the privacy	3/7/2016 Notified sender (their data).	2016-03-17	Privacy Specialist	Policy breach	PE breach	N/A	Business Unit	N/A	See "Containment Measure".	2016

Program	Date of the breach	Date breach was identified or suspected	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Breach of policy or privacy?	Applicable legislative authority	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
					treatment information.	Funding Implementation & Operations, via STFM@cancercare.on.ca (team's joint inbox). PHI was identified in the email some time after. The sender of the email was a pharmacist at Hospital. They wanted to know if a particular case was going to be funded via the Systemic Treatment Quality Based Procedure funding model. 4 individuals have access to the STFM mailbox; they would normally use an SSL portal to share PHI.]		breach and requesting that all emails be deleted from their sent boxes and deleted items. The manager then deleted all emails from their inbox and deleted items.]										

Presccribed Person – non-CC

Program	Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
P&CC	2013-10-28	2013-11-06	External/Internal	2013-10-31	PHI - first and last name, phone number, address, OBSP and CCC test dates.	Email from client to a former VP of Prevention and Cancer Screening at his work email address containing PHI - first and last name, phone number, address, OBSP and CCC test dates. Email was then forwarded to current VP who then forwarded it to Managing Director, Cancer Screening. Then forwarded on to the director, Provincial Operations who then also reforwarded it to Sr. Manager, Contact Centre who then printed it and delivered it to Analyst at Contact Centre.	2013-11-06	Manager, Contact Centre printed it and delivered it to Analyst at Contact Centre. Analyst reported the breach to Privacy. All affected people were told to deleted it from all mail folders. Client's email was uploaded to InScreen from the server on H Drive. Hard copy was destroyed	2013-10-28	2013-11-06	Senior Privacy Specialist	Privacy breach	All directed to delete email from all mail folders	Business Unit	2013-11-06	N/A	2013
P&CC	2013-11-04	2013-11-05	Internal	2013-11-05	Training breach. PHI was 1 or 2 pathology reports from the OCR (eMaRC application).	PHI was exposed to one individual who was not yet authorized to view OCR data during a training session.	N/A	The perpetrator of the breach acknowledged their error in displaying PHI during the training when one person had not yet received full approval to	N/A - internal	N/A	Privacy Specialist	Privacy breach	N/A	Business Unit	N/A	See "Containment Measure".	2013

Program	Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
								access the PHI.									
P&CC	2013-11-12	2013-11-12	Internal	2013-11-13	PHI - chart number, client name, appointment date and hospital site	Accounts payable received 9 hard copy of pages containing PHI for 30 patients which was included with screening invoices	2013-11-13	Finance reported breach to LPO. Sender notified.	2013-11-13	2013-11-13	Senior Privacy Specialist	Privacy breach	Director, Regional programs notified of the breach	Business Unit	2013-11-13	N/A	2013
P&CC	2013-11-13	2013-11-13	Internal	2013-11-13	client's results of pap test	voicemail from client with personal information - results of Pap test - complaining about CCO's practice of mailing out results letters. Voicemail was forwarded to Privacy Office Manager and Analyst as an attachment to an email to resolve the caller's request to be withdrawn from correspondence. Email then forwarded to CSR	2013-11-13	email was deleted from all folders by all involved and informed not to forward voicemails with PHI but to upload to client's InScreen record	2013-11-13	2013-11-13	Senior Privacy Specialist	Policy breach	email was deleted from all folders by all involved and informed not to forward voicemails with PHI but to upload to client's InScreen record	Privacy Specialist	2013-11-13	N/A	2013
P&CC	2013-11-15	2013-11-18	External	2013-11-15	PHI - name, Physician name, description of medical test	fax with PHI - name, Physician name, description of medical test received by CCO receptionist was email to Screening at	2013-11-15	Project Coordinator contacted Contact Centre to confirm that fax should be directed to them. Then contacted LPO to request fax	2013-11-15	2013-11-15	Senior Privacy Specialist	Privacy breach	Project Coord. And receptionist to delete it from email and fax folders. Contact Center to contact physician's office to notify	Business Unit	2013-11-15	N/A	2013

Program	Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						Cancercare.on.ca		be deleted from all sources. Print the fax and have it delivered to Contact Centre in person					them of the breach and have them redirect inquiry to a screening site				
P&CC	2013-11-19	2013-11-25	internal	2013-11-19	PHI in an email i.e. patient name	PHI in an email i.e. patient name was sent by an Analyst to the Contact Centre in an effort to resolve an inquiry from a member of the public	2013-11-19	Analyst alerted the sender to delete the email and informed LPO.	2013-11-19	2013-11-19	Senior Privacy Specialist	Privacy breach	Sender reminder to follow established Contact Centre procedures	Business Unit	2013-11-19	N/A	2013
CTO	2015-04-17	2015-04-20	External	2015-04-20	Email breach. Email contained appointment information, HIN, MRN, DOB, and gender.	The Pathology mailbox was emailed PHI by a user which was a breach of procedure... Everyone with access to the Pathology mailbox is authorized to handle the PHI contained. The person who emailed the PHI masked the PHI by inserting blocks over the PHI but the PHI was still available and visible. [Note: under timeline, states that the user was from Life Labs]	2015-04-20	An email reply was sent to the user notifying of the breach, ways to avoid future breaches, steps to delete the email, informing them to notify their Privacy office. Pathology mailbox was removed of the email [Note: specified in part B that they "deleted the message from the inbox and the deleted folder"]. Breach form was filled out.	2015-04-20	2015-04-20	Privacy Specialist	Policy breach	N/A	Business Unit	N/A	See "Containment Measure".	2015

Program	Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
P&CC	2015-06-18	2015-06-18	External	2015-06-18	Email breach. PHI included HIN and address for approximately 30 records (OBSP clients).	PHI data...was included in an email to [Senior Analyst, Implementation, Cancer Screening] from an individual at the Hospital. The email was sent in an effort to investigate some cases where centralized Ontario Breast Screening Program correspondence letters could not be sent due to a bad mailing address.	2015-06-18	• [Senior Analyst] deleted the email from her inbox and the deleted items folder • [Senior Analyst] phoned the sender to inform them not to send PHI via email and that the email must be deleted from all folders	2015-06-18	2015-06-18	Privacy Specialist	Privacy breach	N/A	Business Unit	N/A	See "Containment Measure".	2015
P&CC	2015-06-24	2015-06-26	External	2015-06-26	Email breach. PHI included first and last name, residential address, and an unspecified file number – possibly a health service provider-specific identifier.	A member of the general public sent an email to datarequest @cancercare .on.ca listing their personal information. The individual had sent this info in order to update their address information within CCO data holdings. The associate analyst monitoring the datarequest inbox reviewed this email for the	2015-06-26	The associate analyst contacted her privacy representative, noting the nature of the breach and requesting next steps. The senior privacy specialist advised that a hardcopy of the email be printed and provided to CCO's contact centre for follow-up. The associate analyst then deleted the electronic	N/A	2015-06-26	Privacy Specialist	Privacy breach	N/A	Business Unit	N/A	See "Containment Measure".	2015

Program	Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						first time two days later.		copy of the request from the datarequest inbox and from the deleted items folder. ...Contact center to shred the copy once the changes have been documented.									
CTO	2015-07-03	2015-09-28	Internal	2015-09-28	Breach in the ICMS ticketing system. The first PDF file attached to Ticket 219884 contained 11 patients, and the following fields: time type, con, stat, client name, hospital ID, HIN, physician, telephone, screening type, DOB, chart number, special needs, external mammogram, films, charts. The 2 other PDF files contained the following PHI: - Ticket 224109, 23 patients: chart number, screen number, screen date, clinical	From submitter, Team Lead, Development and Architecture Services: PHI data was included in a PDF file attached to a ticket in our ticketing system (TFS) for the ICMS project. The PDF was attached by [name omitted], Business Analyst with PMCS at CCO. The PDF was attached as part of a description for system requirements. Subsequently, two more PDF attachments were deleted from TFS as a precaution because they contained a patient chart number with	2015-09-28	[Senior Developer] deleted the attachment from the TFS ticket 219884. [Senior Developer] queried TFS for all Requirements for the ICMS project submitted by [the original uploader] to evaluate if any other attachments contained PHI. As a precaution, the attachments for two more tickets were deleted (224109 & 224759) because they contained patient chart number with the site name.	N/A - internal	2015-09-28	Privacy Specialist	Policy breach	N/A	Business Unit	N/A	See "Containment Measure".	2015

Program	Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
					information, etc. - Ticket 224759, 20 patients: chart number, screen number, DOB, clinical information, family history, etc.	the site name. ...There are 43 user accounts that could have had access to the PDF file. 18 of those are contractors outside of CCO. The TFS system only audits write activities to the system...so the exact number of people who have accessed the PDF file is not known. The issue was discovered by...a Senior Developer, who has an [approved access] for PHI on the ICMS project.											
P&CC	2015-07-22	2015-07-22	External	2015-07-22	Email breach. PHI included DOB, first and last name, HIN.	[PHI was included in an email to CCO [analyst, Cancer Screening Evaluation and Performance Management] from a CML lab analyst. The email was sent in an effort to resolve resubmission issue of missing fecal occult blood	2015-07-22	[• Analyst instructed in a separate e-mail all parties involved to delete the email immediately from their inbox, deleted items and sent items Outlook folders. Analyst also reminded CML of CCO Privacy policy not to send	N/A	N/A	Group Manager, Privacy	Policy breach	Question from Privacy: Is there a protocol in place with labs detailing the process for communicating these type of issues with CCO? Does this protocol include the type of information labs can include in an email response to CCO?	Business Unit	N/A	N/A	2015

Program	Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						test (FOBT) kits. CCO IT noticed missing laboratory reporting tool (LRT) FOBT data loads. The analyst requested the lab to resubmit. The lab checked and confirmed that there were multiple attempts to resubmit, but there seemed to be a technical issue preventing resubmission. An email was sent by CML to 3 CCO staff, containing a screen shot with PHI...from the submission file.]		PHI data by e-mail. • Analyst deleted the file from her inbox and deleted items folder. The CML lab analyst confirmed that she deleted the e-mail on her end and that she would follow up with parties involved at the lab.]					A from P&CC: ...during the investigation process between CCO and the labs, it is permitted to share accession #id number that lab assigns to a result by e-mail (non-PHI). PHI data (First Name, Last Name, HIN etc. any other detail that could identify a patient) are not permitted to be shared by e-mail... Question from Privacy: Is there any procedure developed between labs and CCO in regards to how to communicate issues related to FOBT? If there is none then I suggest we draft a procedure and communicate to labs to ensure that labs have documented understanding of what type of information can be communicated via email. I will review				

Program	Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
													the agreement in detail as well (I reviewed it quickly and I did not see any procedure related to communication being part of the agreement).				
PSC	2015-08-13	2015-08-19	Internal	2015-08-19	Email breach. PHI contained name, birthday and address information for approximately 30 individuals.	PHI was included in an email to CCO employee [name omitted] (Sr. Programmer Analyst) and [name omitted] (Project Manager). The email was sent to provide the test sample data for Client Mailing, Film Bag and Wrist Band Labels as part of the ICMS Redesign QA testing. [Based on associated emails, believe sender was from CCO - Technology Services.]	2015-08-19	[Project manager] reported the suspected breach to Privacy Representative.	N/A	N/A	Group Manager, Privacy	Policy breach	Instructions given by the Project Manager to internal staff involved, based on Privacy advice: "Please delete the Client Mailing, Film Bag and Wrist Band Labels that was generated and emailed last week as this contains PHI information... [Recipient], please ensure to delete from your mailbox and the delete folder. [Sender], please ensure to delete it from your sent folder and the delete folder."	Business Unit & Privacy Specialist	N/A	N/A	2015

Program	Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
P&CC	2015-10-23	2015-10-23	External/Internal	2015-10-27	Email breach. PHI included the individual's family and personal medical history, attached to the individual's first and last name and email address.	A member of the public included PHI in an email to [name omitted], Radiologist-in-Chief of the Ontario Breast Screening Program and [name omitted], Provincial Lead Scientist of the Ontario Breast Screening Program (OBSP), to inquire about the OBSP's screening guidelines in response to a letter in the Globe and Mail. In an effort to provide a resolution to this inquiry, the email was then sent internally within CCO to [name omitted], (Director, Program Design), [name omitted] (Provincial Lead Scientist, OBSP), [name omitted] (Senior Analyst, Program Design), [name omitted] (Director,	2015-10-26	Upon discovery of the breach, all the recipients of the email containing the PHI were instructed to hard delete the email from their inbox and sent mail folder. Follow-up to the original email inquiry will be carried out by the Cancer Screening Contact Centre following appropriate privacy practices.	N/A	N/A	Group Manager, Privacy	Privacy breach	N/A	Business Unit	N/A	See "Containment Measure".	2015

Program	Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						Corporate Communications), and the Screen for Life mailbox. [The two directors did not have approved IDAR access to PHI, while the others did.]											
CTO	2015-11-07	2015-11-09	Internal	2015-11-10	Visual Studio Team Foundation Server (TFS) breach. Submitter believed that the PHI included client name, and perhaps HIN and DOB, for one individual.	On October 30 a screenshot for Bug 292269 with PHI information was uploaded to TFS by [name omitted] (CCO Senior Analyst) to TFS. Subsequently additional information was uploaded using the same screenshot to TFS by [name omitted] vendor QA tester. The information was sent to respond to defect that was encountered during user acceptance testing (UAT). ...Authorized members of the ICMS project team, both at CCO and [the vendor],	2015-11-09	The TFS administrator. ..was conducted to remove the PHI data in TFS. The data (Bug 292269) was removed on November 9 at 9:14 a.m. ...the content except for the PHI was put into a new TFS item, # 294029. An email was sent to the vendor [name omitted] to remind the vendor team to not upload PHI data into TFS. Another email was sent to [the original uploader] to remind everyone from CCO UAT testing teams to not upload PHI data to TFS.	11/9/2015 Notification to DapaSoft PM.	N/A	Group Manager, Privacy	Policy breach	N/A	Business Unit	N/A	See "Containment Measure".	2015

Program	Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						could have viewed it. [The submitter, a different senior analyst in Technology Services*], did view it and reported it. He is likely the only person to have viewed the TFS after the PHI was added, based on the TFS update history. *Current title.											
A&I	2015-11-20	2015-11-20	Internal	2015-11-24	Breach through a web portal. [On further investigation: the file uploaded contained 1744 individuals. Data source was the Ontario Cancer Registry.]	[An Excel file containing PHI was uploaded to the hospital web portal, in order to facilitate research. However the research data disclosure agreement allowing for CCO's disclosure was not yet fully executed.] [Associate analyst, Data Disclosure team uploaded a password-protected Excel file containing PHI to the hospital secure online portal in fulfillment of a research data request...The	2015-11-20	Contacted the recipient right away. [More from the submitter: We are unable to log back into the hospital secure file portal to delete the file but recipient from hospital has confirmed that the downloaded files were deleted.]	11/20/2015 Notified OCR team.	2015-11-26	Privacy Specialist	Privacy breach	Recommended that the submitter notify the Ontario Cancer Registry team within CCO of the breach. Further recommended that the data disclosure team implement a checklist for ensuring that all policy requirements (such as RDDA sign-off) are met prior to disclosure of the final research request package.	Business Unit & Privacy Specialist	2015-11-20	N/A	2015

Program	Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						associate analyst provided a password to the requestor, received confirmation that they had downloaded and could open the file, then realized that the research data disclosure agreement underlying the transaction was not fully executed. The recipients will not be authorized to view the data until this is done.]											
P&CC	2015-11-24	2015-11-25	External	2015-12-01	Email breach. The email included PHI in the form of a client's full name, phone number, and address.	PHI data was included in an email sent to the Screening inbox (a general inbox managed by Program Operations of Operations under Cancer Screening). The email was sent to Screening by an external stakeholder ([name omitted] from Hospital). [More info from submitter: RVH did intend to send the email to us.	2015-11-25	The email was permanently deleted on our end and instructions were emailed to [name omitted, external contact at Hospital] on how to permanently delete the email from his inbox. [Submitter confirmed that the email was deleted from all Outlook locations on CCO's end.]	2015-11-25	2015-12-03	Privacy Specialist	Policy breach	N/A	Business Unit	N/A	See "Containment Measure".	2015

Program	Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						Just gave us incorrect details. The email was intended for the screening inbox but they are not supposed to talk to us about PHI at all. In these situations they are advised to give a general overview without any specifics.]											
PSC	2015-12-09	2016-02-24	External	2016-02-24	ICMS breach. The Screening Detail Report within the newly redesigned ICMS contained PHI on 18 clients, including: • Client Name • HIN • Screening Result • Region OBSP Site Name	On December 9th, 2015, screenshots of the Ontario Breast Screening Program (OBSP)'s "Screening Details Report" with Personal Health Information (PHI) was inadvertently attached by CCO staff (Business Analyst) in Cancer Care Ontario (CCO) ticketing system (TFS). The screenshot was attached to TFS by the CCO staff to report a defect identified in the report during the User	2016-02-24	[The Developer Lead notified the CCO Project Manager and the Business Analyst of the presence of the PHI. The Project Manager requested the QA Lead to upload the copy of the screenshot to the H: drive and password protect it. The Project Manage informed the Privacy Specialist of the incident and confirmed steps required to contain the breach. The Project Manager instructed the Business	N/A	2016-02-24	Manager, Privacy	Privacy breach	Privacy has provided the following recommendations: 1) Advise CCO staff to not to attach documents containing PHI to the TFS 2) Notify Windsor Regional Hospital of the breach.	Business Unit & Privacy Specialist	2016-05-17	Email sent to staff reminding not to attach PHI in the TFS. Summary of the incident was sent to the HIC.	2016

Program	Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						Acceptance Testing (UAT) for the ICMS Redesign project. The breach was identified...when the CCO Developer Lead accessed the TFS investigate the defect... The TFS was accessed by the following four individuals. • vendor Manager • vendor Developer (offshore) • vendor Developer (onshore) • CCO Senior Developer		Analyst to remove the screenshot attachment from the TFS. Additionally the email reminded the team not to upload PHI data to TFS. The Business Analyst confirmed via email that the screenshot with PHI data has been removed from TFS.]									
A&I	2015-12-18	2015-12-18	External/Internal	2015-12-18	iPort breach. Unclear if individuals viewed PHI that they were not supposed to, however their permissions were configured in such a way that they could. Various iPort reports involved. See description for details.	From submitter, Group Manager, BI: In our internal review of user access on iPort (MicroStrategy tool hosting Cancer reports), we observed that (a) About five external users who are no longer associated with CCO had access to certain reports with PHI. (b) About 50 external users had access to	2015-12-23	1) Revoking user access a. Access to iPort was revoked for the five external users who are no longer associated with CCO b. Access to specific iPort reports with PHI data was revoked for the 50 users 2) Informed Cancer program managers about list of users and reports in question. User access for 50 users	N/A	2016-03-16	Privacy Specialist	Policy breach	Final recommendations for all iPort and iPort Access suspected privacy breaches that took place between Dec 2015 and Jan 2016 were sent on Mar 16, 2016 to key internal stakeholders. Resolutions: 1) • BI to validate all user profiles involved in iPort Access breaches, as well as all	Business Unit & Privacy Specialist	N/A	See "recommendations". BI later verified that all resolutions were carried out.	2015

Program	Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
						data for all RCCs for the below mentioned five Symptom Management reports that contained PHI data. (a) HCP Patient Reports (b) Chart Audit Tool (two reports) (c) Numerator (d) Denominator. The data included Patient name, DOB, Health card number, Disease, etc. The user would have to log into iPort (MicroStrategy tool hosting Cancer reports) to access these reports.		will be reinstated with appropriate security implemented based on advice from Cancer program managers.					CCAC profiles. • ATC program to advise BI development team when to re-enable user access. • Clinical Manager, ALC & MHA to confirm that profiles for CCAC users do not include access to PHI. • BI to consult with other programs using iPort and iPort Access to validate users. 2) • Revisit the resolutions from the June 2015 breach and determine whether they or a comparable alternative can be implemented. • Review the process of request submission and approval for both iPort and iPort Access; consult with Enterprise Information Security Office to ensure the process is secure and consistent with CCO's policies for				

Program	Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
													accessing PHI. The review and approval processes for iPort and iPort Access are currently being documented through the "OneID Process Redesign" initiative; this may provide an opportunity for improvement. "				
CTO	2016-01-04	2016-01-04	Internal	2016-01-08	Email breach. PHI included patient chart number, submitting hospital number, registration date, disease sequence number, visit hospital number, and program code, for 476 records.	[In the wake of a technical issue involving a secure portal, a Sr. QA Analyst at CCO sent an email containing PHI to 6 other CCO internal staff members. All were authorized to view the PHI.]	2016-01-04	[The Senior QA Analyst emailed the list of recipients to delete the email which has the attachment from their inbox and deleted item folders. After this breach incident took place, the Senior QA Analyst left the organization.] Unclear whether the individual deleted the email from their own inbox. Need to follow up with EISO. Update 4/15/2016: Was redirected to IT Ops. The information would now be	N/A - internal	2016-01-08	Privacy Specialist	Policy breach	Privacy Specialist wrote back to the Sr. QA Analyst: "...In general where PHI cannot be transferred via the appropriate secure mechanism, it should be transferred via an alternative approved mechanism rather than emailed. If unclear on what other transfer methods are available, please consult CCO's Secure Transfer of PHI Standard and/or engage the Enterprise Information Security	Business Unit & Privacy Specialist	N/A	N/A	2016

Program	Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
								encrypted and in offsite storage, where it will stay for 7 years.					Office prior to the transfer. Link to the standard: https://ecco.cancercare.on.ca/Divisions/Legal/Policy%20and%20Procedure%20Docs%208/Secure%20Transfer%20of%20Personal%20Health%20Information%20Standard.pdf"				
P&CC	2016-04-06	2016-05-05	External	2016-05-18	Email breach. Attachment contained Registered Nurse Flexible Sigmoidoscopy (RNFS) data (patient names, HINs) associated with 11 records.	[PHI was included in an email to CCO's Screening inbox from a booking clerk for colorectal screening at Hospital. The booking clerk was having difficulty submitting their PHI through the Data Submission Portal and therefore emailed the data. The breach was later detected when the same booking clerk later contacted an analyst on the Cancer Screening team regarding the April RNFS data submission.]	2016-05-05	The analyst notified the Screening inbox of the email in question, and informed the sender that he cannot send RNFS data by email. The CCO IT Service Desk is helping the booking clerk resolve their technical issue.]	5/5/2016 Notified sender (their data).	2016-05-13	Senior Privacy Specialist	Policy breach	CCO Cancer Screening staff to remind the booking clerk at the hospital that RNFS data cannot be submitted via email when experiencing issues with the DSP.	Business Unit	2016-05-05	On May 5, 2016, the Analyst with CCO Cancer Screening emailed the hospital. See "recommendation".	2016

Program	Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
P&CC	2016-04-28	2016-04-28	Internal	2016-05-04	Email breach. Attachment contained a screenshot that included the Client's Name, Chart Number and the Entry Date of one Mammogram screening.	PHI was included in an email [from an Analyst in P&CC] to [2 Senior Analysts in P&CC] at CCO. The email was sent in an effort to resolve discrepancies identified between the ICMS 2.1 Addendum to Business System Requirements Document and ICMS. The email included a word document that incorporated a list of discrepancies along with a screenshot image of the 4. Results tab on ICMS. The screenshot image was PHI. Another email was sent with an updated word document, with the same screenshot image of the same client's information. Both images contained PHI for one client.	2016-04-28	At 11:30 [On Apr 28th, one Senior Analyst] discovered the breach and verbally informed the sender...that the two emails contained PHI. [The Senior Analyst] then instructed [the sender] to delete the two emails from her Sent Items folder and Deleted Items Folder. At 11:32 AM [the sender] sent a third email that identified the discrepancies in a word document without PHI. [Both Senior Analysts deleted the email from their inbox and deleted items folder. The sender deleted the email from their sent box and deleted items folder, plus deleted the attachment containing PHI from her computer (M:drive) and recycling bin.]	N/A - internal	2016-05-13	Senior Privacy Specialist	Policy breach	N/A	Business Unit	N/A	See "containment measure".	2016

Program	Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
P&CC	2016-06-27	2016-06-27	External	2016-07-06	Email breach. Attachment contained PHI (including patient name, HIN, and FOBT result) for one patient.	[PHI was included in an e-mail from the lab to the Senior Analyst, Evaluation and Performance Management. The e-mail was sent in an effort to confirm whether CCO received an FOBT result from 2013 in the Laboratory Reporting Tool.]	2016-06-27	[The Senior Analyst emailed the original sender, advising him to delete the e-mail from his Outlook Sent and Delete folder. She reminded the user not to send any PHI by e-mail to CCO, and to only email accession number (non-PHI) for any FOBT result requests. The Senior Analyst also deleted the patient's partial last name in the subject line of the return email that she sent. She then filed a privacy breach with the Legal and Privacy Office, cc'ing her manager and the Manager, Lab Services.]	6/27/2016 Notified sender (their data).	n/a	Senior Privacy Specialist	Policy breach	N/A	Business Unit	N/A	See "containment measure".	2016

Program	Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
P&CC	2016-06-28	2016-06-28	Internal	2016-07-06	Dropbox breach. PHI included client names and health information.	[PHI was found in two drop box videos that were linked to defects logged in Team Foundation Server (TFS) for the ICMS Redesign Project. The videos were demonstrating system defects in ICMS 2.0 and exposed client names as well as other health information.]	N/A	[Senior Analyst, Cancer Screening Implementation contacted Privacy to determine next steps. Privacy contacted the Product Management team to determine if the data exposed in the video is client PHI or test data, and found that it was PHI. Privacy contacted the Strategy and Business Management team to determine who has access to TFS and could have potentially accessed the drop box videos. It was confirmed that individual who had access to the TFS for this detect were authorized to view the PHI. Product Management deleted the videos from Dropbox displaying PHI and the links to the videos from the TFS.] [Outcome of investigation: The first of	N/A - internal	2016-07-07	Manager, Privacy	Policy breach	Remind staff to not to attach PHI to TFS.	Business Unit & Privacy Specialist	2016-07-07	Sent out notice to screening staff reminding them not to attach PHI to TFS.	2016

Program	Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
								the two videos was created as part of ICMS triage and was recorded/edited for hiding PHI using Camtasia...Once done, the video was saved on Dropbox for Vendor testers to see how the defect is reproduced since sometimes they are not able to reproduce things that CCO sees happening in the system. Since Product Management does not have the original raw file from which the final video was made, he could not verify or deny if the masking failed or if the masking worked and the incorrect raw video was uploaded. Unclear whether the second video resulted from the same issue.] [Privacy notified the Manager of the									

Program	Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
								Enterprise Information Security Office of the incident, to note the use of off the shelf software for masking of PHI.]									
P&CC	2016-07-11	2016-07-26	External	2016-08-03	Email breach. Email contained one record (CCC program FOBT result).	[PHI was sent by e-mail from Lab Team Lead to Performance Analyst, Quality Management Program. The purpose was to resolve a missing FOBT record.]	2016-07-11	[Performance Analyst immediately deleted the email containing PHI. She sent a separate e-mail advising labTeam Lead not to e-mail any PHI data. For the purpose of resolving the missing FOBT result in LRT, non-PHI accession number is sufficient to communicate to CCO to investigate. The lab Lead acknowledged the error and apologized. This was an exception, one time occurrence. The Lead was eager to resolve outstanding missing results to	7/11/2016 Notified sender (their data).	2016-07-26	Privacy Specialist	Policy breach	N/A	Business Unit	N/A	See "containment measure".	2016

Program	Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
								submit to LRT.]									
P&CC	2016-09-22	2016-09-22	Internal	2016-09-22	Internal email breach. The email contained a HIN.	A report was shared internally among CCO staff via email for the purpose of discussing its content and methodology. The attachement to the email contained a HIN.	2016-09-22	9/22-2016: The email was deleted from the recipient's inboxes and deleted items folders by the recipients.	9/22/2016- Sender was notified	2016-09-22	Senior Privacy Specialist	Policy breach	N/A	Business Unit	N/A	See "containment measure".	2016
P&CC	N/A	2014-02-27	External	2014-02-27	Email breach. PHI included patient name and patient ID number.	PHI was sent via email to the Project Manager of Regional Operations [by whom?], in an effort to answer a patient-related question. The recipient of the PHI informed their Senior Manager in a separate email.	2014-02-27	The recipient reported the breach to the LPO. The email was deleted from all folders on CCO's side, and the sender was advised to do the same [by Regional Operations?). The sender was cautioned not to send PHI via email.	N/A	2014-02-27	Senior Privacy Specialist	Privacy breach	N/A	Business Unit	2014-02-27	See "Containment Measure".	2014

Program	Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
CTO	N/A	N/A	Internal	N/A	Breach was on the web but confined to internal viewers. PHI included one record. Unsure of contents.	[PHI was visible on the quality assurance (QA) and operational acceptance testing (OAT) site for the integrated cancer management system, https://icmsqa.cancercare.on.ca or https://icmsqas.cancercare.on.ca. A vendor had disabled the security feature during iterations. 1 record was visible on the site and was viewed by the Enterprise Information Security Office (EISO). The site was published internally, and could be viewed by anyone with knowledge of the URL.]	N/A	[Steps taken: 1. OPS (?) team was requested to disable the site, and IIS (?) for both QA and OAT. 2. The sites were disabled. 3. Vendor was asked to deploy the security component (authentication/authorization) in development, before moving to QA; as well as prior to QA deployment, as it has PHI. The EISO has asked the following be in place prior to turning on IIS in QA: a. Authentication is fully functional b. Authorization is in place c. Integration with [a security software] is fully operational and validated by EISO A Vulnerability Assessment was completed by EISO and no critical vulnerabilities were found.]	N/A - internal	N/A	Group Manager, Privacy	Privacy breach	N/A	Business Unit	N/A	See "Containment Measure".	N/A

Program	Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified	Nature of PHI	Description of breach	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	yr
								[From EISO: ...Since the link was not known to many people and the exposure was less than 2 weeks, we can probably affirm that internal employees are not actively looking for rogue links. All the people who had the link also had the clearance to view PHI in the context of developing the new ICMS solution.]									

Prescribed Person – CC

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
2012-11-24	2013-11-24	External	2012-11-24	Birthday letter opened by unintended recipient who returned the letter to the client	2013-11-26	CSR was able to contact client and confirm the correct address and a breach letter was sent	N/A	2013-11-26	Privacy Analyst	Privacy breach	None	CSR was able to contact client to confirm correct address	N/A	N/A	N/A	2013
2012-12-19	2013-12-19	external	2012-12-19	Results letter opened by unintended recipient	N/A	Unintended recipient called to say she received a results letter for someone else and had opened it.	N/A	2013-01-02	Privacy Analyst	Privacy breach	N/A	breach notification letter and a copy of the result letter was sent to client	N/A	N/A	N/A	2013

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
						Agreed to return letter. CSR contacted the client and confirmed the correct address.										
2013-09-19	2014-09-19	External	2013-09-19	Birthday letter opened by unintended recipient	2013-09-19	Unintended recipient, client's Sister-in-law opened the recall letter and gave it to the client.	N/A	2013-09-19	Senior Privacy Specialist	Privacy breach	None	CSR confirmed the client's phone #, contacted the client to update his address	N/A	N/A	N/A	2014
2013-11-01	2013-11-01	External	2013-11-01	Birthday letter opened by unintended recipient	2013-11-01	unintended recipient returned the client's opened birthday letter and marked "moved - pls remove from mailing list" on the letter. CSR attempted to call but no answer and no option to leave a voice mail; client does not have a PCP	N/A	2013-11-01	Senior Privacy Specialist	Privacy breach	N/A - no recommendations logged.	None	N/A	N/A	N/A - no recommendations logged.	2013
2013-11-04	2013-11-04	External	2013-11-04	Birthday letter opened by unintended recipient	2013-11-15	Unintended recipient received client birthday letter and agreed to return the letter. CSR was unable to contact client to update address	N/A	2013-11-15	Senior Privacy Specialist	Privacy breach	None	N/A	N/A	N/A	N/A	2013
2013-11-04	2013-11-04	External	2013-11-04	Results letter opened by unintended recipient	2013-11-04	The unintended recipient, client's mother received the results letter. She refused to return the letter as her daughter is in the military and her medical results should	N/A	2013-11-04	Senior Privacy Specialist	Privacy breach	None	N/A	N/A	N/A	N/A	2013

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
						not be sent to CCO. CCO investigated the origin of the test result and there are no agreement in place to prevent the results being reported to CCO. The breach occurred because CCO sent the result letter to an incorrect address. CSR was unable to contact the client										
2013-11-04	2013-11-04	External	2013-11-04	Results letter opened by unintended recipient	2013-11-04	Unintended recipient received and opened client's results letter and said he would destroy it. CSR asked via email that the letter be returned but has not been received to day. CSR attempted to call but was unsuccessful	N/A	2013-12-10	Senior Privacy Specialist	Privacy breach	None	N/A	N/A	N/A	N/A	2013
2013-11-05	2013-11-06	External	2013-11-05	Invitation letter opened by unintended recipient	2013-11-15	unintended recipient received the client's invitation letter and said she would return the letter (but was not received) Client has not lived at this address for 20 years. CSR was able to contact the client	N/A	2013-11-13	Senior Privacy Specialist	Privacy breach	None	N/A	N/A	N/A	N/A	2013
2013-11-07	2013-11-07	External	2013-11-07	Birthday letter opened by	2013-11-18	unintended recipient	N/A	2013-11-07	Senior Privacy Specialist	Privacy breach	None	N/A	N/A	N/A	N/A	2013

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				unintended recipient		received the client's birthday letter. CSR attempted to contact the client as a # provided by PCP. The client refused to authenticate.										
2013-11-07	2013-11-07	External	2013-11-07	Birthday letter opened by unintended recipient	2013-11-07	letter was returned in a MOHLTC envelope. CSR was unable to reach the client and he does not have a PCP; Canada411 did not provide a clear match	N/A	2013-11-07	Senior Privacy Specialist	Privacy breach	N/A - no recommendations logged.	None	N/A	N/A	N/A - no recommendations logged.	2013
2013-11-08	2013-11-08	External	2013-11-08	Results letter opened by unintended recipient	2013-11-08	client's result letter mailed back to CC. There is not contact # inScreen, client does not have a PCO and no definitive match in Canada 411. CSR was unable to updated client's address	N/A	2013-11-08	Senior Privacy Specialist	Privacy breach	N/A - no recommendations logged.	None	N/A	N/A	N/A - no recommendations logged.	2013
2013-11-12	2013-11-18	Internal	2013-11-12	Old address was disclosed in trying to obtain new address. CSR called back to confirm DOB but client declined and did not provide his DOB.	2013-11-12	Contact centre contacted the client to authenticate - thus a risk which deviates from established procedures used by Contact Centre	2013-11-12	2013-11-12	Senior Privacy Specialist	Privacy breach	CSR to make sure to all client's are properly authenticated before commencing address investigation	N/A	Contact Centre	2013-11-12	N/A	2013
2013-11-12	2013-11-20	External	2013-11-20	Fax with PHI sent from Rainy River	2013-11-20	Contact Centre logged inbound fax into InScreen	2013-11-20	2013-11-20	Senior Privacy Specialist	Policy breach	Sender called and informed of the breach and not to	N/A	Contact Centre	2013-11-20	N/A	2013

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				Medical centre. PHI included patient name, DOB and Biopsy results.		and reported the breach to LPO.					send PHI via fax in future					
2013-11-13	2013-11-13	External	2013-11-13	Results letter opened by unintended recipient	2013-11-13	unintended recipient received client's result's letter and agreed to return the letter but was never received and CSR was unable to contact them. CSR was able to contact the client at the number provided	N/A	2013-12-03	Senior Privacy Specialist	Privacy breach	None	N/A	N/A	N/A	N/A	2013
2013-11-13	2013-11-13	External	2013-11-13	Birthday letter opened by unintended recipient	2013-11-13	unintended recipient received client's result's letter and agreed to return the letter but was never received and CSR was unable to contact them. CSR was able to contact the client at the number provided and does not have a PCP	N/A	2013-11-13	Senior Privacy Specialist	Privacy breach	None	N/A	N/A	N/A	N/A	2013
2013-11-13	2013-11-13	External	2013-11-13	Results letter opened by unintended recipient	2013-11-13	Unintended recipient received and opened the client results letter and returned it. There is no contact information for the client in InScreen	N/A	2013-11-13	Senior Privacy Specialist	Privacy breach	None	N/A	N/A	N/A	N/A	2013
2013-11-13	2013-11-13	External	2013-11-13	birthday letter opened by unintended recipient	2013-11-13	Unintended recipient rec'd client's birthday letter	N/A	2013-11-13	Senior Privacy Specialist	Privacy breach	N/A - no recommendations logged.	None	N/A	N/A	N/A - no recommendations logged.	2013

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
						as client had moved abroad 10 years ago and agreed to return the letter CSR was unable to obtain correct address										
2013-11-14	2013-11-14	External	2013-11-14	Results letter opened by unintended recipient	2013-11-14	Unintended recipient rec'd her daughter's result letter and opened, nor sure if it was for her or her daughter as they have the same name. CSR verified that the letter was for her daughter who does not live at that address. Mother indicated she did not have the time to deliver the letter and would shred it. CSR was able to contact the client and update the address and a breach notification was sent out.	N/A	2013-11-14	Senior Privacy Specialist	Privacy breach	N/A - no recommendations logged.	None	N/A	N/A	N/A - no recommendations logged.	2013
2013-11-18	2013-11-20	External	2013-11-18	results letter opened by unintended recipient	2013-11-20	Unintended rec'd and opened the results letter and also had rec'd another letter. Client had not lived at the address for the last 16 yrs. and refused to mail back the letter. CSR was unable to	N/A	2013-11-20	Senior Privacy Specialist	Privacy breach	N/A - no recommendations logged.	None	N/A	N/A	N/A - no recommendations logged.	2013

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
						contact the client										
2013-11-18	2013-11-20	External	2013-11-19	Birthday letter opened by unintended recipient	2013-11-20	Unintended recipient, client's sister rec'd and opened the letter and returned it to CCO. CSR inactivated the address and no contact information is available.	N/A	2013-11-20	Senior Privacy Specialist	Privacy breach	N/A - no recommendations logged.	None	N/A	N/A	N/A - no recommendations logged.	2013
2013-11-19	2013-11-19	External	2013-11-19	Birthday letter opened by unintended recipient	2013-11-19	Unintended recipient received and opened the client results letter and said would return it as the client has moved abroad.	N/A	2014-02-05	Senior Privacy Specialist	Privacy breach	None	N/A	N/A	N/A	N/A	2013
2013-11-19	2013-11-20	External	2013-11-19	Birthday letter opened by unintended recipient	2013-11-20	Unintended recipient received and opened the client results letter and did not return it. There is no contact information for the that person. CSR was not able to contact the client as the phone number was disconnected. Client does not have a PCP	N/A	2013-11-20	Senior Privacy Specialist	Privacy breach	None	N/A	N/A	N/A	N/A	2013
2013-11-19	2013-11-21	External	2013-11-19	Birthday letter opened by unintended recipient	2013-11-19	Unintended recipient received client's birthday letter. The unintended recipient wrote the new address on the return mail. CSR was able	N/A	n/a	Senior Privacy Specialist	Privacy breach	none	N/A	N/A	N/A	N/A	2013

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
						to contact the client and update the address										
2013-11-19	2013-11-21	External	2013-11-19	Results letter opened by unintended recipient	2013-11-19	Unintended recipient received and opened the client results letter and did not return it; claimed it was sent back in March 2014. CSR was not able to contact the client	N/A	2014-03-07	Senior Privacy Specialist	Privacy breach	None	N/A	N/A	N/A	N/A	2013
2013-11-21	2013-12-23	External	2013-11-21	Birthday letter opened by unintended recipient	2013-12-23	unintended recipient received the client's birthday letter and said she would return the letter (but was not received) who has been living abroad for the past 15 years. No contact info or PCP listed for the client in InScreen.	N/A	n/a	Senior Privacy Specialist	Privacy breach	none	N/A	N/A	N/A	N/A	2013
2013-11-22	2013-11-22	External	2013-11-22	Birthday letter opened by unintended recipient	2013-11-22	Unintended recipient returned the client's birthday letter indicating client has moved abroad. CSR was unable to contact the client and does not have PCP	N/A	n/a	Senior Privacy Specialist	Privacy breach	none	N/A	N/A	N/A	N/A	2013
2013-11-22	2013-11-22	External	2013-11-22	Results letter opened by unintended recipient	2013-11-22	Unintended recipient, ad administrator at CAS, received client's results letter and returned letter with a note	N/A	2013-11-22	Senior Privacy Specialist	Privacy breach	N/A - no recommendations logged.	None	N/A	N/A	N/A - no recommendations logged.	2013

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
						saying client not longer a resident and no contact info is available. CSR was unable to obtain the correct address										
2013-11-23	2013-11-23	External	2013-11-25	Invitation letter opened by unintended recipient	2013-11-23	unintended recipient, client's mother opened the invitation letter and destroyed the letter as client has moved to B.C. CSR inactivated the address	N/A	2013-11-23	Senior Privacy Specialist	Privacy breach	N/A - no recommendations logged.	None	N/A	N/A	N/A - no recommendations logged.	2013
2013-11-25	2013-11-23	External	2013-11-25	Invitation letter opened by unintended recipient	2013-11-23	Unintended recipient, client's father opened the client's invitation letter, saying client had moved abroad year ago. Letter will be destroyed. CSR was unable to obtain address	N/A	2013-11-23	Senior Privacy Specialist	Privacy breach	N/A - no recommendations logged.	None	N/A	N/A	N/A - no recommendations logged.	2013
2013-11-25	2013-11-25	External	2013-11-25	Invitation letter opened by unintended recipient	2013-12-05	Unintended recipient received the client's letter and has not lived at the address for 12 years. CSR was unable to contact the client	N/A	2013-12-05	Senior Privacy Specialist	Privacy breach	none	N/A	N/A	N/A	N/A	2013
2013-11-26	2013-11-26	External	2013-11-26	Invitation letter opened by unintended recipient	2013-12-16	Unintended recipient rec'd and opened the client's invitation letter. Source was RPDB and his HIN was inactivated in	N/A	2013-11-26	Senior Privacy Specialist	Privacy breach	none	N/A	N/A	N/A	N/A	2013

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
						2011. CSR contacted the client at the number listed in InScreen but client refused to authenticate and indicated she had also rec'd a letter for another screening program. InScreen does not show any other correspondence was sent to the client										
2013-11-26	2013-11-26	External	2013-11-26	Invitation letter opened by unintended recipient	2013-12-23	Unintended recipient opened client's invitation letter and agreed to return the letter. CSR was able to contact the client and a breach notification was sent	N/A	2013-11-28	Senior Privacy Specialist	Privacy breach	None	N/A	N/A	N/A	N/A	2013
2013-11-26	2013-11-26	External	2013-11-26	Birthday letter opened by unintended recipient	2013-11-28	Unintended recipient received and opened the client results letter and said would return it as the. Client does not have a PCP and no number in InScreen and Canada 411 did not produce a match.	N/A	2013-11-28	Senior Privacy Specialist	Privacy breach	None	N/A	N/A	N/A	N/A	2013
2013-11-26	2013-11-26	External	2013-11-26	Invitation letter opened by unintended recipient	2013-11-28	Unintended recipient received and opened the client results letter and said would return it. CSR was	N/A	2013-11-28	Senior Privacy Specialist	Privacy breach	None	N/A	N/A	N/A	N/A	2013

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
						unable to contact client.										
2013-11-26	2013-11-26	External	2013-11-26	Invitation letter opened by unintended recipient	2013-11-27	unintended recipient, client's sister, opened the letter and said client now lives with an aunt and is not able to care for herself. CSR attempted to contact the client at her aunt's home as the number does not accept incoming calls	N/A	2013-11-27	Senior Privacy Specialist	Privacy breach	None	N/A	N/A	N/A	N/A	2013
2013-11-26	2013-11-26	External	2013-11-26	Invitation letter opened by unintended recipient	2013-11-26	Unintended recipient received and opened the client results letter and was very concerned fraud was occurring. An investigation determined the client likely has an incorrect address in her RPDB file. CSR was unable to contact the client. Client does not have a PCP and no number in InScreen and Canada 411 did not produce a match.	N/A	2013-11-26	Senior Privacy Specialist	Privacy breach	None	N/A	N/A	N/A	N/A	2013
2013-11-26	2013-11-26	External	2013-11-26	Invitation letter opened by unintended recipient	2013-12-03	Unintended recipient opened client's invitation letter and said client has not lived there for over 20 years when	N/A	2013-12-03	Senior Privacy Specialist	Privacy breach	none	N/A	N/A	N/A	N/A	2013

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
						she was a foreign student. Said she would return the letter.										
2013-11-26	2013-11-26	External	2013-11-26	Invitation letter opened by unintended recipient	2013-11-26	Unintended recipient opened client's invitation letter and agreed to return the letter but was never received. CSR could not reach the client.	N/A	2013-11-26	Senior Privacy Specialist	Privacy breach	None	N/A	N/A	N/A	N/A	2013
2013-11-26	2013-11-26	External	2013-11-26	Birthday letter opened by unintended recipient	2013-12-17	Unintended recipient opened client's birthday letter. CSR updated the client's contact information by contacting his PCP but the number turned out to be not in service.	N/A	2013-11-26	Senior Privacy Specialist	Privacy breach	None	N/A	N/A	N/A	N/A	2013
2013-11-26	2013-11-26	External	2013-11-25	Other	2013-11-26	Unintended recipient, client's mother in law called to say client lives abroad and did not provide any further details. CSR inactivated the address	N/A	2013-11-26	Senior Privacy Specialist	Privacy breach	N/A - no recommendations logged.	None	N/A	N/A	N/A - no recommendations logged.	2013
2013-11-26	2013-11-26	External	2013-11-26	Other	2013-11-26	Unintended recipient, opened and destroyed client's letter and does not have any contact info. CSR has unable to contact the client and inactivated the address	N/A	2013-11-26	Senior Privacy Specialist	Privacy breach	N/A - no recommendations logged.	None	N/A	N/A	N/A - no recommendations logged.	2013

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
2013-11-26	2013-11-26	External	2013-11-26	invitation letter	2013-11-26	Unintended recipient, client's father rec'd and opened the client's invitation letter. Client's has been living abroad for the last 10 years and will shred the letter. No contact info available for client in InScreen	N/A	2013-11-26	Senior Privacy Specialist	Privacy breach	N/A - no recommendations logged.	None	N/A	N/A	N/A - no recommendations logged.	2013
2013-11-26	2014-11-26	External	2013-11-26	Invitation letter opened by unintended recipient	2014-01-06	Unintended recipient received and opened the client results letter and said would return it as the. Client does not have a PCP and no number in InScreen and Canada 411 did not produce a match.	N/A	2014-01-06	Senior Privacy Specialist	Privacy breach	None	N/A	N/A	N/A	N/A	2014
2013-11-27	2013-11-02	External	2013-11-27	Results letter opened by unintended recipient	2013-12-02	The unintended recipient opened the invitation letter for the client . The source of the address is RPDB dating back to 2012. The unintended recipient provided a phone number for the client. CSR was not able to contact the client	N/A	2013-12-02	Senior Privacy Specialist	Privacy breach	none	N/A	N/A	N/A	N/A	2013
2013-11-27	2013-11-23	External	2013-11-27	Results letter opened by unintended recipient	2013-11-27	Unintended recipient received client birthday letter and agreed to	N/A	2013-11-23	Senior Privacy Specialist	Privacy breach	none	N/A	N/A	N/A	N/A	2013

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
						return the letter. CSR was unable to contact client to update address										
2013-11-27	2013-11-26	External	2013-11-27	invitation letter	2013-11-26	Unintended recipient, client's father rec'd and opened the client's invitation letter. Client's HIN was inactivated in 1995 and moved abroad. Recipient will not return the letter but will remind his daughter to get screened. No contact info available for client in InScreen	N/A	2013-11-26	Senior Privacy Specialist	Privacy breach	N/A - no recommendations logged.	None	N/A	N/A	N/A - no recommendations logged.	2013
2013-11-27	2013-11-27	External	2013-11-27	Invitation letter opened by unintended recipient	2013-11-27	Unintended recipient received and opened the client results letter and returned it. Client is a foreign student to lived there 15 years ago. Source is RPDB dating back to 1990 and HIN was inactivated in 1991.	N/A	2013-11-27	Senior Privacy Specialist	Privacy breach	None	N/A	N/A	N/A	N/A	2013
2013-11-27	2013-11-27	External	2013-11-27	Invitation letter opened by unintended recipient	2013-11-27	Client who has been living outside Ontario for a number of years called. Her mother had opened the letter. Client's HIN was still active and the source	N/A	2013-11-27	Senior Privacy Specialist	Privacy breach	None	N/A	N/A	N/A	N/A	2013

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
						of the address is RPDB dating back to 2005. Client does not require a breach notification										
2013-11-27	2013-11-27	External	2013-11-27	Invitation letter opened by unintended recipient	2013-11-27	Unintended recipient received and opened the client results letter and said letter is already destroyed. The client moved away a few ago. Client does not have a PCP and phone number is disconnected.	N/A	2013-11-27	Senior Privacy Specialist	Privacy breach	None	N/A	N/A	N/A	N/A	2013
2013-11-27	2013-11-27	External	2013-11-27	Invitation letter opened by unintended recipient	2013-12-03	Unintended recipient, opened the letter and returned it. Client moved away several years ago. Client's HIN has been inactive since 2007.	N/A	2013-11-27	Senior Privacy Specialist	Privacy breach	None	N/A	N/A	N/A	N/A	2013
2013-11-27	2013-11-27	External	2013-11-27	Invitation letter	2013-11-27	Unintended recipient, client's mother rec'd and opened the client's invitation letter. Client's has been living abroad for the last 10 years and will shred the letter. No contact info available for client in InScreen	N/A	2013-11-27	Senior Privacy Specialist	Privacy breach	N/A - no recommendations logged.	None	N/A	N/A	N/A - no recommendations logged.	2013
2013-11-28	2013-11-28	External	2013-11-28	Invitation letter opened by	2013-12-04	Unintended recipient,	N/A	2013-11-28	Senior Privacy Specialist	Privacy breach	None	N/A	N/A	N/A	N/A	2013

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				unintended recipient		client's mother, opened the letter. Client moved abroad several years ago. CSR confirmed with the client PCO that she has moved abroad. Client's HIN is still active										
2013-11-28	2013-11-28	External	2013-11-28	Invitation letter opened by unintended recipient	2013-11-28	Unintended recipient, client's relative, opened the letter and shredded it. Client moved away and lives in another province. There is not contact information for the client in InScreen.	N/A	2013-11-28	Senior Privacy Specialist	Privacy breach	None	N/A	N/A	N/A	N/A	2013
2013-11-28	2013-11-28	External	2013-11-28	Invitation letter opened by unintended recipient	2013-11-28	Unintended recipient, opened the letter and agreed to return it but the letter never arrived and CSR followed up and was told it was in the mail. There is not contact information for the client in InScreen and client does not have a PCP.	N/A	2013-11-28	Senior Privacy Specialist	Privacy breach	None	N/A	N/A	N/A	N/A	2013
2013-11-29	2013-11-29	External	2013-11-29	Invitation letter opened by unintended recipient	2013-11-29	Unintended recipient, client's mother received and opened the invitation letter and said would return the letter.	N/A	2013-12-05	Senior Privacy Specialist	Privacy breach	N/A - no recommendations logged.	None	N/A	N/A	N/A - no recommendations logged.	2013

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
						Client no longer lives n Ontario and does not have a phone # or PCP listed inScreen										
2013-11-29	2013-11-29	External	2013-11-29	Invitation letter opened by unintended recipient	2013-11-29	Unintended recipient, client's mother received and opened the invitation letter and said would return the letter. Client no longer lives n Ontario. Client's HIN was inactivated in 2005 and does not have a phone # or PCP listed inScreen	N/A	2013-12-06	Senior Privacy Specialist	Privacy breach	N/A - no recommendations logged.	None	N/A	N/A	N/A - no recommendations logged.	2013
2013-11-29	2013-11-29	External	2013-11-29	Invitation letter opened by unintended recipient	2013-11-29	Unintended recipient, client's mother received and opened the invitation letter and said would return the letter. Client no longer lives n Ontario and does not have a phone # or PCP listed inScreen	N/A	2014-01-09	Senior Privacy Specialist	Privacy breach	N/A - no recommendations logged.	None	N/A	N/A	N/A - no recommendations logged.	2013
2013-12-09	2013-12-09	External	N/A	PHI data was included in a fax sent to CCO's main fax line from a screening program in Saskatchewan. The fax was emailed to the Contact Centre by the receptionist in an effort to obtain	2013-12-09	Contact Centre reported the breach to LPO.	N/A	2013-12-09	Senior Privacy Specialist	Policy breach	None	N/A	N/A	N/A	N/A	2013

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				previous mammo films for the patient PHI included patient name and DOB												
2013-12-09	2013-12-09	External	2013-12-09	Results letter opened by unintended recipient	2013-12-17	Unintended recipient opened the client's letter and agreed to return the letter. Privacy flag is checked in InScreen record indicating the privacy notice was not returned. CSR was able to contact the client and update her address	N/A	2013-12-17	Senior Privacy Specialist	Privacy breach	none	N/A	N/A	N/A	N/A	2013
2013-12-10	2013-12-10	External	2013-12-10	Invitation letter opened by unintended recipient	2013-12-10	Unintended recipient, client's mother received and opened the invitation letter and said would return the letter. Client has been living abroad and does not have a phone # or PCP listed inScreen	N/A	2013-12-17	Senior Privacy Specialist	Privacy breach	N/A - no recommendations logged.	None	N/A	N/A	N/A - no recommendations logged.	2013
2013-12-10	2013-12-10	External	2013-12-10	Invitation letter opened by unintended recipient	2013-12-10	Unintended recipient, client's mother received and opened the invitation letter and said would return the letter. Client no longer lives in Ontario and the phone # is the same as the mothers but does not	N/A	2013-01-09	Senior Privacy Specialist	Privacy breach	N/A - no recommendations logged.	None	N/A	N/A	N/A - no recommendations logged.	2013

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
						PCP listed inScreen										
2013-12-10	2013-12-10	External	2013-12-10	Birthday letter opened by unintended recipient	2013-12-10	Unintended recipient called to report that she had received client's birthday letter and refused to provide her name or contact info; did not want to mail the letter back and said she would return it in person to CCO when she is in Toronto but it is unlikely the letter will ever be returned.	N/A	2013-12-10	Senior Privacy Specialist	Privacy breach	None	N/A	N/A	N/A	N/A	2013
2013-12-11	2013-12-11	External	2013-12-11	invitation letter opened by unintended recipient	2013-12-11	Unintended recipient, client's mother rec'd and opened the letter and destroyed the letter. Client no longer lives in Ontario.	N/A	2013-12-11	Senior Privacy Specialist	Privacy breach	N/A - no recommendations logged.	None	N/A	N/A	N/A - no recommendations logged.	2013
2013-12-12	2014-01-03	External	2013-12-12	invitation letter opened by unintended recipient	2013-12-27	Unintended recipient opened invitation letter and agreed to mail it back but has not as of yet been received. CSR attempted to contact the client at the # in inScreen but unsuccessful	N/A	2014-01-03	Senior Privacy Specialist	Privacy breach	None	None	N/A	N/A	N/A	2014
2013-12-13	2013-12-13	External	2013-12-13	invitation letter opened by unintended recipient	2013-12-13	Unintended recipient received and opened client invitation letter which was sent to an	N/A	2013-12-23	Senior Privacy Specialist	Privacy breach	None	None	N/A	N/A	N/A	2013

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
						inactive address. Investigation revealed that the client's birthday letter had been returned the same day the invitation letter was sent. Client does not have a phone # or PCT in InScreen. CSR was unable to contact the client										
2013-12-13	2013-12-13	external	2013-12-13	invitation letter opened by unintended recipient	2013-12-13	Unintended recipient, client's grandmother rec'd and opened the letter; client had moved abroad a long time ago. She said she would return the letter	N/A	2013-12-13	Senior Privacy Specialist	Privacy breach	None	None	N/A	N/A	N/A	2013
2013-12-16	2013-12-16	External	2013-12-16	invitation letter opened by unintended recipient	2013-12-16	Unintended recipient, client's mother rec'd and opened the letter; client had moved from the province long time ago. She said she would return the letter	N/A	2013-12-16	Senior Privacy Specialist	Privacy breach	N/A - no recommendations logged.	None	N/A	N/A	N/A - no recommendations logged.	2013
2013-12-16	2013-12-16	External	2013-12-16	invitation letter opened by unintended recipient	2013-12-16	Unintended recipient, client's mother rec'd and opened the letter and agreed to return the letter. Client has no contact info or PCP	N/A	2013-12-16	Senior Privacy Specialist	Privacy breach	N/A - no recommendations logged.	None	N/A	N/A	N/A - no recommendations logged.	2013

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
						listed in inScreen										
2013-12-17	2013-12-17	External	2013-12-17	Results letter opened by unintended recipient	2013-12-17	Unintended recipient, clients mother received the results letter and agreed to return the letter but has not been received as yet. Client now lives on a military base outside of the province.	N/A	2013-12-17	Senior Privacy Specialist	Privacy breach	N/A - no recommendations logged.	None	N/A	N/A	N/A - no recommendations logged.	2013
2013-12-17	2013-12-17	External	2013-12-17	invitation letter opened by unintended recipient	2013-12-17	Unintended recipient called from retirement home to report that the client no longer lives there; opened and shredded the letter. Client's phone # has been disconnected and she does not have a PCP	N/A	2013-12-17	Senior Privacy Specialist	Privacy breach	N/A - no recommendations logged.	None	N/A	N/A	N/A - no recommendations logged.	2013
2013-12-18	2013-12-18	External	2013-12-18	invitation letter opened by unintended recipient	2013-12-18	Unintended recipient, client's mother rec'd and opened the letter and destroyed the letter. Client no longer lives in Ontario and lives abroad. Client does not have a PCP and there is no phone # in InScreen to verify that she has moved	N/A	2013-12-18	Senior Privacy Specialist	Privacy breach	N/A - no recommendations logged.	None	N/A	N/A	N/A - no recommendations logged.	2013
2013-12-20	2013-12-20	External	2013-12-20	invitation letter opened by unintended recipient	2013-12-20	Unintended rec'd and opened the letter who has the same last name as the client. CSR	N/A	2013-12-20	Senior Privacy Specialist	Privacy breach	N/A - no recommendations logged.	None	N/A	N/A	N/A - no recommendations logged.	2013

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
						confirmed the unintended DOB did not match the client's. Recipient insisted that it belonged to her and would not return it and was angry that correspondence containing PHI and would discuss the matter with her MP. The client's phone # was not valid and only the PCP had the same number on file										
2013-12-20	2013-12-20	External	2013-12-20	invitation letter opened by unintended recipient	2013-12-20	Unintended recipient received client's invitation letter and agreed to return the letter. CSR was unable to contact the client	N/A	2013-12-20	Senior Privacy Specialist	Privacy breach	N/A - no recommendations logged.	None	N/A	N/A	N/A - no recommendations logged.	2013
2013-12-27	2013-12-27	External	2013-12-27	invitation letter opened by unintended recipient	2013-12-27	Unintended rec'd and opened the client's invitation letter and had rec'd several letters for this client but had never called CCO to report misdirected correspondence and also refused to return the letter but will shred it. CSR called the phone # and was told client no longer lives there. Client	N/A	2014-01-02	Senior Privacy Specialist	Privacy breach	N/A - no recommendations logged.	None	N/A	N/A	N/A - no recommendations logged.	2013

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
						does not a PCP listed inScreen										
2014-01-02	2014-01-02	External	2014-01-02	Invitation letter opened by unintended recipient	2014-01-02	unintended recipient opened client's invitation letter and said the letter was sent to client's previous work address and client has lived outside Canada since 2008. Recipient refused to return the letter but would shred it. There is no contact info and no PCP in InScreen	N/A	2014-01-02	Senior Privacy Specialist	Privacy breach	None	N/A	N/A	N/A	N/A	2014
2014-01-06	2014-01-06	External	N/A	Fax containing OBSP high risk req. form mammo was sent to CCO's primary fax # instead of the screening site. PHI included patient name, DOB, Telephone #, address, description of patient high risk status	2014-01-06	Once informed by Receptionist, Privacy Analyst hand delivered the fax to the Contact Centre	N/A	2014-01-06	Senior Privacy Specialist	Policy breach	None	N/A	N/A	N/A	N/A	2014
2014-01-15	2014-01-15	Internal	N/A	Contact Centre received a voicemail from a CCO program participant and uploaded the voicemail into the client's InScreen. There was one record matching the client's name in InScreen.	2014-01-15	Contact Centre reported the breach to LPO.	N/A	2014-01-24	Senior Privacy Specialist	Privacy breach	None	N/A	N/A	N/A	N/A	2014

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				When returning the phone call, Contact Centre answered the questions but did not authenticate the client. Contact Centre confirmed the name, DOB but not his address. Client wanted to know why his FOBT test was rejected. PHI - FOBT												
2014-01-16	2014-01-16	External	N/A	Fax containing high risk req. from for mammo was sent to CCO's primary fax number instead of the screen site. It was sent by a PCP PHI included Patient name, DOB, Telephone #, address and description of patient high risk status	2014-01-17	Once informed by the receptionist, Privacy analyst had delivered the req. to the Contact Centre for follow-up with PCP office	N/A	2014-01-17	Senior Privacy Specialist	Policy breach	None	N/A	N/A	N/A	N/A	2014
2014-01-24	2014-01-24	External	N/A	Fax containing OBSP high risk req. form mammo was sent to CCO's primary fax # instead of the screening site. PHI included patient name, DOB, Telephone #, address, description of	2014-01-24	Once informed by Receptionist, Privacy Analyst hand delivered the fax to the Contact Centre for follow up with the PCP's office	N/A	2014-01-24	Senior Privacy Specialist	Policy breach	None	N/A	N/A	N/A	N/A	2014

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				patient high risk status												
2014-01-24	2014-01-24	External	N/A	Fax containing high risk req. from for mammo was sent to CCO's primary fax number instead of the screen site. It was sent by a PCP PHI included Patient name, DOB, Telephone #, address and description of patient high risk status	2014-01-27	Once informed by the receptionist, Privacy analyst had delivered the req. to the Contact Centre for follow-up with PCP office	N/A	2014-01-27	Senior Privacy Specialist	Policy breach	None	N/A	N/A	N/A	N/A	2014
2014-01-27	2014-01-27	External	N/A	Fax containing OBSP high risk req. form mammo was sent to CCO's primary fax # by a PCP instead of the screening site. PHI included patient name, DOB, Telephone #, address, description of patient high risk status	2014-01-27	Once informed by Receptionist, Privacy Analyst hand delivered the fax to the Contact Centre for follow up with the PCP's office	N/A	2014-01-27	Senior Privacy Specialist	Policy breach	None	N/A	N/A	N/A	N/A	2014
2014-02-03	2014-02-03	Internal	2014-02-03	Email with PHI was sent to Project Coordinator with Policy and KTE who then forwarded it to 4 CCO employees. Email was sent by a client wanting to withdraw from CCO's screening program. It was sent to	2014-02-03	All employees who received email have been instructed to delete the email from all mail boxes and reminded not to forward emails that may contact PHI. Project Coord was instructed to print and hand deliver a hard copy to Sr.	N/A	2014-02-03	Senior Privacy Specialist	Privacy breach	None	N/A	N/A	N/A	N/A	2014

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				CCO's primary fax number. PHI - patient name, work contact info, age and screen program.		manager, Provincial Operations or Contact Center.										
2014-02-12	2014-04-15	External	N/A	Fax containing OBSP high risk requisition form (sent by a PCP) for a mamo was sent to COO primary fax # instead of the screening site PHI included Patient name, DOB, telephone #, address and description of patient high risk status	2014-02-14	Receptionist reported the fax to LPO. Privacy analyst hand delivered the requisition form to the Contact Centre for follow-up with the primary care provider.	N/A	2014-02-14	Senior Privacy Specialist	Policy breach	none	N/A	N/A	N/A	N/A	2014
2014-02-19	2014-02-19	External	2014-02-19	Fax with PHI sent by a primary care provider was sent to CCO's primary fax number. PHI included patient name, DOB, HIN, description of medical history, list of meds, test results, exam notes, assessment notes, chronic disease history. Fax with Info should have been sent to Contact Center using the secure Fax number	2014-02-19	Receptionist notified LPO of the breach and deleted the fax from inbox and deleted items folders and provided a hard copy to the Privacy Specialist for delivery to the Contact Centre	N/A	2014-02-19	Senior Privacy Specialist	Policy breach	None	N/A	N/A	N/A	N/A	2014
2014-02-21	2014-02-21	External	2014-02-21	Fax with PHI sent by a primary care provider	2013-02-21	Receptionist notified LPO of the breach and deleted	N/A	2014-02-12	Senior Privacy Specialist	Policy breach	None	N/A	N/A	N/A	N/A	2014

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				accidentally to CCO's primary fax number but should have been sent to Hospital. PHI included patient name, DOB, phone #, address and health card #.		the fax from inbox and deleted items folders and provided a hard copy to the Privacy Specialist for delivery to the Contact Centre										
2014-03-05	2014-04-15	External	N/A	Fax containing OBSP high risk requisition form (sent by a PCP) for a mamo was sent to COO primary fax # instead of the screening site PHI included Patient name, DOB, telephone #, address and description of patient high risk status	2014-03-05	Receptionist reported the fax to LPO. Privacy analyst hand delivered the requisition form to the Contact Centre for follow-up with the primary care provider.	N/A	2014-03-05	Senior Privacy Specialist	Policy breach	none	N/A	N/A	N/A	N/A	N/A	2014
2014-03-18	2014-04-16	External	N/A	Fax containing OBSP high risk requisition form (sent by a PCP) for a mamo was sent to COO primary fax # instead of the screening site PHI included Patient name, DOB, telephone #, address and description of patient high risk status	2014-03-18	Receptionist reported the fax to LPO. Privacy analyst hand delivered the requisition form to the Contact Centre for follow-up with the primary care provider.	N/A	2014-03-18	Senior Privacy Specialist	Policy breach	None	N/A	N/A	N/A	N/A	N/A	2014
2014-05-01	2014-05-01	External	2014-05-01	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-01	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-05-01	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-05-01	Address inactivated. CC was unable to reach the client.	2014
2014-05-01	2014-05-01	External	2014-05-01	Client's Invitation/Remi	2014-05-01	CC inactivated the address +	N/A	2014-05-01	Contact Center &	Privacy breach	Address to be inactivated.	NO	Contact Center &	2014-05-01	Address inactivated.	2014

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				nder Letter (Screening Status/Eligibility)		Unintended Recipient to destroy letter			Privacy Specialist		CC to attempt to contact intended client.		Privacy Specialist		CC was unable to reach the client.	
2014-05-01	2014-05-01	External	2014-05-01	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-01	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-05-01	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-01	Address inactivated. CC was unable to reach the client.	2014
2014-05-01	2014-05-01	External	2014-05-01	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-01	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-01	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-01	Address inactivated. CC was unable to reach the client.	2014
2014-05-01	2014-05-01	External	2014-05-01	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-01	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-05-01	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-05-01	Address inactivated. CC was unable to reach the client.	2014
2014-05-01	2014-05-01	External	2014-05-01	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-01	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-05-01	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-01	Address inactivated. CC was unable to reach the client.	2014
2014-05-01	2014-05-01	Internal	2014-05-01	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-01	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-01	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-01	Address inactivated. CC was unable to reach the client.	2014
2014-05-01	2014-05-01	External	2014-05-01	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-01	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-01	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-01	Address inactivated. CC was unable to reach the client.	2014
2014-05-02	2014-05-02	External	2014-05-02	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-02	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-02	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-02	Address inactivated. CC was unable to reach the client.	2014
2014-05-02	2014-05-02	External	2014-05-02	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-02	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-02	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-02	Address inactivated. CC was unable to reach the client.	2014
2014-05-02	2014-05-02	External	2014-05-02	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-02	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-02	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-02	Address inactivated. CC was unable to reach the client.	2014

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
2014-05-02	2014-05-02	External	2014-05-02	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-02	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-02	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-02	Address inactivated. CC was unable to reach the client.	2014
2014-05-05	2014-05-05	External	2014-05-05	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-05	None - CCO received a fax containing PHI from a health care provider. No containment possible.	N/A	2014-05-05	Contact Center & Privacy Specialist	Privacy breach	The PHI should not have been faxed to CCO . CC to advise sender.	NO	Contact Center & Privacy Specialist	2014-05-05	CC contacted sender (office of the health care provider to the client) to let them know that PHI should not be faxed to CCO.	2014
2014-05-05	2014-05-05	External	2014-05-05	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-05	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-05	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-05	Address inactivated. CC was unable to reach the client.	2014
2014-05-05	2014-05-05	External	2014-05-05	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-05	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-05	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-05	Address inactivated. CC was unable to reach the client.	2014
2014-05-05	2014-05-05	External	2014-05-05	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-05	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-05-05	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-05-05	Address inactivated. CC was unable to reach the client.	2014
2014-05-05	2014-05-05	External	2014-05-05	Client's Result Letter (Test Result)	2014-05-05	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-05	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-05	Address inactivated. CC was unable to reach the client.	2014
2014-05-05	2014-05-05	External	2014-05-05	Client's Result Letter (Test Result)	2014-05-05	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-05	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	2014-05-05	CC was unable to reach the PCP and address inactivated.	2014
2014-05-05	2014-05-05	External	2014-05-05	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-05	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-05-05	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	2014-05-05	Address inactivated. CC was unable to reach the client.	2014
2014-05-05	2014-05-05	External	2014-05-05	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-05	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-05	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-05	Address inactivated. CC was unable to reach the client.	2014

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
2014-05-05	2014-05-05	External	2014-05-05	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-05	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-05-05	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-05	Address inactivated. CC was unable to reach the client.	2014
2014-05-05	2014-05-05	External	2014-05-05	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-05	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-05-05	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-05-05	Address inactivated. CC was unable to reach the client.	2014
2014-05-06	2014-05-06	External	2014-05-06	Client's Result Letter (Test Result)	2014-05-06	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-06	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center	2014-05-06	CC called the client and updated the address.	2014
2014-05-06	2014-05-06	External	2014-05-06	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-06	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-06	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-06	Address inactivated. CC was unable to reach the client.	2014
2014-05-06	2014-05-06	External	2014-05-06	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-06	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-05-06	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-05-06	Address inactivated. CC was unable to reach the client.	2014
2014-05-07	2014-05-07	External	2014-05-07	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-07	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-05-07	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-07	Address inactivated. CC was unable to reach the client.	2014
2014-05-09	2014-05-09	External	2014-05-09	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-09	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-09	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-09	Address inactivated. CC was unable to reach the client.	2014
2014-05-09	2014-05-09	External	2014-05-09	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-09	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-09	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-09	Address inactivated. CC was unable to reach the client.	2014
2014-05-12	2014-05-12	External	2014-05-12	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-12	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-12	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-12	Address inactivated. CC was unable to reach the client.	2014
2014-05-12	2014-05-12	External	2014-05-12	Client's Invitation/Reminder Letter (Screening	2014-05-12	CC inactivated address + Unintended Recipient	N/A	2014-05-12	Contact Center & Privacy Specialist	Privacy breach	Contact Center could not reach client, address	NO	Contact Center & Privacy Specialist	2014-05-12	Address updated. CC was able to contact the	2014

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				Status/Eligibility)		asked to return letter					to be inactivated.				client via number provided by their PCP.	
2014-05-12	2014-05-12	External	2014-05-12	Client's Result Letter (Test Result)	2014-05-12	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-05-12	Contact Center	Privacy breach	Contact Center could not reach client, address to be inactivated.	NO	Contact Center	2014-05-12	Address inactivated. CC was unable to obtain client's phone number from PCP.	2014
2014-05-12	2014-05-12	External	2014-05-12	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-12	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-12	Contact Center & Privacy Specialist	Privacy breach	Contact Center could not reach client, address to be inactivated.	NO	Contact Center & Privacy Specialist	2014-05-12	Address inactivated. CC was unable to obtain client's phone number from PCP.	2014
2014-05-12	2014-05-12	External	2014-05-12	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-12	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-05-12	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-12	Address inactivated. CC was unable to reach the client.	2014
2014-05-12	2014-05-12	External	2014-05-12	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-12	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-12	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-12	Address inactivated. CC was unable to reach the client.	2014
2014-05-13	2014-05-13	External	2014-05-13	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-13	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-13	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-13	Address inactivated. CC was unable to reach the client.	2014
2014-05-13	2014-05-13	External	2014-05-13	Client's Result Letter (Test Result)	2014-05-13	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-13	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-13	Address inactivated. CC was unable to reach the client.	2014
2014-05-13	2014-05-13	External	2014-05-13	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-13	CC inactivated incorrect address	N/A	2014-05-13	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-05-13	Address inactivated. CC was unable to reach the client.	2014
2014-05-13	2014-05-13	External	2014-05-13	Client's Result Letter (Test Result)	2014-05-13	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-13	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-13	Address inactivated. CC was unable to reach the client.	2014
2014-05-13	2014-05-13	External	2014-05-13	Client's Invitation/Reminder Letter (Screening	2014-05-13	CC inactivated address + Unintended Recipient	N/A	2014-05-13	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact	NO	Contact Center & Privacy Specialist	2014-05-13	Address inactivated. CC was unable to	2014

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				Status/Eligibility)		asked to return letter					intended client.				reach the client.	
2014-05-13	2014-05-13	External	2014-05-13	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-13	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-13	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-13	Address inactivated. CC was unable to reach the client.	2014
2014-05-13	2014-05-13	External	2014-05-13	Client's Result Letter (Test Result)	2014-05-13	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-13	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-13	Address inactivated. CC was unable to reach the client.	2014
2014-05-14	2014-05-14	External	2014-05-14	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-14	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-14	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-14	Address inactivated. CC was unable to reach the client.	2014
2014-05-14	2014-05-14	External	2014-05-14	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-14	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-14	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-14	Address inactivated. CC was unable to reach the client.	2014
2014-05-14	2014-05-14	External	2014-05-14	Client's Result Letter (Test Result)	2014-05-14	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-05-14	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-14	Address inactivated. CC was unable to reach the client.	2014
2014-05-15	2014-05-15	External	2014-05-15	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-15	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-05-15	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-05-15	Address inactivated. CC was unable to reach the client.	2014
2014-05-15	2014-05-15	External	2014-05-15	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-15	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-05-15	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-15	Address inactivated. CC was unable to reach the client.	2014
2014-05-16	2014-05-16	External	2014-05-16	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-16	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-05-16	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-16	Address inactivated. CC was unable to reach the client.	2014
2014-05-16	2014-05-16	External	2014-05-16	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-16	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-05-16	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-05-16	Address inactivated. CC was unable to reach the client.	2014
2014-05-16	2014-05-16	External	2014-05-16	Client's Invitation/Remi	2014-05-16	CC inactivated address +	N/A	2014-05-16	Privacy Specialist	Privacy breach	Address to be inactivated.	NO	Privacy Specialist	2014-05-16	Address inactivated.	2014

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				nder Letter (Screening Status/Eligibility)		Unintended Recipient asked to return letter					CC to attempt to contact intended client.				CC was unable to reach the client.	
2014-05-16	2014-05-16	External	2014-05-16	Client's Result Letter (Test Result)	2014-05-16	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-16	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-16	Address inactivated. CC was unable to reach the client.	2014
2014-05-20	2014-05-20	External	2014-05-20	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-20	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-05-20	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-05-20	Address inactivated. CC was unable to reach the client.	2014
2014-05-20	2014-05-20	External	2014-05-20	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-20	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-20	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-20	Address inactivated. CC was unable to reach the client.	2014
2014-05-20	2014-05-20	External	2014-05-20	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-20	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-05-20	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-20	Address inactivated. CC was unable to reach the client.	2014
2014-05-20	2014-05-20	External	2014-05-20	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-20	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-05-20	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-05-20	Address inactivated. CC was unable to reach the client.	2014
2014-05-20	2014-05-20	External	2014-05-20	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-20	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-05-20	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-20	Address inactivated. CC was unable to reach the client.	2014
2014-05-20	2014-05-20	External	2014-05-20	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-20	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-20	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-20	Address inactivated. CC was unable to reach the client.	2014
2014-05-20	2014-05-20	External	2014-05-20	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-20	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-20	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-05-20	Address inactivated. CC was unable to reach the client.	2014
2014-05-20	2014-05-20	External	2014-05-20	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-20	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-20	Contact Center & Privacy Specialist	Privacy breach	Contact Center could not reach client, address to be inactivated.	NO	Contact Center & Privacy Specialist	2014-05-20	Address inactivated. CC was unable to obtain client's	2014

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
															phone number from PCP.	
2014-05-20	2014-05-20	External	2014-05-20	Client's Result Letter (Test Result)	2014-05-20	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-20	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-20	Address inactivated. CC was unable to reach the client.	2014
2014-05-20	2014-05-20	External	2014-05-20	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-20	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-20	Privacy Specialist	Privacy breach	Contact Center to call client/PCP and update address.	YES	Privacy Specialist	2014-05-20	Address inactivated. CC was unable to reach the client.	2014
2014-05-20	2014-05-20	External	2014-05-20	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-20	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-20	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-20	Address inactivated. CC was unable to reach the client.	2014
2014-05-21	2014-05-21	External	2014-05-21	Client's Result Letter (Test Result)	2014-05-21	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-05-21	Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Privacy Specialist	2014-05-21	Address inactivated. CC was unable to reach the client.	2014
2014-05-21	2014-05-21	External	2014-05-21	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-21	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-21	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-21	Address inactivated. CC was unable to reach the client.	2014
2014-05-21	2014-05-21	External	2014-05-21	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-21	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-21	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-21	Address inactivated. CC was unable to reach the client.	2014
2014-05-21	2014-05-21	External	2014-05-21	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-21	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-21	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-21	Address inactivated. CC was unable to reach the client.	2014
2014-05-21	2014-05-21	External	2014-05-21	Client's Result Letter (Test Result)	2014-05-21	Address inactivated - Letter will not be returned	N/A	2014-05-21	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-21	Address inactivated. CC was unable to reach the client.	2014
2014-05-21	2014-05-21	External	2014-05-21	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-21	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-21	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-21	Address inactivated. CC was unable to reach the client.	2014
2014-05-21	2014-05-21	External	2014-05-21	Client's Invitation/Remi	2014-05-21	CC inactivated the address +	N/A	2014-05-21	Contact Center &	Privacy breach	Address to be inactivated.	NO	Contact Center &	2014-05-21	Address inactivated.	2014

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				nder Letter (Screening Status/Eligibility)		Unintended Recipient to destroy letter			Privacy Specialist		CC to attempt to contact intended client.		Privacy Specialist		CC was unable to reach the client.	
2014-05-21	2014-05-21	External	2014-05-21	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-21	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-21	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-05-21	Address inactivated. CC was unable to reach the client.	2014
2014-05-21	2014-05-21	External	2014-05-21	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-21	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-21	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-21	Address inactivated. CC was unable to reach the client.	2014
2014-05-22	2014-05-22	External	2014-05-22	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-22	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-22	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-22	Address inactivated. CC was unable to reach the client.	2014
2014-05-22	2014-05-22	External	2014-05-22	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-22	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-22	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-22	Address inactivated. CC was unable to reach the client.	2014
2014-05-22	2014-05-22	External	2014-05-22	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-22	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-22	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-22	Address inactivated. CC was unable to reach the client.	2014
2014-05-22	2014-05-22	External	2014-05-22	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-22	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-05-22	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-22	Address inactivated. CC was unable to reach the client.	2014
2014-05-22	2014-05-22	External	2014-05-22	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-22	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-05-22	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-05-22	Address inactivated. CC was unable to reach the client.	2014
2014-05-22	2014-05-22	External	2014-05-22	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-22	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-22	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-22	Address inactivated. CC was unable to reach the client.	2014
2014-05-22	2014-05-22	External	2014-05-22	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-22	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-22	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-05-22	Address inactivated. CC was unable to reach the client.	2014

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
2014-05-23	2014-05-23	External	2014-05-23	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-23	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-23	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-23	Address inactivated. CC was unable to reach the client.	2014
2014-05-23	2014-05-23	External	2014-05-23	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-23	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-23	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-05-23	Address inactivated. CC was unable to reach the client.	2014
2014-05-23	2014-05-23	External	2014-05-23	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-23	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-23	Privacy Specialist	Privacy breach	Contact Center could not reach client, address to be inactivated.	NO	Privacy Specialist	2014-05-23	Address inactivated. CC was unable to obtain client's phone number from PCP.	2014
2014-05-23	2014-05-23	Internal	2014-05-23	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-23	None - misdirected mail, mail was sent to old address - client received the letter from the unintended recipient.	N/A	2014-05-23	Privacy Specialist	Privacy breach	Client's address should be updated, or client should be withdrawn from screening programs as per their request.	YES	Privacy Specialist	2014-05-23	CC transferred the client to Service Ontario so that they can update their address. Client has since been withdrawn from all 3 screening programs.	2014
2014-05-23	2014-05-23	External	2014-05-23	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-23	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-23	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-05-23	Address inactivated. CC was unable to reach the client.	2014
2014-05-26	2014-05-26	External	2014-05-26	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-26	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-26	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-26	Address inactivated. CC was unable to reach the client.	2014
2014-05-26	2014-05-26	External	2014-05-26	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-26	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-26	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-26	Address inactivated. CC was unable to reach the client.	2014
2014-05-26	2014-05-26	External	2014-05-26	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-26	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-26	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-26	Address inactivated. CC was unable to reach the client.	2014
2014-05-26	2014-05-26	External	2014-05-26	Client's Invitation/Remi	2014-05-26	CC inactivated the address +	N/A	2014-05-26	Contact Center	Privacy breach	Address to be inactivated.	NO	Contact Center	2014-05-26	Address inactivated.	2014

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				nder Letter (Screening Status/Eligibility)		Unintended Recipient to destroy letter					CC to attempt to contact intended client.				CC was unable to reach the client.	
2014-05-26	2014-05-26	External	2014-05-26	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-26	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-05-26	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-05-26	Address inactivated. CC was unable to reach the client.	2014
2014-05-26	2014-05-26	External	2014-05-26	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-26	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-26	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-26	Address inactivated. CC was unable to reach the client.	2014
2014-05-26	2014-05-26	External	2014-05-26	Client's Result Letter (Test Result)	2014-05-26	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-26	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	2014-05-26	Address inactivated. CC was unable to reach the client.	2014
2014-05-26	2014-05-26	External	2014-05-26	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-26	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-26	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-26	Address inactivated. CC was unable to reach the client.	2014
2014-05-26	2014-05-26	External	2014-05-26	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-26	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-26	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-26	Address inactivated. CC was unable to reach the client.	2014
2014-05-27	2014-05-27	External	2014-05-27	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-27	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-05-27	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-27	Address inactivated. CC was unable to reach the client.	2014
2014-05-27	2014-05-27	External	2014-05-27	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-27	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-27	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-27	Address inactivated. CC was unable to reach the client.	2014
2014-05-27	2014-05-27	External	2014-05-27	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-27	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-27	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-05-27	Address inactivated. CC was unable to reach the client.	2014
2014-05-27	2014-05-27	External	2014-05-27	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-27	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-05-27	Contact Center & Privacy Specialist	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center & Privacy Specialist	2014-05-27	Address inactivated. CC was unable to reach the client.	2014

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
2014-05-27	2014-05-27	External	2014-05-27	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-27	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-27	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-27	Address inactivated. CC was unable to reach the client.	2014
2014-05-27	2014-05-27	Internal	2014-05-27	Client's Result Letter (Test Result)	2014-05-27	N/A - received returned result mail - unclear why the result was considered breached. Per InScreen, CCO was unable to reach the intended recipient of the result or their primary care provider.	N/A	2014-05-27	Contact Center	Privacy breach	Client's address should be updated.	N/A	Contact Center	2014-05-28	CCO was unable to reach the intended recipient of the result or their primary care provider	2014
2014-05-27	2014-05-27	External	2014-05-27	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-27	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-27	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-27	Address inactivated. CC was unable to reach the client.	2014
2014-05-28	2014-05-28	External	2014-05-28	Client's Result Letter (Test Result)	2014-05-28	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-28	Contact Center & Privacy Specialist	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center & Privacy Specialist	2014-05-28	CC called the client and updated the address.	2014
2014-05-28	2014-05-28	External	2014-05-28	Client's Result Letter (Test Result)	2014-05-28	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-05-28	Contact Center & Privacy Specialist	Privacy breach	Contact Center could not reach client, address to be inactivated.	NO	Contact Center & Privacy Specialist	2014-05-28	Address inactivated. CC was unable to obtain client's phone number from PCP.	2014
2014-05-28	2014-05-28	External	2014-05-28	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-28	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-05-28	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-28	Address inactivated. CC was unable to reach the client.	2014
2014-05-28	2014-05-28	External	2014-05-28	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-28	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-28	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-28	Address inactivated. CC was unable to reach the client.	2014
2014-05-28	2014-05-28	External	2014-05-28	Client's Invitation/Reminder Letter (Screening	2014-05-28	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-05-28	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact	NO	Contact Center	2014-05-28	Address inactivated. CC was unable to	2014

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				Status/Eligibility)							intended client.				reach the client.	
2014-05-28	2014-05-28	External	2014-05-28	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-28	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-28	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-28	Address inactivated. CC was unable to reach the client.	2014
2014-05-28	2014-05-28	External	2014-05-28	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-28	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-28	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-28	Address inactivated. CC was unable to reach the client.	2014
2014-05-28	2014-05-28	External	2014-05-28	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-28	CC inactivated incorrect address	N/A	2014-05-28	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-05-28	Address inactivated. CC was unable to reach the client.	2014
2014-05-28	2014-05-28	External	2014-05-28	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-28	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-28	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-28	Address inactivated. CC was unable to reach the client.	2014
2014-05-28	2014-05-28	Internal	2014-05-28	N/A	2014-05-28	N/A - received email from unintended recipient notifying of the breach; client moved. CC advised unintended recipient to return the letter to CCO. Unclear whether the letter was returned.	N/A	2014-05-28	Contact Center	Privacy breach	CC could not find the client's profile in InScreen, no follow-up possible.	NO	Contact Center	2014-05-28	CC could not find the client's profile in InScreen, no follow-up possible.	2014
2014-05-28	2014-05-28	External	2014-05-28	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-28	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-28	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-28	Address inactivated. CC was unable to reach the client.	2014
2014-05-28	2014-05-28	External	2014-05-28	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-28	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-28	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-28	Address inactivated. CC was unable to reach the client.	2014
2014-05-28	2014-05-28	External	2014-05-28	Client's Invitation/Reminder Letter (Screening	2014-05-28	CC inactivated the address + Unintended	N/A	2014-05-28	Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact	NO	Privacy Specialist	2014-05-28	Address inactivated. CC was unable to	2014

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				Status/Eligibility)		Recipient to destroy letter					intended client.				reach the client.	
2014-05-28	2014-05-28	External	2014-05-28	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-28	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-28	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-05-28	Address inactivated. CC was unable to reach the client.	2014
2014-05-29	2014-05-29	External	2014-05-29	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-29	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-29	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-29	Address inactivated. CC was unable to reach the client.	2014
2014-05-29	2014-05-29	External	2014-05-29	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-29	CC inactivated incorrect address	N/A	2014-05-29	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-29	Address inactivated. CC was unable to reach the client.	2014
2014-05-29	2014-05-29	External	2014-05-29	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-29	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-29	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-29	Address inactivated. CC was unable to reach the client.	2014
2014-05-29	2014-05-29	External	2014-05-29	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-29	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-05-29	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-29	Address inactivated. CC was unable to reach the client.	2014
2014-05-29	2014-05-29	External	2014-05-29	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-29	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-05-29	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-29	Address inactivated. CC was unable to reach the client.	2014
2014-05-29	2014-05-29	External	2014-05-29	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-29	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-05-29	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-29	Address inactivated. CC was unable to reach the client.	2014
2014-05-29	2014-05-29	External	2014-05-29	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-29	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-29	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-29	Address inactivated. CC was unable to reach the client.	2014
2014-05-29	2014-05-29	External	2014-05-29	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-29	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-05-29	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-05-29	Address inactivated. CC was unable to reach the client.	2014
2014-05-29	2014-05-29	External	2014-05-29	Client's Invitation/Remi	2014-05-29	CC inactivated address +	N/A	2014-05-29	Contact Center &	Privacy breach	Address to be inactivated.	NO	Contact Center &	2014-05-29	Address inactivated.	2014

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				nder Letter (Screening Status/Eligibility)		Unintended Recipient asked to return letter			Privacy Specialist		CC to attempt to contact intended client.		Privacy Specialist		CC was unable to reach the client.	
2014-05-29	2014-05-29	External	2014-05-29	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-29	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-29	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-29	Address inactivated. CC was unable to reach the client.	2014
2014-05-30	2014-05-30	External	2014-05-30	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-30	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-05-30	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-05-30	Address inactivated. CC was unable to reach the client.	2014
2014-05-30	2014-05-30	External	2014-05-30	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-05-30	CC inactivated incorrect address	N/A	2014-05-30	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-05-30	Address inactivated. CC was unable to reach the client.	2014
2014-06-02	2014-06-02	External	2014-06-02	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-02	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-02	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-02	Address inactivated. CC was unable to reach the client.	2014
2014-06-02	2014-06-02	External	2014-06-02	Client's Result Letter (Test Result)	2014-06-02	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-02	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-02	Address inactivated. CC was unable to reach the client.	2014
2014-06-02	2014-06-02	External	2014-06-02	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-02	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-02	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-02	Address inactivated. CC was unable to reach the client.	2014
2014-06-02	2014-06-02	External	2014-06-02	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-02	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-06-02	Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Privacy Specialist	2014-06-02	Address inactivated. CC was unable to reach the client.	2014
2014-06-02	2014-06-02	External	2014-06-02	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-02	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-02	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-02	Address inactivated. CC was unable to reach the client.	2014
2014-06-03	2014-06-03	External	2014-06-03	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-03	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-06-03	Contact Center	Privacy breach	Contact Center could not reach client, address to be inactivated.	NO	Contact Center	2014-06-03	Address inactivated. CC was unable to obtain client's	2014

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
															phone number from PCP.	
2014-06-03	2014-06-03	External	2014-06-03	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-03	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-03	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-03	Address inactivated. CC was unable to reach the client.	2014
2014-06-03	2014-06-03	External	2014-06-03	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-03	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-06-03	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-03	Address inactivated. CC was unable to reach the client.	2014
2014-06-03	2014-06-03	External	2014-06-03	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-03	CC inactivated incorrect address	N/A	2014-06-03	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-06-03	Address inactivated. CC was unable to reach the client.	2014
2014-06-03	2014-06-03	External	2014-06-03	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-03	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-03	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-03	Address inactivated. CC was unable to reach the client.	2014
2014-06-03	2014-06-03	External	2014-06-03	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-03	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-03	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-03	Address inactivated. CC was unable to reach the client.	2014
2014-06-03	2014-06-03	External	2014-06-03	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-03	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-06-03	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-06-03	Address inactivated. CC was unable to reach the client.	2014
2014-06-04	2014-06-04	External	2014-06-04	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-04	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-06-04	Privacy Specialist	Privacy breach	Contact Center could not reach client, address to be inactivated.	NO	Privacy Specialist	2014-06-04	Address inactivated. CC was unable to obtain client's phone number from PCP.	2014
2014-06-04	2014-06-04	External	2014-06-04	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-04	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-04	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-04	Address inactivated. CC was unable to reach the client.	2014
2014-06-04	2014-06-04	External	2014-06-04	Client's Invitation/Reminder Letter (Screening	2014-06-04	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-06-04	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact	NO	Contact Center	2014-06-04	Address inactivated. CC was unable to	2014

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				Status/Eligibility)							intended client.				reach the client.	
2014-06-04	2014-06-04	External	2014-06-04	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-04	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-04	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-06-04	Address inactivated. CC was unable to reach the client.	2014
2014-06-04	2014-06-04	External	2014-06-04	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-04	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-04	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-04	Address inactivated. CC was unable to reach the client.	2014
2014-06-05	2014-06-05	External	2014-06-05	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-05	CC inactivated incorrect address	N/A	2014-06-05	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-06-05	Address inactivated. CC was unable to reach the client.	2014
2014-06-05	2014-06-05	External	2014-06-05	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-05	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-05	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-05	Address inactivated. CC was unable to reach the client.	2014
2014-06-05	2014-06-05	External	2014-06-05	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-05	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-05	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-05	Address inactivated. CC was unable to reach the client.	2014
2014-06-05	2014-06-05	External	2014-06-05	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-05	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-06-05	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-06-05	Address inactivated. CC was unable to reach the client.	2014
2014-06-05	2014-06-05	External	2014-06-05	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-05	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-05	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-06-05	Address inactivated. CC was unable to reach the client.	2014
2014-06-06	2014-06-06	External	2014-06-06	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-06	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-06	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-06	Address inactivated. CC was unable to reach the client.	2014
2014-06-06	2014-06-06	External	2014-06-06	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-06	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-06-06	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-06	Address inactivated. CC was unable to reach the client.	2014
2014-06-06	2014-06-06	External	2014-06-06	Client's Invitation/Remi	2014-06-06	CC inactivated address +	N/A	2014-06-06	Contact Center &	Privacy breach	Contact Center to call	NO	Contact Center &	2014-06-06	Address inactivated.	2014

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				nder Letter (Screening Status/Eligibility)		Unintended Recipient asked to return letter			Privacy Specialist		client/PCP and update address.		Privacy Specialist		CC was unable to reach the client.	
2014-06-06	2014-06-06	External	2014-06-06	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-06	CC inactivated incorrect address	N/A	2014-06-06	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-06-06	Address inactivated. CC was unable to reach the client.	2014
2014-06-06	2014-06-06	External	2014-06-06	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-06	CC inactivated incorrect address	N/A	2014-06-06	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-06-06	Address inactivated. CC was unable to reach the client.	2014
2014-06-06	2014-06-06	External	2014-06-06	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-06	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-06	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-06	Address inactivated. CC was unable to reach the client.	2014
2014-06-06	2014-06-06	External	2014-06-06	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-06	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-06	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-06-06	Address inactivated. CC was unable to reach the client.	2014
2014-06-06	2014-06-06	External	2014-06-06	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-06	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-06	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-06	Address inactivated. CC was unable to reach the client.	2014
2014-06-06	2014-06-06	External	2014-06-06	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-06	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-06	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-06	Address inactivated. CC was unable to reach the client.	2014
2014-06-06	2014-06-06	External	2014-06-06	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-06	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-06	Contact Center	Privacy breach	Contact Center could not reach client, address to be inactivated.	NO	Contact Center	2014-06-06	Address inactivated. CC was unable to obtain client's phone number from PCP.	2014
2014-06-06	2014-06-06	External	2014-06-06	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-06	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-06	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-06-06	Address inactivated. CC was unable to reach the client.	2014
2014-06-06	2014-06-06	External	2014-06-06	Client's Invitation/Reminder Letter (Screening	2014-06-06	CC inactivated incorrect address	N/A	2014-06-06	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact	NO	Contact Center	2014-06-06	Address inactivated. CC was unable to	2014

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				Status/Eligibility)							intended client.				reach the client.	
2014-06-06	2014-06-06	External	2014-06-06	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-06	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-06	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-06	Address inactivated. CC was unable to reach the client.	2014
2014-06-06	2014-06-06	External	2014-06-06	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-06	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-06	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-06	Address inactivated. CC was unable to reach the client.	2014
2014-06-06	2014-06-06	External	2014-06-06	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-06	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-06-06	Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Privacy Specialist	2014-06-06	Address inactivated. CC was unable to reach the client.	2014
2014-06-09	2014-06-09	External	2014-06-09	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-09	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-09	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-09	Address inactivated. CC was unable to reach the client.	2014
2014-06-09	2014-06-09	External	2014-06-09	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-09	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-09	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-09	Address inactivated. CC was unable to reach the client.	2014
2014-06-09	2014-06-09	External	2014-06-09	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-09	CC inactivated incorrect address	N/A	2014-06-09	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-09	Address inactivated. CC was unable to reach the client.	2014
2014-06-09	2014-06-09	External	2014-06-09	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-09	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-09	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-06-09	Address inactivated. CC was unable to reach the client.	2014
2014-06-09	2014-06-09	External	2014-06-09	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-09	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-09	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-09	Address inactivated. CC was unable to reach the client.	2014
2014-06-09	2014-06-09	External	2014-06-09	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-09	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-09	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-09	Address inactivated. CC was unable to reach the client.	2014
2014-06-09	2014-06-09	External	2014-06-09	Client's Invitation/Remi	2014-06-09	CC inactivated address +	N/A	2014-06-09	Contact Center	Privacy breach	Address to be inactivated.	NO	Contact Center	2014-06-09	Address inactivated.	2014

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				nder Letter (Screening Status/Eligibility)		Unintended Recipient asked to return letter					CC to attempt to contact intended client.				CC was unable to reach the client.	
2014-06-10	2014-06-10	External	2014-06-10	Client's Result Letter (Test Result)	2014-06-10	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-10	Contact Center & Privacy Specialist	Privacy breach	Contact Center could not reach client, address to be inactivated.	NO	Contact Center & Privacy Specialist	2014-06-10	Address inactivated. CC was unable to obtain client's phone number from PCP.	2014
2014-06-10	2014-06-10	External	2014-06-10	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-10	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-10	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-10	Address inactivated. CC was unable to reach the client.	2014
2014-06-10	2014-06-10	External	2014-06-10	Privacy Notice	2014-06-10	Address inactivated - Letter will not be returned	N/A	2014-06-10	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-06-10	Address inactivated. CC was unable to reach the client.	2014
2014-06-10	2014-06-10	External	2014-06-10	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-10	CC inactivated incorrect address	N/A	2014-06-10	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-06-10	Address inactivated. CC was unable to reach the client.	2014
2014-06-10	2014-06-10	External	2014-06-10	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-10	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-06-10	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-06-10	Address inactivated. CC was unable to reach the client.	2014
2014-06-10	2014-06-10	External	2014-06-10	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-10	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-06-10	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-06-10	Address inactivated. CC was unable to reach the client.	2014
2014-06-10	2014-06-10	External	2014-06-10	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-10	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-10	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-06-10	Address inactivated. CC was unable to reach the client.	2014
2014-06-10	2014-06-10	External	2014-06-10	Client's Result Letter (Test Result)	2014-06-10	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-10	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	YES	Contact Center & Privacy Specialist	2014-06-10	Address inactivated. CC was unable to reach the client.	2014
2014-06-11	2014-06-11	External	2014-06-11	Client's Invitation/Reminder Letter (Screening	2014-06-11	CC inactivated address + Unintended Recipient	N/A	2014-06-11	Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact	NO	Privacy Specialist	2014-06-11	Address inactivated. CC was unable to	2014

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				Status/Eligibility)		asked to return letter					intended client.				reach the client.	
2014-06-11	2014-06-11	External	2014-06-11	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-11	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-11	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-11	Address inactivated. CC was unable to reach the client.	2014
2014-06-11	2014-06-11	Internal	2014-06-11	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-11	None - received voicemail from unintended recipient notifying of the breach; client had moved. Could not contact the unintended recipient as they did not leave a callback number. Could not authenticate the intended recipient in InScreen.	N/A	2014-06-11	Contact Center	Privacy breach	CC could not find the client's profile in InScreen, no follow-up possible.	NO	Contact Center & Privacy Specialist	2014-06-11	CC could not find the client's profile in InScreen, no follow-up possible.	2014
2014-06-11	2014-06-11	External	2014-06-11	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-11	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-11	Contact Center & Privacy Specialist	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center & Privacy Specialist	2014-06-11	CC called the client and updated the address.	2014
2014-06-11	2014-06-11	External	2014-06-11	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-11	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-11	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-11	Address inactivated. CC was unable to reach the client.	2014
2014-06-11	2014-06-11	External	2014-06-11	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-11	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-11	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-11	Address inactivated. CC was unable to reach the client.	2014
2014-06-11	2014-06-11	External	2014-06-11	Client's Result Letter (Test Result)	2014-06-11	CC inactivated incorrect address	N/A	2014-06-11	Contact Center & Privacy Specialist	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center & Privacy Specialist	2014-06-11	Address inactivated. CC was unable to reach the client.	2014
2014-06-11	2014-06-11	External	2014-06-11	Client's Invitation/Reminder Letter (Screening	2014-06-11	CC inactivated address + Unintended Recipient	N/A	2014-06-11	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact	NO	Contact Center & Privacy Specialist	2014-06-11	Address inactivated. CC was unable to	2014

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				Status/Eligibility)		asked to return letter					intended client.				reach the client.	
2014-06-12	2014-06-12	External	2014-06-12	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-12	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-12	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-12	Address inactivated. CC was unable to reach the client.	2014
2014-06-12	2014-06-12	External	2014-06-12	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-12	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-06-12	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-12	Address inactivated. CC was unable to reach the client.	2014
2014-06-12	2014-06-12	External	2014-06-12	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-12	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-12	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-12	Address inactivated. CC was unable to reach the client.	2014
2014-06-12	2014-06-12	External	2014-06-12	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-12	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-12	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-12	Address inactivated. CC was unable to reach the client.	2014
2014-06-12	2014-06-12	External	2014-06-12	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-12	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-12	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-12	Address inactivated. CC was unable to reach the client.	2014
2014-06-12	2014-06-12	External	2014-06-12	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-12	CC inactivated incorrect address	N/A	2014-06-12	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-12	Address inactivated. CC was unable to reach the client.	2014
2014-06-12	2014-06-12	External	2014-06-12	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-12	CC inactivated incorrect address	N/A	2014-06-12	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-12	Address inactivated. CC was unable to reach the client.	2014
2014-06-12	2014-06-12	External	2014-06-12	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-12	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-12	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-12	Address inactivated. CC was unable to reach the client.	2014
2014-06-12	2014-06-12	External	2014-06-12	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-12	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-12	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-12	Address inactivated. CC was unable to reach the client.	2014

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
2014-06-12	2014-06-12	External	2014-06-12	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-12	CC inactivated incorrect address	N/A	2014-06-12	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-06-12	Address inactivated. CC was unable to reach the client.	2014
2014-06-13	2014-06-13	External	2014-06-13	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-13	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-13	Contact Center	Privacy breach	Contact Center could not reach client, address to be inactivated.	NO	Contact Center	2014-06-13	Address inactivated. CC was unable to obtain client's phone number from PCP.	2014
2014-06-13	2014-06-13	External	2014-06-13	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-13	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-13	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-06-13	Address inactivated. CC was unable to reach the client.	2014
2014-06-13	2014-06-13	External	2014-06-13	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-13	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-13	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-13	Address inactivated. CC was unable to reach the client.	2014
2014-06-13	2014-06-13	External	2014-06-13	Client's Result Letter (Test Result)	2014-06-13	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-13	Contact Center & Privacy Specialist	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center & Privacy Specialist	2014-06-13	CC called the client and updated the address.	2014
2014-06-13	2014-06-13	Internal	2014-06-13	Cannot be determined	2014-06-13	None - received voicemail from unintended recipient notifying of the breach. Could not contact the unintended recipient as they did not leave a callback number. Could not authenticate the intended recipient in InScreen.	N/A	2014-06-13	Contact Center	Privacy breach	CC could not find the client's profile in InScreen, no follow-up possible.	N/A	Contact Center	2014-06-13	CC could not find the client's profile in InScreen, no follow-up possible.	2014
2014-06-13	2014-06-13	Unclear	2014-06-13	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-13	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-06-13	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-06-13	Address inactivated. CC was unable to reach the client.	2014
2014-06-13	2014-06-13	External	2014-06-13	Client's Invitation/Remi	2014-06-13	CC inactivated the address +	N/A	2014-06-13	Contact Center	Privacy breach	Address to be inactivated.	NO	Contact Center	2014-06-13	Address inactivated.	2014

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				nder Letter (Screening Status/Eligibility)		Unintended Recipient to destroy letter					CC to attempt to contact intended client.				CC was unable to reach the client.	
2014-06-13	2014-06-13	External	2014-06-13	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-13	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-06-13	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-06-13	Address inactivated. CC was unable to reach the client.	2014
2014-06-13	2014-06-13	External	2014-06-13	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-13	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-06-13	Contact Center & Privacy Specialist	Privacy breach	Contact Center could not reach client, address to be inactivated.	NO	Contact Center & Privacy Specialist	2014-06-13	CC called the client and updated the address.	2014
2014-06-13	2014-06-13	External	2014-06-13	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-13	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-06-13	Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Privacy Specialist	2014-06-13	Address inactivated. CC was unable to reach the client.	2014
2014-06-13	2014-06-13	External	2014-06-13	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-13	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-06-13	Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Privacy Specialist	2014-06-13	Address inactivated. CC was unable to reach the client.	2014
2014-06-16	2014-06-16	External	2014-06-16	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-16	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-06-16	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-06-16	Address inactivated. CC was unable to reach the client.	2014
2014-06-16	2014-06-16	External	2014-06-16	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-16	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-06-16	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-06-16	Address inactivated. CC was unable to reach the client.	2014
2014-06-16	2014-06-16	External	2014-06-16	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-16	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-16	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-16	Address inactivated. CC was unable to reach the client.	2014
2014-06-16	2014-06-16	External	2014-06-16	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-16	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-06-16	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-16	Address inactivated. CC was unable to reach the client.	2014
2014-06-16	2014-06-16	External	2014-06-16	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-16	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-06-16	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-16	Address inactivated. CC was unable to reach the client.	2014

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
2014-06-16	2014-06-16	External	2014-06-16	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-16	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-06-16	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-16	Address inactivated. CC was unable to reach the client.	2014
2014-06-16	2014-06-16	External	2014-06-16	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-16	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-06-16	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-16	Address inactivated. CC was unable to reach the client.	2014
2014-06-16	2014-06-16	External	2014-06-16	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-16	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-16	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-16	Address inactivated. CC was unable to reach the client.	2014
2014-06-16	2014-06-16	External	2014-06-16	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-16	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-06-16	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-06-16	Address inactivated. CC was unable to reach the client.	2014
2014-06-16	2014-06-16	External	2014-06-16	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-16	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-06-16	Contact Center & Privacy Specialist	Privacy breach	Contact Center could not reach client, address to be inactivated.	NO	Contact Center & Privacy Specialist	2014-06-16	Address inactivated. CC was unable to obtain client's phone number from PCP.	2014
2014-06-17	2014-06-17	External	2014-06-17	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-17	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-17	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-17	Address inactivated. CC was unable to reach the client.	2014
2014-06-17	2014-06-17	External	2014-06-17	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-17	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-17	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-17	Address inactivated. CC was unable to reach the client.	2014
2014-06-17	2014-06-17	External	2014-06-17	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-17	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-17	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-17	Address inactivated. CC was unable to reach the client.	2014
2014-06-17	2014-06-17	Unclear	2014-06-17	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-17	None - relative of client provided the client's information to the CC. The CC then disclosed PHI to this relative;	N/A	2014-06-17	Contact Center	Privacy breach	CC to advise the relative of the client to apply for substitute decision-maker status.	NO	Contact Center	2014-06-17	CC advised the relative of the client to apply for substitute decision-maker status. No action taken to	2014

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
						therefore it is considered a breach. No containment possible.									provide training to the CC agent - possibly because authentication methods were correct.	
2014-06-17	2014-06-17	External	2014-06-17	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-17	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-06-17	Contact Center & Privacy Specialist	Privacy breach	Contact Center could not reach client, address to be inactivated.	NO	Contact Center & Privacy Specialist	2014-06-17	Address inactivated. CC was unable to obtain client's phone number from PCP.	2014
2014-06-17	2014-06-17	External	2014-06-17	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-17	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-06-17	Contact Center & Privacy Specialist	Privacy breach	Contact Center could not reach client, address to be inactivated.	NO	Contact Center & Privacy Specialist	2014-06-17	Address inactivated. CC was unable to obtain client's phone number from PCP.	2014
2014-06-17	2014-06-17	External	2014-06-17	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-17	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-17	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-17	Address inactivated. CC was unable to reach the client.	2014
2014-06-17	2014-06-17	External	2014-06-17	Client's Result Letter (Test Result)	2014-06-17	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-06-17	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center	2014-06-17	CC called the client and updated the address.	2014
2014-06-17	2014-06-17	External	2014-06-17	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-17	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-17	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-06-17	Address inactivated. CC was unable to reach the client.	2014
2014-06-17	2014-06-17	External	2014-06-17	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-17	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-17	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-17	Address inactivated. CC was unable to reach the client.	2014
2014-06-17	2014-06-17	External	2014-06-17	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-17	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-06-17	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-17	Address inactivated. CC was unable to reach the client.	2014
2014-06-17	2014-06-17	External	2014-06-17	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-17	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-17	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-17	Address inactivated. CC was unable to reach the client.	2014

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
2014-06-17	2014-06-17	External	2014-06-17	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-17	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-17	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-17	Address inactivated. CC was unable to reach the client.	2014
2014-06-18	2014-06-18	External	2014-06-18	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-18	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-18	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-18	Address inactivated. CC was unable to reach the client.	2014
2014-06-18	2014-06-18	External	2014-06-18	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-18	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-18	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-18	Address inactivated. CC was unable to reach the client.	2014
2014-06-18	2014-06-18	External	2014-06-18	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-18	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-18	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-18	Address inactivated. CC was unable to reach the client.	2014
2014-06-18	2014-06-18	External	2014-06-18	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-18	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-18	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-18	Address inactivated. CC was unable to reach the client.	2014
2014-06-18	2014-06-18	External	2014-06-18	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-18	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-06-18	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-18	Address inactivated. CC was unable to reach the client.	2014
2014-06-20	2014-06-20	External	2014-06-20	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-20	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-06-20	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	YES	Contact Center	2014-06-20	Address inactivated. CC was unable to reach the client.	2014
2014-06-20	2014-06-20	External	2014-06-20	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-20	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-20	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-06-20	Address inactivated. CC was unable to reach the client.	2014
2014-06-23	2014-06-23	External	2014-06-23	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-23	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-06-23	Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Privacy Specialist	2014-06-23	Address inactivated. CC was unable to reach the client.	2014
2014-06-23	2014-06-23	External	2014-06-23	Client's Invitation/Reminder Letter (Screening	2014-06-23	CC inactivated address + Unintended Recipient	N/A	2014-06-23	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact	NO	Contact Center & Privacy Specialist	2014-06-23	Address inactivated. CC was unable to	2014

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				Status/Eligibility)		asked to return letter					intended client.				reach the client.	
2014-06-23	2014-06-23	External	2014-06-23	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-23	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-06-23	Contact Center	Privacy breach	Contact Center could not reach client, address to be inactivated.	NO	Contact Center	2014-06-23	Address inactivated. CC was unable to obtain client's phone number from PCP.	2014
2014-06-23	2014-06-23	External	2014-06-23	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-23	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-06-23	Contact Center & Privacy Specialist	Privacy breach	Contact Center could not reach client, address to be inactivated.	NO	Contact Center & Privacy Specialist	2014-06-23	Address inactivated. CC was unable to obtain client's phone number from PCP.	2014
2014-06-23	2014-06-23	External	2014-06-23	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-23	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-23	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-23	Address inactivated. CC was unable to reach the client.	2014
2014-06-23	2014-06-23	External	2014-06-23	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-23	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-23	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-23	Address inactivated. CC was unable to reach the client.	2014
2014-06-23	2014-06-23	External	2014-06-23	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-23	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-23	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-23	Address inactivated. CC was unable to reach the client.	2014
2014-06-23	2014-06-23	External	2014-06-23	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-23	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-06-23	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-23	Address inactivated. CC was unable to reach the client.	2014
2014-06-23	2014-06-23	External	2014-06-23	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-23	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-06-23	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-06-23	Address inactivated. CC was unable to reach the client.	2014
2014-06-23	2014-06-23	External	2014-06-23	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-23	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-23	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-23	Address inactivated. CC was unable to reach the client.	2014
2014-06-23	2014-06-23	External	2014-06-23	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-23	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-23	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-23	Address inactivated. CC was unable to reach the client.	2014

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
2014-06-24	2014-06-24	External	2014-06-24	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-24	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-06-24	Contact Center & Privacy Specialist	Privacy breach	Contact Center could not reach client, address to be inactivated.	NO	Contact Center & Privacy Specialist	2014-06-24	Address inactivated. CC was unable to obtain client's phone number from PCP.	2014
2014-06-24	2014-06-24	External	2014-06-24	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-24	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-24	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-06-24	Address inactivated. CC was unable to reach the client.	2014
2014-06-24	2014-06-24	External	2014-06-24	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-24	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-24	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-24	Address inactivated. CC was unable to reach the client.	2014
2014-06-24	2014-06-24	External	2014-06-24	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-24	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-24	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-24	Address inactivated. CC was unable to reach the client.	2014
2014-06-24	2014-06-24	External	2014-06-24	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-24	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-24	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-24	Address inactivated. CC was unable to reach the client.	2014
2014-06-24	2014-06-24	External	2014-06-24	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-24	CC inactivated incorrect address	N/A	2014-06-24	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-06-24	Address inactivated. CC was unable to reach the client.	2014
2014-06-24	2014-06-24	External	2014-06-24	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-24	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-24	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-24	Address inactivated. CC was unable to reach the client.	2014
2014-06-24	2014-06-24	External	2014-06-24	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-24	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-24	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-24	Address inactivated. CC was unable to reach the client.	2014
2014-06-24	2014-06-24	External	2014-06-24	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-24	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-24	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-06-24	Address inactivated. CC was unable to reach the client.	2014
2014-06-24	2014-06-24	External	2014-06-24	Client's Invitation/Reminder Letter	2014-06-24	Address inactivated -	N/A	2014-06-24	Contact Center &	Privacy breach	Address to be inactivated. CC to attempt	NO	Contact Center &	2014-06-24	Address inactivated. CC was	2014

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				(Screening Status/Eligibility)		Letter will not be returned			Privacy Specialist		to contact intended client.		Privacy Specialist		unable to reach the client.	
2014-06-24	2014-06-24	External	2014-06-24	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-24	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-24	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-06-24	Address inactivated. CC was unable to reach the client.	2014
2014-06-24	2014-06-24	External	2014-06-24	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-24	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-24	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-24	Address inactivated. CC was unable to reach the client.	2014
2014-06-24	2014-06-24	External	2014-06-24	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-24	CC inactivated incorrect address	N/A	2014-06-24	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-06-24	Address inactivated. CC was unable to reach the client.	2014
2014-06-24	2014-06-24	External	2014-06-24	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-24	CC inactivated incorrect address	N/A	2014-06-24	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-06-24	Address inactivated. CC was unable to reach the client.	2014
2014-06-24	2014-06-24	External	2014-06-24	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-24	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-24	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-24	Address inactivated. CC was unable to reach the client.	2014
2014-06-24	2014-06-24	External	2014-06-24	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-24	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-24	Contact Center & Privacy Specialist	Privacy breach	Contact Center could not reach client, address to be inactivated.	NO	Contact Center & Privacy Specialist	2014-06-24	Address inactivated. CC was unable to obtain client's phone number from PCP.	2014
2014-06-24	2014-06-24	External	2014-06-24	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-24	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-06-24	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-06-24	Address inactivated. CC was unable to reach the client.	2014
2014-06-25	2014-06-25	External	2014-06-25	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-25	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-25	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-25	Address inactivated. CC was unable to reach the client.	2014
2014-06-25	2014-06-25	External	2014-06-25	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-25	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-25	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-25	Address inactivated. CC was unable to reach the client.	2014

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
2014-06-25	2014-06-25	Internal	2014-06-25	N/A	2014-06-25	None - could not reach unintended recipient after initial voicemail. Could not authenticate the intended recipient in InScreen.	N/A	2014-06-25	Contact Center	Privacy breach	CC could not find the client (intended recipient)'s profile in InScreen, no follow-up possible.	NO	Contact Center	2014-06-25	CC could not find the client (intended recipient)'s profile in InScreen, no follow-up possible.	2014
2014-06-25	2014-06-25	External	2014-06-25	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-25	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-25	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-25	Address inactivated. CC was unable to reach the client.	2014
2014-06-25	2014-06-25	External	2014-06-25	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-25	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-25	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-25	Address inactivated. CC was unable to reach the client.	2014
2014-06-25	2014-06-25	External	2014-06-25	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-25	CC inactivated incorrect address	N/A	2014-06-25	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-06-25	Address inactivated. CC was unable to reach the client.	2014
2014-06-25	2014-06-25	Internal	2014-06-25	N/A	2014-06-25	None - could not reach unintended recipient after initial voicemail. Could not authenticate the intended recipient in InScreen.	N/A	2014-06-25	Contact Center	Privacy breach	CC could not find the client (intended recipient)'s profile in InScreen, no follow-up possible.	NO	Contact Center	2014-06-25	CC could not find the client (intended recipient)'s profile in InScreen, no follow-up possible.	2014
2014-06-25	2014-06-25	External	2014-06-25	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-25	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-25	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-06-25	Address inactivated. CC was unable to reach the client.	2014
2014-06-25	2014-06-25	External	2014-06-25	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-25	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-25	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-25	Address inactivated. CC was unable to reach the client.	2014
2014-06-25	2014-06-25	External	2014-06-25	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-25	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-25	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-25	Address inactivated. CC was unable to reach the client.	2014

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
2014-06-26	2014-06-26	External	2014-06-26	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-26	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-26	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-26	Address inactivated. CC was unable to reach the client.	2014
2014-06-26	2014-06-26	External	2014-06-26	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-26	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-26	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-26	Address inactivated. CC was unable to reach the client.	2014
2014-06-26	2014-06-26	External	2014-06-26	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-26	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-06-26	Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Privacy Specialist	2014-06-26	Address inactivated. CC was unable to reach the client.	2014
2014-06-26	2014-06-26	External	2014-06-26	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-26	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-26	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-26	Address inactivated. CC was unable to reach the client.	2014
2014-06-26	2014-06-26	External	2014-06-26	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-26	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-26	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-06-26	Address inactivated. CC was unable to reach the client.	2014
2014-06-26	2014-06-26	External	2014-06-26	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-26	CC inactivated incorrect address	N/A	2014-06-26	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-06-26	Address inactivated. CC was unable to reach the client.	2014
2014-06-26	2014-06-26	External	2014-06-26	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-26	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-06-26	Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Privacy Specialist	2014-06-26	Address inactivated. CC was unable to reach the client.	2014
2014-06-26	2014-06-26	External	2014-06-26	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-26	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-26	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-26	Address inactivated. CC was unable to reach the client.	2014
2014-06-26	2014-06-26	External	2014-06-26	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-26	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-06-26	Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Privacy Specialist	2014-06-26	Address inactivated. CC was unable to reach the client.	2014
2014-06-26	2014-06-26	External	2014-06-26	Client's Invitation/Reminder Letter (Screening	2014-06-26	CC inactivated the address + Unintended	N/A	2014-06-26	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact	NO	Contact Center	2014-06-26	Address inactivated. CC was unable to	2014

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				Status/Eligibility)		Recipient to destroy letter					intended client.				reach the client.	
2014-06-26	2014-06-26	External	2014-06-26	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-26	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-06-26	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-06-26	Address inactivated. CC was unable to reach the client.	2014
2014-06-27	2014-06-27	External	2014-06-27	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-27	CC inactivated incorrect address	N/A	2014-06-27	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-06-27	Address inactivated. CC was unable to reach the client.	2014
2014-06-30	2014-06-30	External	2014-06-30	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-30	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-30	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-30	Address inactivated. CC was unable to reach the client.	2014
2014-06-30	2014-06-30	External	2014-06-30	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-30	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-30	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-30	Address inactivated. CC was unable to reach the client.	2014
2014-06-30	2014-06-30	External	2014-06-30	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-30	Address inactivated - Letter will not be returned	N/A	2014-06-30	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	2014-06-30	CC was unable to reach the PCP and address inactivated.	2014
2014-06-30	2014-06-30	External	2014-06-30	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-30	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-06-30	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-30	Address inactivated. CC was unable to reach the client.	2014
2014-06-30	2014-06-30	External	2014-06-30	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-30	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-30	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-06-30	Address inactivated. CC was unable to reach the client.	2014
2014-06-30	2014-06-30	External	2014-06-30	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-06-30	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-06-30	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-06-30	Address inactivated. CC was unable to reach the client.	2014
2014-07-02	2014-07-02	External	2014-07-02	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-07-02	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-07-02	Contact Center & Privacy Specialist	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center & Privacy Specialist	2014-07-02	CC called the client and updated the address.	2014
2014-07-02	2014-07-02	External	2014-07-02	Client's Invitation/Remi	2014-07-02	Address inactivated -	N/A	2014-07-02	Contact Center &	Privacy breach	Contact Center to call	NO	Contact Center	2014-07-02	Address inactivated.	2014

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				nder Letter (Screening Status/Eligibility)		Letter will not be returned			Privacy Specialist		client/PCP and update address.				CC was unable to reach the client.	
2014-07-02	2014-07-02	External	2014-07-02	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-07-02	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-07-02	Privacy Specialist	Privacy breach	Contact Center could not reach client, address to be inactivated.	NO	Privacy Specialist	2014-07-02	Address inactivated. CC was unable to obtain client's phone number from PCP.	2014
2014-07-02	2014-07-02	External	2014-07-02	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-07-02	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-07-02	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-07-02	Address inactivated. CC was unable to reach the client.	2014
2014-07-02	2014-07-02	External	2014-07-02	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-07-02	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-07-02	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-07-02	Address inactivated. CC was unable to reach the client.	2014
2014-07-02	2014-07-02	External	2014-07-02	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-07-02	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-07-02	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-07-02	Address inactivated. CC was unable to reach the client.	2014
2014-07-02	2014-07-02	External	2014-07-02	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-07-02	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-07-02	Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Privacy Specialist	2014-07-02	Address inactivated. CC was unable to reach the client.	2014
2014-07-02	2014-07-02	External	2014-07-02	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-07-02	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-07-02	Privacy Specialist	Privacy breach	Contact Center could not reach client, address to be inactivated.	NO	Privacy Specialist	2014-07-02	Address inactivated. CC was unable to obtain client's phone number from PCP.	2014
2014-07-03	2014-07-03	External	2014-07-03	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-07-03	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-07-03	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-07-03	Address inactivated. CC was unable to reach the client.	2014
2014-07-03	2014-07-03	External	2014-07-03	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-07-03	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-07-03	Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Privacy Specialist	2014-07-03	Address inactivated. CC was unable to reach the client.	2014
2014-07-03	2014-07-03	External	2014-07-03	Client's Invitation/Reminder Letter (Screening	2014-07-03	CC inactivated address + Unintended Recipient	N/A	2014-07-03	Contact Center & Privacy Specialist	Privacy breach	Contact Center to call client/PCP and	NO	Contact Center & Privacy Specialist	2014-07-03	Address inactivated. CC was unable to	2014

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				Status/Eligibility)		asked to return letter					update address.				reach the client.	
2014-07-03	2014-07-03	External	2014-07-03	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-07-03	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-07-03	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-07-03	Address inactivated. CC was unable to reach the client.	2014
2014-07-03	2014-07-03	External	2014-07-03	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-07-03	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-07-03	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-07-03	Address inactivated. CC was unable to reach the client.	2014
2014-07-03	2014-07-03	External	2014-07-03	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-07-03	CC inactivated incorrect address	N/A	2014-07-03	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-07-03	Address inactivated. CC was unable to reach the client.	2014
2014-07-03	2014-07-03	External	2014-07-03	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-07-03	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-07-03	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-07-03	Address inactivated. CC was unable to reach the client.	2014
2014-07-03	2014-07-03	External	2014-07-03	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-07-03	N/A - Canada Post delivery error - unintended said that they would send the letter back to CCO, however it is unclear if they did.	N/A	2014-07-03	Contact Center	Privacy breach	N/A - no recommendations logged.	NO	Contact Center	2014-07-03	N/A - no recommendations logged.	2014
2014-07-03	2014-07-03	External	2014-07-03	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-07-03	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-07-03	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-07-03	Address inactivated. CC was unable to reach the client.	2014
2014-07-04	2014-07-04	External	2014-07-04	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-07-04	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-07-04	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-07-04	Address inactivated. CC was unable to reach the client.	2014
2014-07-04	2014-07-04	External	2014-07-04	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-07-04	CC inactivated incorrect address	N/A	2014-07-04	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-07-04	Address inactivated. CC was unable to reach the client.	2014
2014-07-04	2014-07-04	External	2014-07-04	Client's Invitation/Reminder Letter	2014-07-04	CC inactivated the address + Unintended	N/A	2014-07-04	Contact Center	Privacy breach	Address to be inactivated. CC to attempt	NO	Contact Center	2014-07-04	Address inactivated. CC was	2014

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				(Screening Status/Eligibility)		Recipient to destroy letter					to contact intended client.				unable to reach the client.	
2014-07-04	2014-07-04	External	2014-07-04	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-07-04	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-07-04	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-07-04	Address inactivated. CC was unable to reach the client.	2014
2014-07-04	2014-07-04	External	2014-07-04	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-07-04	CC inactivated incorrect address	N/A	2014-07-04	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-07-04	Address inactivated. CC was unable to reach the client.	2014
2014-07-07	2014-07-07	External	2014-07-07	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-07-07	Address inactivated - Letter will not be returned	N/A	2014-07-07	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-07-07	Address inactivated. CC was unable to reach the client.	2014
2014-07-07	2014-07-07	External	2014-07-07	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-07-07	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-07-07	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-07-07	Address inactivated. CC was unable to reach the client.	2014
2014-07-07	2014-07-07	External	2014-07-07	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-07-07	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-07-07	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-07-07	Address inactivated. CC was unable to reach the client.	2014
2014-07-07	2014-07-07	External	2014-07-07	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-07-07	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-07-07	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-07-07	Address inactivated. CC was unable to reach the client.	2014
2014-07-07	2014-07-07	External	2014-07-07	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-07-07	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-07-07	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-07-07	Address inactivated. CC was unable to reach the client.	2014
2014-07-07	2014-07-07	External	2014-07-07	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-07-07	CC inactivated incorrect address	N/A	2014-07-07	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-07-07	Address inactivated. CC was unable to reach the client.	2014
2014-07-07	2014-07-07	External	2014-07-07	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-07-07	CC inactivated incorrect address	N/A	2014-07-07	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-07-07	Address inactivated. CC was unable to reach the client.	2014

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
2014-07-07	2014-07-07	External	2014-07-07	Client's Result Letter (Test Result)	2014-07-07	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-07-07	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-07-07	Address inactivated. CC was unable to reach the client.	2014
2014-07-07	2014-07-07	External	2014-07-07	Client's Result Letter (Test Result)	2014-07-07	CC inactivated incorrect address	N/A	2014-07-07	Contact Center & Privacy Specialist	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center & Privacy Specialist	2014-07-07	Address updated. CC was able to contact the client via number provided by their PCP.	2014
2014-07-07	2014-07-07	External	2014-07-07	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-07-07	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-07-07	Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Privacy Specialist	2014-07-07	Address inactivated. CC was unable to reach the client.	2014
2014-07-08	2014-07-08	Internal	2014-07-08	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-07-08	N/A - results letter from OBSP screening site was sent in an envelope addressed to a different client. Unclear whether this was the screening site's own breach or CCO's breach.	N/A	2014-07-08	Contact Center	Privacy breach	Screening site should be notified of the breach.	NO	Contact Center	2014-07-08	Unintended recipient was asked to notify the screening site of the breach.	2014
2014-07-08	2014-07-08	External	2014-07-08	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-07-08	CC inactivated incorrect address	N/A	2014-07-08	Contact Center & Privacy Specialist	Privacy breach	Contact Center could not reach client, address to be inactivated.	NO	Contact Center & Privacy Specialist	2014-07-08	CC called the client and updated the address.	2014
2014-07-08	2014-07-08	External	2014-07-08	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-07-08	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-07-08	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-07-08	Address inactivated. CC was unable to reach the client.	2014
2014-07-08	2014-07-08	External	2014-07-08	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-07-08	CC inactivated incorrect address	N/A	2014-07-08	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-07-08	Address inactivated. CC was unable to reach the client.	2014
2014-07-08	2014-07-08	External	2014-07-08	Client's Invitation/Reminder Letter (Screening	2014-07-08	CC inactivated incorrect address	N/A	2014-07-08	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact	NO	Contact Center	2014-07-08	Address inactivated. CC was unable to	2014

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				Status/Eligibility)							intended client.				reach the client.	
2014-07-08	2014-07-08	External	2014-07-08	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-07-08	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-07-08	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-07-08	Address inactivated. CC was unable to reach the client.	2014
2014-07-08	2014-07-08	External	2014-07-08	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-07-08	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-07-08	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-07-08	Address inactivated. CC was unable to reach the client.	2014
2014-07-08	2014-07-08	External	2014-07-08	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-07-08	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-07-08	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-07-08	Address inactivated. CC was unable to reach the client.	2014
2014-07-08	2014-07-08	External	2014-07-08	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-07-08	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-07-08	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-07-08	Address inactivated. CC was unable to reach the client.	2014
2014-07-09	2014-07-09	External	2014-07-09	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-07-09	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-07-09	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-07-09	Address inactivated. CC was unable to reach the client.	2014
2014-07-09	2014-07-09	External	2014-07-09	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-07-09	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-07-09	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-07-09	Address inactivated. CC was unable to reach the client.	2014
2014-07-09	2014-07-09	External	2014-07-09	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-07-09	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-07-09	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-07-09	Address inactivated. CC was unable to reach the client.	2014
2014-07-10	2014-07-10	Internal	2014-07-10	N/A	2014-07-10	None - unintended recipient left voicemail notifying that the intended recipient had moved out of province. Unclear if there was any way to call the unintended recipient back	N/A	2014-07-10	Contact Center	Privacy breach	CC could not find the client (intended recipient)'s profile in InScreen, no follow-up possible.	N/A	Contact Center	2014-07-10	CC could not find the client (intended recipient)'s profile in InScreen, no follow-up possible.	2014

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
						or what actions were taken to reach them. Could not authenticate the intended recipient in InScreen.										
2014-07-10	2014-07-10	External	2014-07-10	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-07-10	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-07-10	Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Privacy Specialist	2014-07-10	Address inactivated. CC was unable to reach the client.	2014
2014-07-10	2014-07-10	External	2014-07-10	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-07-10	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-07-10	Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Privacy Specialist	2014-07-10	Address inactivated. CC was unable to reach the client.	2014
2014-07-10	2014-07-10	External	2014-07-10	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-07-10	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-07-10	Privacy Specialist	Privacy breach	Contact Center to call client/PCP and update address.	YES	Privacy Specialist	2014-07-10	CC was unable to reach the PCP and address inactivated.	2014
2014-07-10	2014-07-10	External	2014-07-10	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-07-10	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-07-10	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-07-10	Address inactivated. CC was unable to reach the client.	2014
2014-07-11	2014-07-11	External	2014-07-11	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-07-11	Address inactivated - Letter will not be returned	N/A	2014-07-11	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	2014-07-11	Address updated. CC was able to contact the client via number provided by their PCP.	2014
2014-07-11	2014-07-11	External	2014-07-11	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-07-11	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-07-11	Privacy Specialist	Privacy breach	Contact Center could not reach client, address to be inactivated.	NO	Privacy Specialist	2014-07-11	Address inactivated. CC was unable to obtain client's phone number from PCP.	2014
2014-07-14	2014-07-14	External	2014-07-14	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-07-14	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-07-14	Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Privacy Specialist	2014-07-14	Address inactivated. CC was unable to reach the client.	2014
2014-07-14	2014-07-14	External	2014-07-14	Client's Invitation/Reminder Letter (Screening	2014-07-14	CC inactivated address + Unintended Recipient	N/A	2014-07-14	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact	NO	Contact Center & Privacy Specialist	2014-07-14	Address inactivated. CC was unable to	2014

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				Status/Eligibility)		asked to return letter					intended client.				reach the client.	
2014-07-14	2014-07-14	External	2014-07-14	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-07-14	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-07-14	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-07-14	Address inactivated. CC was unable to reach the client.	2014
2014-07-14	2014-07-14	External	2014-07-14	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-07-14	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-07-14	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-07-14	Address inactivated. CC was unable to reach the client.	2014
2014-07-15	2014-07-15	External	2014-07-15	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-07-15	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-07-15	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-07-15	Address inactivated. CC was unable to reach the client.	2014
2014-07-15	2014-07-15	External	2014-07-15	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-07-15	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-07-15	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-07-15	Address inactivated. CC was unable to reach the client.	2014
2014-07-15	2014-07-15	External	2014-07-15	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-07-15	CC inactivated incorrect address	N/A	2014-07-15	Contact Center & Privacy Specialist	Privacy breach	Contact Center could not reach client, address to be inactivated.	NO	Contact Center & Privacy Specialist	2014-07-15	Address inactivated. CC was unable to obtain client's phone number from PCP.	2014
2014-07-16	2014-07-16	External	2014-07-16	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-07-16	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-07-16	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-07-16	Address inactivated. CC was unable to reach the client.	2014
2014-07-16	2014-07-16	External	2014-07-16	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-07-16	Address inactivated - Letter will not be returned	N/A	2014-07-16	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-07-16	Address inactivated. CC was unable to reach the client.	2014
2014-07-16	2014-07-16	External	2014-07-16	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-07-16	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-07-16	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-07-16	Address inactivated. CC was unable to reach the client.	2014
2014-07-17	2014-07-17	External	2014-07-17	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-07-17	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-07-17	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-07-17	Address inactivated. CC was unable to reach the client.	2014

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
2014-07-17	2014-07-17	External	2014-07-17	Client's Result Letter (Test Result)	2014-07-17	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-07-17	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	YES	Contact Center	2014-07-17	Address inactivated. CC was unable to reach the client.	2014
2014-07-17	2014-07-17	External	2014-07-17	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-07-17	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-07-17	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-07-17	Address inactivated. CC was unable to reach the client.	2014
2014-07-17	2014-07-17	External	2014-07-17	Client's Result Letter (Test Result)	2014-07-17	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-07-17	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-07-17	Address inactivated. CC was unable to reach the client.	2014
2014-07-17	2014-07-17	External	2014-07-17	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-07-17	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-07-17	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center	2014-07-17	Address inactivated. CC was unable to reach the client.	2014
2014-07-17	2014-07-17	External	2014-07-17	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-07-17	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-07-17	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-07-17	Address inactivated. CC was unable to reach the client.	2014
2014-07-17	2014-07-17	External	2014-07-17	Client's Result Letter (Test Result)	2014-07-17	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-07-17	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	2014-07-17	Address inactivated. CC was unable to reach the client.	2014
2014-07-18	2014-07-18	External	2014-07-18	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-07-18	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-07-18	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-07-18	Address inactivated. CC was unable to reach the client.	2014
2014-07-18	2014-07-18	External	2014-07-18	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-07-18	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-07-18	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-07-18	Address inactivated. CC was unable to reach the client.	2014
2014-07-21	2014-07-21	External	2014-07-21	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-07-21	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-07-21	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-07-21	Address inactivated. CC was unable to reach the client.	2014
2014-07-21	2014-07-21	External	2014-07-21	Client's Invitation/Reminder Letter (Screening	2014-07-21	CC inactivated incorrect address	N/A	2014-07-21	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact	NO	Contact Center	2014-07-21	Address inactivated. CC was unable to	2014

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				Status/Eligibility)							intended client.				reach the client.	
2014-07-21	2014-07-21	External	2014-07-21	Client's Result Letter (Test Result)	2014-07-21	CC inactivated incorrect address	N/A	2014-07-21	Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	YES	Privacy Specialist	2014-07-21	Address inactivated. CC was unable to reach the client.	2014
2014-07-21	2014-07-21	External	2014-07-21	Client's Result Letter (Test Result)	2014-07-21	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-07-21	Contact Center & Privacy Specialist	Privacy breach	Contact Center could not reach client, address to be inactivated.	NO	Contact Center & Privacy Specialist	2014-07-21	Address inactivated. CC was unable to obtain client's phone number from PCP.	2014
2014-07-21	2014-07-21	External	2014-07-21	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-07-21	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-07-21	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-07-21	Address inactivated. CC was unable to reach the client.	2014
2014-07-22	2014-07-22	External	2014-07-22	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-07-22	Address inactivated - Letter will not be returned	N/A	2014-07-22	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	YES	Contact Center	2014-07-22	Address inactivated. CC was unable to reach the client.	2014
2014-07-22	2014-07-22	External	2014-07-22	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-07-22	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-07-22	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-07-22	Address inactivated. CC was unable to reach the client.	2014
2014-07-23	2014-07-23	External	2014-07-23	Client's Result Letter (Test Result)	2014-07-23	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-07-23	Privacy Specialist	Privacy breach	Contact Center to call client/PCP and update address.	NO	Privacy Specialist	2014-07-23	CC called the client and updated the address.	2014
2014-07-23	2014-07-23	External	2014-07-23	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-07-23	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-07-23	Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Privacy Specialist	2014-07-23	Address inactivated. CC was unable to reach the client.	2014
2014-07-25	2014-07-25	External	2014-07-25	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-07-25	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-07-25	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-07-25	Address inactivated. CC was unable to reach the client.	2014
2014-07-28	2014-07-28	External	2014-07-28	Client's Result Letter (Test Result)	2014-07-28	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-07-28	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	YES	Contact Center & Privacy Specialist	2014-07-28	Address inactivated. CC was unable to reach the client.	2014

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
2014-07-30	2014-07-30	External	2014-07-30	Client's Result Letter (Test Result)	2014-07-30	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-07-30	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center	2014-07-30	CC called the client and updated the address.	2014
2014-07-31	2014-07-31	External	2014-07-31	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-07-31	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-07-31	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-07-31	Address inactivated. CC was unable to reach the client.	2014
2014-08-06	2014-08-06	External	2014-08-06	Client's Result Letter (Test Result)	2014-08-06	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-08-06	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-08-06	Address inactivated. CC was unable to reach the client.	2014
2014-08-06	2014-08-06	External	2014-08-06	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-08-06	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-08-06	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-08-06	Address inactivated. CC was unable to reach the client.	2014
2014-08-07	2014-08-07	External	2014-08-07	Client's Result Letter (Test Result)	2014-08-07	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-08-07	Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Privacy Specialist	2014-08-07	Address inactivated. CC was unable to reach the client.	2014
2014-08-07	2014-08-07	External	2014-08-07	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-08-07	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-08-07	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-08-07	Address inactivated. CC was unable to reach the client.	2014
2014-08-07	2014-08-07	External	2014-08-07	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-08-07	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-08-07	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-08-07	Address inactivated. CC was unable to reach the client.	2014
2014-08-11	2014-08-11	External	2014-08-11	Client's Result Letter (Test Result)	2014-08-11	CC inactivated incorrect address	N/A	2014-08-11	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	YES	Contact Center & Privacy Specialist	2014-08-11	Address inactivated. CC was unable to reach the client.	2014
2014-08-11	2014-08-11	External	2014-08-11	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-08-11	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-08-11	Contact Center & Privacy Specialist	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center & Privacy Specialist	2014-08-11	CC called the client and updated the address.	2014
2014-08-11	2014-08-11	External	2014-08-11	Client's Result Letter (Test Result)	2014-08-11	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-08-11	Contact Center	Privacy breach	Contact Center could not reach client, address	NO	Contact Center	2014-08-11	CC called the client and updated the address.	2014

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
											to be inactivated.					
2014-08-13	2014-08-13	External	2014-08-13	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-08-13	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-08-13	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-08-13	Address inactivated. CC was unable to reach the client.	2014
2014-08-13	2014-08-13	External	2014-08-13	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-08-13	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-08-13	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-08-13	Address inactivated. CC was unable to reach the client.	2014
2014-08-18	2014-08-18	External	2014-08-18	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-08-18	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-08-18	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-08-18	Address inactivated. CC was unable to reach the client.	2014
2014-08-19	2014-08-19	External	2014-08-19	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-08-19	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-08-19	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-08-19	Address inactivated. CC was unable to reach the client.	2014
2014-08-19	2014-08-19	External	2014-08-19	Client's Result Letter (Test Result)	2014-08-19	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-08-19	Contact Center & Privacy Specialist	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center & Privacy Specialist	2014-08-19	CC called the client and updated the address.	2014
2014-08-19	2014-08-19	External	2014-08-19	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-08-19	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-08-19	Contact Center & Privacy Specialist	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center & Privacy Specialist	2014-08-19	CC called the client and updated the address.	2014
2014-08-19	2014-08-19	External	2014-08-19	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-08-19	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-08-19	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-08-19	Address inactivated. CC was unable to reach the client.	2014
2014-08-19	2014-08-19	External	2014-08-19	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-08-19	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-08-19	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-08-19	Address inactivated. CC was unable to reach the client.	2014
2014-08-20	2014-08-20	External	2014-08-20	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-08-20	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-08-20	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-08-20	Address inactivated. CC was unable to reach the client.	2014
2014-08-20	2014-08-20	External	2014-08-20	Client's Invitation/Remi	2014-08-20	CC inactivated address +	N/A	2014-08-20	Contact Center &	Privacy breach	Address to be inactivated.	NO	Contact Center &	2014-08-20	Address inactivated.	2014

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				nder Letter (Screening Status/Eligibility)		Unintended Recipient asked to return letter			Privacy Specialist		CC to attempt to contact intended client.		Privacy Specialist		CC was unable to reach the client.	
2014-08-20	2014-08-20	External	2014-08-20	Client's Result Letter (Test Result)	2014-08-20	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-08-20	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-08-20	Address inactivated. CC was unable to reach the client.	2014
2014-08-20	2014-08-20	External	2014-08-20	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-08-20	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-08-20	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-08-20	Address inactivated. CC was unable to reach the client.	2014
2014-08-20	2014-08-20	Internal	2014-08-20	N/A	2014-08-20	None - unintended recipient called to advise that they received a letter for the intended recipient. Per InScreen, could not authenticate the intended recipient in InScreen. (However, the log states that CC had inactivated the client's address.)	N/A	2014-08-20	Contact Center	Privacy breach	CC could not find the client (intended recipient)'s profile in InScreen, no follow-up possible.	N/A	Contact Center	2014-08-20	CC could not find the client (intended recipient)'s profile in InScreen, no follow-up possible.	2014
2014-08-21	2014-08-21	External	2014-08-21	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-08-21	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-08-21	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-08-21	Address inactivated. CC was unable to reach the client.	2014
2014-08-21	2014-08-21	External	2014-08-21	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-08-21	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-08-21	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-08-21	Address inactivated. CC was unable to reach the client.	2014
2014-08-21	2014-08-21	External	2014-08-21	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-08-21	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-08-21	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-08-21	Address inactivated. CC was unable to reach the client.	2014
2014-08-26	2014-08-26	Internal	2014-08-26	Client's Invitation/Reminder Letter	2014-08-26	None - improper authentication	N/A	2014-08-26	Contact Center	Privacy breach	N/A - no recommendations logged.	NO	Contact Center	2014-08-26	N/A - no recommendations logged.	2014

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				(Screening Status/Eligibility)		prior to disclosing PHI. No containment possible.										
2014-08-26	2014-08-26	External	2014-08-26	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-08-26	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-08-26	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-08-26	Address inactivated. CC was unable to reach the client.	2014
2014-08-26	2014-08-26	Internal	2014-08-26	Client's Result Letter (Test Result)	2014-08-26	None - CC spoke to the relative of a client who opened the client's letter. Since the relative hung up before the agent could gather more info about the client, no containment possible.	N/A	2014-08-26	Contact Center	Privacy breach	CC could not find the client (intended recipient)'s profile in InScreen, no follow-up possible.	NO	Contact Center	2014-08-26	CC could not find the client (intended recipient)'s profile in InScreen, no follow-up possible.	2014
2014-08-27	2014-08-27	External	2014-08-27	Client's Result Letter (Test Result)	2014-08-27	CC inactivated incorrect address	N/A	2014-08-27	Privacy Specialist	Privacy breach	Contact Center to call client/PCP and update address.	NO	Privacy Specialist	2014-08-27	CC called the client and updated the address.	2014
2014-09-05	2014-09-05	External	2014-09-05	Client's Result Letter (Test Result)	2014-09-05	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-09-05	Contact Center & Privacy Specialist	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center & Privacy Specialist	2014-09-05	Address inactivated. CC was unable to reach the client.	2014
2014-09-05	2014-09-05	External	2014-09-05	Client's Result Letter (Test Result)	2014-09-05	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-09-05	Contact Center & Privacy Specialist	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center & Privacy Specialist	2014-09-05	Address updated. CC was able to contact the client via number provided by their PCP.	2014
2014-09-08	2014-09-08	External	2014-09-08	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-09-08	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-09-08	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-09-08	Address inactivated. CC was unable to reach the client.	2014
2014-09-09	2014-09-09	External	2014-09-09	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-09-09	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-09-09	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-09-09	Address inactivated. CC was unable to reach the client.	2014

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
2014-09-10	2014-09-10	External	2014-09-10	Client's Result Letter (Test Result)	2014-09-10	CC inactivated incorrect address	N/A	2014-09-10	Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Privacy Specialist	2014-09-10	Address inactivated. CC was unable to reach the client.	2014
2014-09-15	2014-09-15	Unclear	2014-09-15	N/A	2014-09-15	N/A - limited info about this breach. Provider faxed a form asking for client results, but it is unclear what PHI was breached and how.	N/A	2014-09-15	Contact Center	Policy breach	The PHI should not have been faxed to CCO. CC to advise sender.	N/A	Contact Center	2014-09-15	CC advised provider's office to contact the client's lab or their previous provider for these requests going forward.	2014
2014-09-15	2014-09-15	External	2014-09-15	Client's Result Letter (Test Result)	2014-09-15	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-09-15	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-09-15	Address inactivated. CC was unable to reach the client.	2014
2014-09-16	2014-09-16	External	2014-09-16	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-09-16	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-09-16	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-09-16	Address inactivated. CC was unable to reach the client.	2014
2014-09-16	2014-09-16	External	2014-09-16	Client's Result Letter (Test Result)	2014-09-16	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-09-16	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	YES	Contact Center & Privacy Specialist	2014-09-16	Address inactivated. CC was unable to reach the client.	2014
2014-09-16	2014-09-16	External	2014-09-16	Client's Result Letter (Test Result)	2014-09-16	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-09-16	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-09-16	Address inactivated. CC was unable to reach the client.	2014
2014-09-16	2014-09-16	External	2014-09-16	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-09-16	CC inactivated incorrect address	N/A	2014-09-16	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-09-16	Address inactivated. CC was unable to reach the client.	2014
2014-09-16	2014-09-16	External	2014-09-16	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-09-16	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-09-16	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-09-16	Address inactivated. CC was unable to reach the client.	2014
2014-09-17	2014-09-17	External	2014-09-17	Client's Invitation/Reminder Letter (Screening	2014-09-17	CC inactivated address + Unintended Recipient	N/A	2014-09-17	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact	NO	Contact Center & Privacy Specialist	2014-09-17	Address inactivated. CC was unable to	2014

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				Status/Eligibility)		asked to return letter					intended client.				reach the client.	
2014-09-17	2014-09-17	External	2014-09-17	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-09-17	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-09-17	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-09-17	Address inactivated. CC was unable to reach the client.	2014
2014-09-17	2014-09-17	External	2014-09-17	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-09-17	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-09-17	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-09-17	Address inactivated. CC was unable to reach the client.	2014
2014-09-18	2014-09-18	External	2014-09-18	N/A	2014-09-18	Provider faxed over 2 forms asking for client results. Forms contained identifying information about the client. Both faxes were deleted.	N/A	2014-09-18	Contact Center	Policy breach	The PHI should not have been faxed to CCO . CC to advise sender.	NO	Contact Center	2014-09-26	CC called the provider's office and left a voicemail indicating that requests for results should be sent to the client's screening site.	2014
2014-09-18	2014-09-18	External	2014-09-18	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-09-18	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-09-18	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-09-18	Address inactivated. CC was unable to reach the client.	2014
2014-09-19	2014-09-19	External	2014-09-19	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-09-19	CC inactivated incorrect address	N/A	2014-09-19	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-09-19	Address inactivated. CC was unable to reach the client.	2014
2014-09-19	2014-09-19	External	2014-09-19	Client's Result Letter (Test Result)	2014-09-19	Address inactivated - Letter will not be returned	N/A	2014-09-19	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-09-19	Address inactivated. CC was unable to reach the client.	2014
2014-09-22	2014-09-22	External	2014-09-22	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-09-22	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-09-22	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-09-22	Address inactivated. CC was unable to reach the client.	2014
2014-09-24	2014-09-24	External	2014-09-24	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-09-24	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-09-24	Contact Center & Privacy Specialist	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center & Privacy Specialist	2014-09-24	Address updated. CC was able to contact the client via number provided by their PCP.	2014

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
2014-09-24	2014-09-24	External	2014-09-24	Client's Result Letter (Test Result)	2014-09-24	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-09-24	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-09-24	Address inactivated. CC was unable to reach the client.	2014
2014-09-29	2014-09-29	External	2014-09-29	Client's Result Letter (Test Result)	2014-09-29	Address inactivated - Letter will not be returned	N/A	2014-09-29	Contact Center & Privacy Specialist	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center & Privacy Specialist	2014-09-29	CC called the client and updated the address.	2014
2014-09-29	2014-09-29	External	2014-09-29	N/A	2014-09-29	N/A - member of the public emailed PHI to CCO (breastscreen @cancercare. on.ca) and other contacts. Unclear whether the PHI was purged from CCO's email system.	N/A	2014-09-29	Contact Center	Privacy breach	N/A - no recommendations logged.	N/A	Contact Center	2014-09-29	N/A - no recommendations logged.	2014
2014-10-01	2014-10-01	External	2014-10-01	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-10-01	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-10-01	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-10-01	Address inactivated. CC was unable to reach the client.	2014
2014-10-01	2014-10-01	External	2014-10-01	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-10-01	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-10-01	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-10-01	Address inactivated. CC was unable to reach the client.	2014
2014-10-02	2014-10-02	External	2014-10-02	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-10-02	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-10-02	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-10-02	Address inactivated. CC was unable to reach the client.	2014
2014-10-03	2014-10-03	External	2014-10-03	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-10-03	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-10-03	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-10-03	Address inactivated. CC was unable to reach the client.	2014
2014-10-06	2014-10-06	External	2014-10-06	Client's Result Letter (Test Result)	2014-10-06	CC inactivated incorrect address	N/A	2014-10-06	Contact Center & Privacy Specialist	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center & Privacy Specialist	2014-10-06	CC called the client and updated the address.	2014
2014-10-07	2014-10-07	External	2014-10-07	Client's Result Letter (Test Result)	2014-10-07	CC inactivated address + Unintended Recipient	N/A	2014-10-07	Contact Center	Privacy breach	Contact Center to call client/PCP and	YES	Contact Center	2014-10-07	CC called the client and updated the address.	2014

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
						asked to return letter					update address.					
2014-10-07	2014-10-07	External	2014-10-07	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-10-07	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-10-07	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-10-07	Address inactivated. CC was unable to reach the client.	2014
2014-10-07	2014-10-07	External	2014-10-07	N/A	2014-10-07	None - Provider faxed a form to CCO asking for client results. Forms contained identifying information about the client.	N/A	2014-10-07	Contact Center	Policy breach	The PHI should not have been faxed to CCO. CC to advise sender.	NO	Contact Center	2014-10-07	CC advised provider's office to contact the client's lab for these requests going forward.	2014
2014-10-07	2014-10-07	External	2014-10-07	N/A	2014-10-07	Provider faxed high risk requisition forms to CCO's fax line. CC deleted PHI from mailbox.	N/A	2014-10-07	Contact Center	Policy breach	The PHI should not have been faxed to CCO. CC to advise sender.	NO	Contact Center	2014-10-08	CC advised provider's office to contact the OBSP site for these requests going forward.	2014
2014-10-08	2014-10-08	External	2014-10-08	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-10-08	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-10-08	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-10-08	Address inactivated. CC was unable to reach the client.	2014
2014-10-08	2014-10-08	External	2014-10-08	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-10-08	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-10-08	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-10-08	Address inactivated. CC was unable to reach the client.	2014
2014-10-09	2014-10-09	External	2014-10-09	Client's Result Letter (Test Result)	2014-10-09	CC inactivated incorrect address	N/A	2014-10-09	Contact Center & Privacy Specialist	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center & Privacy Specialist	2014-10-09	CC called the client and updated the address.	2014
2014-10-09	2014-10-09	External	2014-10-09	Client's Result Letter (Test Result)	2014-10-09	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-10-09	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-10-09	Address inactivated. CC was unable to reach the client.	2014
2014-10-14	2014-10-14	External	2014-10-14	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-10-14	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-10-14	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-10-14	Address inactivated. CC was unable to reach the client.	2014
2014-10-15	2014-10-15	External	2014-10-15	Client's Invitation/Remi	2014-10-15	CC inactivated the address +	N/A	2014-10-15	Contact Center &	Privacy breach	Address to be inactivated.	NO	Contact Center &	2014-10-15	Address inactivated.	2014

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				nder Letter (Screening Status/Eligibility)		Unintended Recipient to destroy letter			Privacy Specialist		CC to attempt to contact intended client.		Privacy Specialist		CC was unable to reach the client.	
2014-10-15	2014-10-15	Internal	2014-10-15	N/A	2014-10-15	N/A - the person at the client's former address emailed CCO Public Affairs to advise that CCO change the address of the client. Client had moved. Unclear how the breach occurred. Unclear what containment measures were taken by CC.	N/A	2014-10-15	Contact Center	Privacy breach	CC to inactivate the incorrect address on file for the client.	NO	Contact Center	2014-10-15	CC emailed the sender thanking them for their info. CC was able to authenticate and inactivate the address for the client. However, the client would have to contact Service Ontario directly to change their address.	2014
2014-10-16	2014-10-16	External	2014-10-16	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-10-16	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-10-16	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-10-16	Address inactivated. CC was unable to reach the client.	2014
2014-10-17	2014-10-17	External	2014-10-17	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-10-17	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-10-17	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-10-17	Address inactivated. CC was unable to reach the client.	2014
2014-10-20	2014-10-20	External	2014-10-20	Client's Result Letter (Test Result)	2014-10-20	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-10-20	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	YES	Contact Center	2014-10-20	Address inactivated. CC was unable to reach the client.	2014
2014-10-20	2014-10-20	External	2014-10-20	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-10-20	CC inactivated incorrect address	N/A	2014-10-20	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	YES	Contact Center & Privacy Specialist	2014-10-20	Address inactivated. CC was unable to reach the client.	2014
2014-10-20	2014-10-20	External	2014-10-20	Client's Result Letter (Test Result)	2014-10-20	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-10-20	Contact Center & Privacy Specialist	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center & Privacy Specialist	2014-10-20	CC called the client and updated the address.	2014
2014-10-20	2014-10-20	External	2014-10-20	Client's Invitation/Reminder Letter (Screening	2014-10-20	CC inactivated the address + Unintended	N/A	2014-10-20	Contact Center & Privacy Specialist	Privacy breach	Contact Center to call client/PCP and	NO	Contact Center & Privacy Specialist	2014-10-20	CC called the client and updated the address.	2014

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				Status/Eligibility)		Recipient to destroy letter					update address.					
2014-10-21	2014-10-21	External	2014-10-21	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-10-21	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-10-21	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-10-21	Address inactivated. CC was unable to reach the client.	2014
2014-10-21	2014-10-21	External	2014-10-21	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-10-21	CC inactivated incorrect address	N/A	2014-10-21	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-10-21	Address inactivated. CC was unable to reach the client.	2014
2014-10-23	2014-10-23	External	2014-10-23	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-10-23	Address inactivated - Letter will not be returned	N/A	2014-10-23	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-10-23	Address inactivated. CC was unable to reach the client.	2014
2014-10-23	2014-10-23	External	2014-10-23	Client's Result Letter (Test Result)	2014-10-23	CC inactivated incorrect address	N/A	2014-10-23	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-10-23	Address inactivated. CC was unable to reach the client.	2014
2014-10-27	2014-10-27	External	2014-10-27	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-10-27	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-10-27	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-10-27	Address inactivated. CC was unable to reach the client.	2014
2014-10-27	2014-10-27	External	2014-10-27	Client's Result Letter (Test Result)	2014-10-27	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-10-27	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-10-27	Address inactivated. CC was unable to reach the client.	2014
2014-10-29	2014-10-29	External	2014-10-29	Client's Result Letter (Test Result)	2014-10-29	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-10-29	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center	2014-10-29	CC called the client and updated the address.	2014
2014-10-29	2014-10-29	External	2014-10-29	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-10-29	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-10-29	Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Privacy Specialist	2014-10-29	Address inactivated. CC was unable to reach the client.	2014
2014-11-03	2014-11-03	External	2014-11-03	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-11-03	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-11-03	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	2014-11-03	Address updated. CC was able to contact the client via number provided by their PCP.	2014

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
2014-11-04	2014-11-04	External	2014-11-04	Client's Result Letter (Test Result)	2014-11-04	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-11-04	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-11-04	Address inactivated. CC was unable to reach the client.	2014
2014-11-04	2014-11-04	External	2014-11-04	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-11-04	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-11-04	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-11-04	Address inactivated. CC was unable to reach the client.	2014
2014-11-04	2014-11-04	External	2014-11-04	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-11-04	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-11-04	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-11-04	Address inactivated. CC was unable to reach the client.	2014
2014-11-04	2014-11-04	External	2014-11-04	N/A	2014-11-04	N/A - Provider faxed over a form asking for client results for 2 clients. Form contained identifying information about the clients. No containment measures indicated.	N/A	2014-11-04	Contact Center	Policy breach	CC could not find the provider's profile in InScreen, no follow-up possible.	N/A	Contact Center	2014-11-04	CC could not find the provider's profile in InScreen, no follow-up possible.	2014
2014-11-05	2014-11-05	External	2014-11-05	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-11-05	CC inactivated incorrect address	N/A	2014-11-05	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-11-05	Address inactivated. CC was unable to reach the client.	2014
2014-11-06	2014-11-06	External	2014-11-06	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-11-06	CC inactivated incorrect address	N/A	2014-11-06	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-11-06	Address inactivated. CC was unable to reach the client.	2014
2014-11-06	2014-11-06	External	2014-11-06	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-11-06	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-11-06	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-11-06	Address inactivated. CC was unable to reach the client.	2014
2014-11-06	2014-11-06	External	2014-11-06	N/A	2014-11-06	N/A - Provider faxed high risk requisition forms to CCO's fax line. Unclear what containment	N/A	2014-11-06	Contact Center	Policy breach	The PHI should not have been faxed to CCO. CC to advise sender.	NO	Contact Center	2014-11-12	CC advised provider's office to contact the OBSP site for these requests going forward.	2014

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
						measures were taken.										
2014-11-07	2014-11-07	External	2014-11-07	Client's Result Letter (Test Result)	2014-11-07	Address inactivated - Letter will not be returned	N/A	2014-11-07	Contact Center & Privacy Specialist	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center & Privacy Specialist	2014-11-07	CC called the client and updated the address.	2014
2014-11-07	2014-11-07	External	2014-11-07	Client's Result Letter (Test Result)	2014-11-07	CC inactivated incorrect address	N/A	2014-11-07	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	2014-11-07	CC called the client and updated the address.	2014
2014-11-10	2014-11-10	External	2014-11-10	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-11-10	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-11-10	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-11-10	Address inactivated. CC was unable to reach the client.	2014
2014-11-10	2014-11-10	External	2014-11-10	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-11-10	CC inactivated incorrect address	N/A	2014-11-10	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center	2014-11-10	CC called the client and updated the address.	2014
2014-11-13	2014-11-13	External	2014-11-13	Client's Result Letter (Test Result)	2014-11-13	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-11-13	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-11-13	Address inactivated. CC was unable to reach the client.	2014
2014-11-17	2014-11-17	External	2014-11-17	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-11-17	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-11-17	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-11-17	Address inactivated. CC was unable to reach the client.	2014

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
2014-11-17	2014-11-17	External	2014-11-17	Client's Result Letter (Test Result)	2014-11-17	CC inactivated incorrect address	N/A	2014-11-17	Privacy Specialist	Privacy breach	Contact Center to call client/PCP and update address.	YES	Privacy Specialist	2014-11-17	CC called the client and updated the address.	2014
2014-11-18	2014-11-18	External	2014-11-18	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-11-18	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-11-18	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-11-18	Address inactivated. CC was unable to reach the client.	2014
2014-11-18	2014-11-18	External	2014-11-18	Client's Result Letter (Test Result)	2014-11-18	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-11-18	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-11-18	Address inactivated. CC was unable to reach the client.	2014
2014-11-19	2014-11-19	External	2014-11-19	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-11-19	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-11-19	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-11-19	Address inactivated. CC was unable to reach the client.	2014
2014-11-19	2014-11-19	External	2014-11-19	Client's Result Letter (Test Result)	2014-11-19	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-11-19	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-11-19	Address inactivated. CC was unable to reach the client.	2014
2014-11-20	2014-11-20	External	2014-11-20	Client's Result Letter (Test Result)	2014-11-20	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-11-20	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center	2014-11-20	CC called the client and updated the address.	2014

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
2014-11-20	2014-11-20	External	2014-11-20	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-11-20	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-11-20	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-11-20	Address inactivated. CC was unable to reach the client.	2014
2014-11-20	2014-11-20	External	2014-11-20	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-11-20	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-11-20	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-11-20	Address inactivated. CC was unable to reach the client.	2014
2014-11-20	2014-11-20	External	2014-11-20	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-11-20	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-11-20	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-11-20	Address inactivated. CC was unable to reach the client.	2014
2014-11-24	2014-11-24	External	2014-11-24	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-11-24	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-11-24	Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Privacy Specialist	2014-11-24	Address inactivated. CC was unable to reach the client.	2014
2014-11-25	2014-11-25	External	2014-11-25	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-11-25	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-11-25	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-11-25	Address inactivated. CC was unable to reach the client.	2014
2014-11-25	2014-11-25	Internal	2014-11-25	N/A	2014-11-25	None - CC disclosed PHI over the phone without full authentication. No	N/A	2014-11-25	Contact Center	Privacy breach	N/A - no recommendations logged.	N/A	Contact Center	2014-11-25	N/A - no recommendations logged.	2014

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
						containment possible.										
2014-11-25	2014-11-25	External	2014-11-25	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-11-25	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-11-25	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-11-25	Address inactivated. CC was unable to reach the client.	2014
2014-11-27	2014-11-27	External	2014-11-27	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-11-27	CC inactivated incorrect address	N/A	2014-11-27	Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Privacy Specialist	2014-11-27	Address inactivated. CC was unable to reach the client.	2014
2014-11-27	2014-11-27	External	2014-11-27	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-11-27	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-11-27	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center	2014-11-27	CC called the client and updated the address.	2014
2014-11-27	2014-11-27	External	2014-11-27	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-11-27	CC inactivated incorrect address	N/A	2014-11-27	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center	2014-11-27	CC called the client and updated the address.	2014
2014-11-27	2014-11-27	External	2014-11-27	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-11-27	CC inactivated incorrect address	N/A	2014-11-27	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-11-27	Address inactivated. CC was unable to reach the client.	2014
2014-11-28	2014-11-28	External	2014-11-28	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-11-28	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-11-28	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-11-28	Address inactivated. CC was unable to reach the client.	2014
2014-12-01	2014-12-01	External	2014-12-01	Client's Result Letter (Test Result)	2014-12-01	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-12-01	Contact Center & Privacy Specialist	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center & Privacy Specialist	2014-12-01	CC called the client and updated the address.	2014
2014-12-01	2014-12-01	External	2014-12-01	Client's Result Letter (Test Result)	2014-12-01	CC inactivated incorrect address	N/A	2014-12-01	Contact Center & Privacy Specialist	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center & Privacy Specialist	2014-12-01	CC called the client and updated the address.	2014
2014-12-02	2014-12-02	External	2014-12-02	Client's Result Letter (Test Result)	2014-12-02	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-12-02	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-12-02	Address inactivated. CC was unable to reach the client.	2014
2014-12-02	2014-12-02	External	2014-12-02	Client's Invitation/Reminder Letter	2014-12-02	CC inactivated the address + Unintended	N/A	2014-12-02	Contact Center	Privacy breach	Address to be inactivated. CC to attempt	NO	Contact Center	2014-12-02	Address inactivated. CC was	2014

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				(Screening Status/Eligibility)		Recipient to destroy letter					to contact intended client.				unable to reach the client.	
2014-12-03	2014-12-03	External	2014-12-03	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-12-03	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-12-03	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	YES	Contact Center & Privacy Specialist	2014-12-03	Address inactivated. CC was unable to reach the client.	2014
2014-12-04	2014-12-04	External	2014-12-04	N/A	2014-12-04	N/A - lab mailed a letter with unauthorized PHI and info. Unclear if this was CCO's breach? Unclear what containment measures were taken.	N/A	2014-12-04	Contact Center	Privacy breach	N/A - no recommendations logged.	NO	Contact Center	2014-12-04	N/A - no recommendations logged. Manager, Lab Services followed up with the lab, but unclear what messaging was communicated.	2014
2014-12-09	2014-12-09	External	2014-12-09	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-12-09	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-12-09	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-12-09	Address inactivated. CC was unable to reach the client.	2014
2014-12-09	2014-12-09	External	2014-12-09	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-12-09	CC inactivated incorrect address	N/A	2014-12-09	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center	2014-12-09	CC called the client and updated the address.	2014
2014-12-10	2014-12-10	External	2014-12-10	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-12-10	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-12-10	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-12-10	Address inactivated. CC was unable to reach the client.	2014
2014-12-11	2014-12-11	External	2014-12-11	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-12-11	CC inactivated incorrect address	N/A	2014-12-11	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-12-11	Address inactivated. CC was unable to reach the client.	2014
2014-12-12	2014-12-12	External	2014-12-12	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-12-12	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-12-12	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-12-12	Address inactivated. CC was unable to reach the client.	2014
2014-12-12	2014-12-12	External	2014-12-12	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-12-12	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-12-12	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-12-12	Address inactivated. CC was unable to reach the client.	2014

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
2014-12-12	2014-12-12	External	2014-12-12	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-12-12	CC inactivated incorrect address	N/A	2014-12-12	Contact Center & Privacy Specialist	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center & Privacy Specialist	2014-12-12	CC called the client and updated the address.	2014
2014-12-12	2014-12-12	External	2014-12-12	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-12-12	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-12-12	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-12-12	Address inactivated. CC was unable to reach the client.	2014
2014-12-15	2014-12-15	External	2014-12-15	Client's Result Letter (Test Result)	2014-12-15	N/A - Ministry of Health forwarded PHI related to CCC to CCO's coloncancercheck@cancercare.on.ca email. Unclear what containment measures were taken.	N/A	2014-12-15	Contact Center	Privacy breach	N/A - no recommendations logged.	NO	Contact Center	2014-12-15	N/A - no recommendations logged.	2014
2014-12-15	2014-12-15	External	2014-12-15	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-12-15	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-12-15	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-12-15	Address inactivated. CC was unable to reach the client.	2014
2014-12-15	2014-12-15	External	2014-12-15	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-12-15	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-12-15	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-12-15	Address inactivated. CC was unable to reach the client.	2014
2014-12-15	2014-12-15	External	2014-12-15	Client's Result Letter (Test Result)	2014-12-15	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-12-15	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-12-15	Address inactivated. CC was unable to reach the client.	2014
2014-12-16	2014-12-16	External	2014-12-16	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-12-16	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-12-16	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-12-16	Address inactivated. CC was unable to reach the client.	2014
2014-12-16	2014-12-16	External	2014-12-16	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-12-16	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-12-16	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-12-16	Address inactivated. CC was unable to reach the client.	2014
2014-12-17	2014-12-17	External	2014-12-17	Client's Invitation/Reminder Letter (Screening	2014-12-17	Address inactivated - Letter will not be returned	N/A	2014-12-17	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact	NO	Contact Center	2014-12-17	Address inactivated. CC was unable to	2014

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				Status/Eligibility)							intended client.				reach the client.	
2014-12-17	2014-12-17	External	2014-12-17	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-12-17	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-12-17	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-12-17	Address inactivated. CC was unable to reach the client.	2014
2014-12-18	2014-12-19	External	2014-12-30	N/A	2014-12-19	Provider sent email (or emails?) containing PHI to datarequest@cancercare.on.ca inbox asking for a client's OBSP results. The emails were deleted from that inbox. There may also have been faxes - no containment possible for these.	N/A	2014-12-30	Contact Center	Policy breach	The PHI should not have been emailed or faxed to CCO. CC to advise sender.	NO	Contact Center	2015-01-15	CC advised provider's office to contact the OBSP site for these requests going forward.	2014
2014-12-18	2014-12-18	Internal	2014-12-18	N/A	2014-12-18	N/A - misdirected mail - unclear what containment measures were taken.	N/A	2014-12-18	Contact Center	Privacy breach	CC could not find the client (intended recipient)'s profile in InScreen, no follow-up possible.	N/A	Contact Center	2014-12-18	CC could not find the client (intended recipient)'s profile in InScreen, no follow-up possible.	2014
2014-12-19	2014-12-19	External	2014-12-19	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-12-19	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-12-19	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-12-19	Address inactivated. CC was unable to reach the client.	2014
2014-12-19	2014-12-19	External	2014-12-19	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-12-19	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-12-19	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-12-19	Address inactivated. CC was unable to reach the client.	2014
2014-12-19	2014-12-19	Internal	2014-12-19	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-12-19	N/A - CC contacted unintended recipient and they will send the letter back. Unclear if they actually did so.	N/A	2014-12-19	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center	2015-01-05	CC called the client and updated the address.	2014

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
2014-12-19	2014-12-19	External	2014-12-19	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-12-19	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-12-19	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-12-19	Address inactivated. CC was unable to reach the client.	2014
2014-12-22	2014-12-22	External	2014-12-22	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-12-22	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2014-12-22	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-12-22	Address inactivated. CC was unable to reach the client.	2014
2014-12-22	2014-12-22	External	2014-12-22	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-12-22	Address inactivated - Letter will not be returned	N/A	2014-12-22	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-12-22	Address inactivated. CC was unable to reach the client.	2014
2014-12-23	2014-12-23	External	2014-12-23	Client's Result Letter (Test Result)	2014-12-23	Address inactivated - Letter will not be returned	N/A	2014-12-23	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-12-23	Address inactivated. CC was unable to reach the client.	2014
2014-12-24	2014-12-24	External	2014-12-24	Client's Result Letter (Test Result)	2014-12-24	CC inactivated incorrect address	N/A	2014-12-24	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	2014-12-24	CC called the client and updated the address.	2014
2014-12-29	2014-12-29	External	2014-12-29	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2014-12-29	CC inactivated incorrect address	N/A	2014-12-29	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2014-12-29	Address inactivated. CC was unable to reach the client.	2014
2014-12-30	2014-12-30	External	2014-12-30	Client's Result Letter (Test Result)	2014-12-30	CC inactivated address + Unintended Recipient asked to return letter	N/A	2014-12-30	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2014-12-30	Address inactivated. CC was unable to reach the client.	2014
2015-01-02	2015-01-02	External	2015-01-02	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-01-02	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-01-02	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2015-01-02	Address inactivated. CC was unable to reach the client.	2015
2015-01-02	2015-01-02	External	2015-01-02	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-01-02	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-01-02	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2015-01-02	Address inactivated. CC was unable to reach the client.	2015
2015-01-07	2015-01-07	External	2015-01-07	Client's Invitation/Reminder Letter (Screening	2015-01-07	CC inactivated address + Unintended Recipient	N/A	2015-01-07	Contact Center & Privacy Specialist	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center & Privacy Specialist	2015-01-07	CC called the client and updated the address.	2015

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				Status/Eligibility)		asked to return letter										
2015-01-09	2015-01-09	External	2015-01-09	Client's Result Letter (Test Result)	2015-01-09	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-01-09	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-01-09	Address inactivated. CC was unable to reach the client.	2015
2015-01-09	2015-01-09	External	2015-01-09	Client's Result Letter (Test Result)	2015-01-09	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-01-09	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-01-09	Address inactivated. CC was unable to reach the client.	2015
2015-01-12	2015-01-12	External	2015-01-12	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-01-12	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-01-12	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-01-12	Address inactivated. CC was unable to reach the client.	2015
2015-01-12	2015-01-12	External	2015-01-12	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-01-12	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-01-12	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2015-01-12	Address inactivated. CC was unable to reach the client.	2015
2015-01-12	2015-01-12	External	2015-01-12	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-01-12	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-01-12	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-01-12	Address inactivated. CC was unable to reach the client.	2015
2015-01-13	2015-01-13	External	2015-01-13	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-01-13	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-01-13	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-01-13	Address inactivated. CC was unable to reach the client.	2015
2015-01-13	2015-01-13	External	2015-01-13	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-01-13	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-01-13	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2015-01-13	Address inactivated. CC was unable to reach the client.	2015
2015-01-13	2015-01-13	External	2015-01-13	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-01-13	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-01-13	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	2015-01-13	CC called the client and updated the address.	2015
2015-01-13	2015-01-13	External	2015-01-13	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-01-13	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-01-13	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-01-13	Address inactivated. CC was unable to reach the client.	2015

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
2015-01-14	2015-01-14	External	2015-01-14	Client's Result Letter (Test Result)	2015-01-14	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-01-14	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	YES	Contact Center	2015-01-14	Address inactivated. CC was unable to reach the client.	2015
2015-01-14	2015-01-14	External	2015-01-14	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-01-14	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-01-14	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-01-14	Address inactivated. CC was unable to reach the client.	2015
2015-01-14	2015-01-14	External	2015-01-14	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-01-14	CC inactivated incorrect address	N/A	2015-01-14	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-01-14	Address inactivated. CC was unable to reach the client.	2015
2015-01-14	2015-01-14	External	2015-01-14	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-01-14	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-01-14	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-01-14	Address inactivated. CC was unable to reach the client.	2015
2015-01-14	2015-01-14	External	2015-01-14	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-01-14	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-01-14	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-01-14	Address inactivated. CC was unable to reach the client.	2015
2015-01-15	2015-01-15	External	2015-01-15	Client's Result Letter (Test Result)	2015-01-15	CC inactivated incorrect address	N/A	2015-01-15	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	2015-01-15	CC called the client and updated the address.	2015
2015-01-15	2015-01-15	External	2015-01-15	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-01-15	CC inactivated incorrect address	N/A	2015-01-15	Contact Center & Privacy Specialist	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center & Privacy Specialist	2015-01-15	CC called the client and updated the address.	2015
2015-01-15	2015-01-15	External	2015-01-15	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-01-15	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-01-15	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-01-15	Address inactivated. CC was unable to reach the client.	2015
2015-01-15	2015-01-15	External	2015-01-15	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-01-15	CC inactivated incorrect address	N/A	2015-01-15	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	2015-01-15	CC called the client and updated the address.	2015
2015-01-15	2015-01-15	External	2015-01-15	Client's Invitation/Reminder Letter (Screening	2015-01-15	CC inactivated address + Unintended Recipient	N/A	2015-01-15	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact	NO	Contact Center	2015-01-15	Address inactivated. CC was unable to	2015

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				Status/Eligibility)		asked to return letter					intended client.				reach the client.	
2015-01-16	2015-01-16	External	2015-01-16	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-01-16	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-01-16	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2015-01-16	Address inactivated. CC was unable to reach the client.	2015
2015-01-16	2015-01-16	External	2015-01-16	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-01-16	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-01-16	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-01-16	Address inactivated. CC was unable to reach the client.	2015
2015-01-19	2015-01-19	External	2015-01-19	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-01-19	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-01-19	Contact Center & Privacy Specialist	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center & Privacy Specialist	2015-01-19	CC called the client and updated the address.	2015
2015-01-20	2015-01-20	External	2015-01-20	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-01-20	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-01-20	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-01-20	Address inactivated. CC was unable to reach the client.	2015
2015-01-21	2015-01-21	External	2015-01-21	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-01-21	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-01-21	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-01-21	Address inactivated. CC was unable to reach the client.	2015
2015-01-21	2015-01-21	External	2015-01-21	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-01-21	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-01-21	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-01-21	Address inactivated. CC was unable to reach the client.	2015
2015-01-21	2015-01-21	External	2015-01-21	Client's Result Letter (Test Result)	2015-01-21	CC inactivated incorrect address	N/A	2015-01-21	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-01-21	Address inactivated. CC was unable to reach the client.	2015
2015-01-21	2015-01-21	External	2015-01-21	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-01-21	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-01-21	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-01-21	Address inactivated. CC was unable to reach the client.	2015
2015-01-21	2015-01-21	External	2015-01-21	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-01-21	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-01-21	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-01-21	Address inactivated. CC was unable to reach the client.	2015

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
2015-01-22	2015-01-22	Internal	2015-01-22	Contact centre breach - phone. CSR released information to the wrong recipient (father not son); provided rationale for a CCC indeterminate result letter. • Client called about a CCC indeterminate result letter received in the mail • CSR looked up client's profile and no result was found • CSR overlooked DOB field as the first two search fields matched and pulled the record for the son instead of the caller (father) • CSR continued to investigate and released PHI to the caller regarding the rationale for the results ...CSR has asked the unintended recipient to mail the letter back and took down his phone number.	2015-01-22	• CSR has asked unintended recipient to mail breached letter back. CSR will follow-up if the letter is not returned. • CSR inactivated the address on the client's record.	1/22/2015 Notified external recipient.	2015-01-22	Privacy Specialist	Privacy breach	Privacy has instructed the Contact Centre staff to authenticate appropriately and ensure no PHI is disclosed to unintended recipients.	N/A	Contact Center & Privacy Specialist	2015-01-22	See "Recommendations".	2015
2015-01-22	2015-01-22	External	2015-01-22	Client's Invitation/Reminder Letter (Screening	2015-01-22	CC inactivated address + Unintended Recipient	N/A	2015-01-22	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact	NO	Contact Center & Privacy Specialist	2015-01-22	Address inactivated. CC was unable to	2015

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				Status/Eligibility)		asked to return letter					intended client.				reach the client.	
2015-01-22	2015-01-22	External	2015-01-22	Client's Result Letter (Test Result)	2015-01-22	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-01-22	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-01-22	Address inactivated. CC was unable to reach the client.	2015
2015-01-22	2015-01-22	External	2015-01-22	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-01-22	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-01-22	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-01-22	Address inactivated. CC was unable to reach the client.	2015
2015-01-23	2015-01-23	External	2015-01-23	Client's Result Letter (Test Result)	2015-01-23	CC inactivated incorrect address	N/A	2015-01-23	Contact Center & Privacy Specialist	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center & Privacy Specialist	2015-01-23	CC called the client and updated the address.	2015
2015-01-26	2015-01-26	External	2015-01-26	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-01-26	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-01-26	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-01-26	Address inactivated. CC was unable to reach the client.	2015
2015-01-26	2015-01-26	External	2015-01-26	Client's Result Letter (Test Result)	2015-01-26	CC inactivated incorrect address	N/A	2015-01-26	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center	2015-01-26	Address updated. CC was able to contact the client via number provided by their PCP.	2015
2015-01-27	2015-01-27	External	2015-01-27	Client's Result Letter (Test Result)	2015-01-27	Address inactivated - Letter will not be returned	N/A	2015-01-27	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center	2015-01-27	CC called the client and updated the address.	2015
2015-01-28	2015-01-28	Internal	2015-01-28	Contact centre breach - mail and phone. A client's mail went to an unintended recipient (actual PHI data elements unclear). Then, the CSR perpetuated the breach by informing the recipient that CCO got the address from a lab after the intended client performed a	2015-01-28	Notified privacy	N/A - internal	2015-01-30	Privacy Specialist	Privacy breach	Privacy Analyst reminded the CSR that PHI details must be not disclosed to unintended recipients.	N/A	Contact Center & Privacy Specialist	2015-01-30	See "Recommendations".	2015

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				test (actual PHI data elements unclear). [From submitter:] Unintended recipient called in to report that she was getting client's mail so client's address was inactivated. When attempting to contact the client, the unintended recipient who initially reported the breach was reached because the client's profile also contained the unintended recipient's phone number. She was upset that we were contacting her when she had already informed us of this error on our end. When she was asking where we got this information, I released PHI by informing her that we got the address from a lab after the client performed a test.												
2015-01-28	2015-01-28	External	2015-01-28	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-01-28	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-01-28	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-01-28	Address inactivated. CC was unable to reach the client.	2015

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
2015-01-28	2015-01-28	External	2015-01-28	Client's Result Letter (Test Result)	2015-01-28	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-01-28	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-01-28	Address inactivated. CC was unable to reach the client.	2015
2015-01-28	2015-01-28	External	2015-01-28	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-01-28	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-01-28	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-01-28	Address inactivated. CC was unable to reach the client.	2015
2015-01-30	2015-01-30	External	2015-01-30	Client's Result Letter (Test Result)	2015-01-30	Address inactivated - Letter will not be returned	N/A	2015-01-30	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center	2015-01-30	CC called the client and updated the address.	2015
2015-02-03	2015-02-03	External	2015-02-03	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-02-03	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-02-03	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-02-03	Address inactivated. CC was unable to reach the client.	2015
2015-02-03	2015-02-03	External	2015-02-03	Client's Result Letter (Test Result)	2015-02-03	CC inactivated incorrect address	N/A	2015-02-03	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-02-03	Address inactivated. CC was unable to reach the client.	2015
2015-02-03	2015-02-03	External	2015-02-03	Client's Result Letter (Test Result)	2015-02-03	CC inactivated incorrect address	N/A	2015-02-03	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-02-03	Address inactivated. CC was unable to reach the client.	2015
2015-02-04	2015-02-04	External	2015-02-04	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-02-04	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-02-04	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-02-04	Address inactivated. CC was unable to reach the client.	2015
2015-02-05	2015-02-05	External	2015-02-05	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-02-05	CC inactivated incorrect address	N/A	2015-02-05	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-02-05	Address inactivated. CC was unable to reach the client.	2015
2015-02-09	2015-02-09	External	2015-02-09	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-02-09	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-02-09	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-02-09	Address inactivated. CC was unable to reach the client.	2015
2015-02-09	2015-02-09	External	2015-02-09	Client's Result Letter (Test Result)	2015-02-09	CC inactivated address + Unintended Recipient	N/A	2015-02-09	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact	YES	Contact Center	2015-02-09	Address inactivated. CC was unable to	2015

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
						asked to return letter					intended client.				reach the client.	
2015-02-10	2015-02-10	External	2015-02-10	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-02-10	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-02-10	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-02-10	Address inactivated. CC was unable to reach the client.	2015
2015-02-11	2015-02-11	External	2015-02-11	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-02-11	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-02-11	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-02-11	Address inactivated. CC was unable to reach the client.	2015
2015-02-11	2015-02-11	External	2015-02-11	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-02-11	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-02-11	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-02-11	Address inactivated. CC was unable to reach the client.	2015
2015-02-11	2015-02-11	External	2015-02-11	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-02-11	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-02-11	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-02-11	Address inactivated. CC was unable to reach the client.	2015
2015-02-13	2015-02-13	External	2015-02-13	Client's Result Letter (Test Result)	2015-02-13	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-02-13	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	2015-02-13	CC called the client and updated the address.	2015
2015-02-17	2015-02-17	External	2015-02-17	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-02-17	Address inactivated - Letter will not be returned	N/A	2015-02-17	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-02-17	Address inactivated. CC was unable to reach the client.	2015
2015-02-18	2015-02-18	External	2015-02-18	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-02-18	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-02-18	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-02-18	Address inactivated. CC was unable to reach the client.	2015
2015-02-18	2015-02-18	External	2015-02-18	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-02-18	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-02-18	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-02-18	Address inactivated. CC was unable to reach the client.	2015
2015-02-19	2015-02-19	External	2015-02-19	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-02-19	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-02-19	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-02-19	Address inactivated. CC was unable to reach the client.	2015
2015-02-23	2015-02-23	External	2015-02-23	Client's Invitation/Remi	2015-02-23	CC inactivated address +	N/A	2015-02-23	Contact Center	Privacy breach	Address to be inactivated.	NO	Contact Center	2015-02-23	Address inactivated.	2015

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				nder Letter (Screening Status/Eligibility)		Unintended Recipient asked to return letter					CC to attempt to contact intended client.				CC was unable to reach the client.	
2015-02-23	2015-02-23	External	2015-02-23	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-02-23	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-02-23	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	2015-02-23	CC called the client and updated the address.	2015
2015-02-24	2015-02-24	External	2015-02-24	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-02-24	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-02-24	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-02-24	Address inactivated. CC was unable to reach the client.	2015
2015-02-24	2015-02-24	External	2015-02-24	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-02-24	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-02-24	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-02-24	Address inactivated. CC was unable to reach the client.	2015
2015-02-24	2015-02-24	External	2015-02-24	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-02-24	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-02-24	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-02-24	Address inactivated. CC was unable to reach the client.	2015
2015-02-25	2015-02-25	External	2015-02-25	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-02-25	CC inactivated incorrect address	N/A	2015-02-25	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-02-25	Address inactivated. CC was unable to reach the client.	2015
2015-02-25	2015-02-25	External	2015-02-25	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-02-25	CC inactivated incorrect address	N/A	2015-02-25	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-02-25	Address inactivated. CC was unable to reach the client.	2015
2015-02-27	2015-02-27	External	2015-02-27	Client's Result Letter (Test Result)	2015-02-27	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-02-27	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center	2015-02-27	CC called the client and updated the address.	2015
2015-03-02	2015-03-02	External	2015-03-02	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-03-02	Address inactivated - Letter will not be returned	N/A	2015-03-02	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-03-02	Address inactivated. CC was unable to reach the client.	2015
2015-03-03	2015-03-03	External	2015-03-03	Client's Result Letter (Test Result)	2015-03-03	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-03-03	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-03-03	Address inactivated. CC was unable to reach the client.	2015

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
2015-03-05	2015-03-05	External	2015-03-05	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-03-05	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-03-05	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-03-05	Address inactivated. CC was unable to reach the client.	2015
2015-03-09	2015-03-09	External	2015-03-09	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-03-09	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-03-09	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-03-09	Address inactivated. CC was unable to reach the client.	2015
2015-03-09	2015-03-09	External	2015-03-09	Client's Result Letter (Test Result)	2015-03-09	CC inactivated incorrect address	N/A	2015-03-09	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-03-09	Address inactivated. CC was unable to reach the client.	2015
2015-03-09	2015-03-09	External	2015-03-09	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-03-09	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-03-09	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-03-09	Address inactivated. CC was unable to reach the client.	2015
2015-03-09	2015-03-09	External	2015-03-09	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-03-09	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-03-09	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	YES	Contact Center	2015-03-09	Address inactivated. CC was unable to reach the client.	2015
2015-03-10	2015-03-10	External	2015-03-10	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-03-10	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-03-10	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-03-10	Address inactivated. CC was unable to reach the client.	2015
2015-03-10	2015-03-10	External	2015-03-10	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-03-10	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-03-10	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center	2015-03-10	Address updated. CC was able to contact the client via number provided by their PCP.	2015
2015-03-10	2015-03-10	External	2015-03-10	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-03-10	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-03-10	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-03-10	Address inactivated. CC was unable to reach the client.	2015
2015-03-10	2015-03-10	External	2015-03-10	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-03-10	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-03-10	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-03-10	Address inactivated. CC was unable to reach the client.	2015
2015-03-11	2015-03-11	Unclear	2015-03-12	Client's Invitation/Remi	2015-03-12	N/A - CC withdrew client	N/A	2015-03-12	Contact Center	Privacy breach	CC to contact the client and	NO	Contact Center	2015-03-12	CC left a voice message	2015

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				nder Letter (Screening Status/Eligibility)		without fully authenticating. PHI was disclosed during the call.					ask them to fully authenticate their identity.				asking client to fully authenticate. Client called back and fully authenticated. Confirmation of withdrawal sent afterwards.	
2015-03-11	2015-03-11	External	2015-03-11	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-03-11	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-03-11	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-03-11	Address inactivated. CC was unable to reach the client.	2015
2015-03-11	2015-03-11	External	2015-03-11	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-03-11	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-03-11	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-03-11	Address inactivated. CC was unable to reach the client.	2015
2015-03-11	2015-03-11	External	2015-03-11	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-03-11	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-03-11	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-03-11	Address inactivated. CC was unable to reach the client.	2015
2015-03-12	2015-03-12	External	2015-03-12	Client's Result Letter (Test Result)	2015-03-12	CC inactivated incorrect address	N/A	2015-03-12	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center	2015-03-12	CC called the client and updated the address.	2015
2015-03-12	2015-03-12	External	2015-03-12	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-03-12	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-03-12	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-03-12	Address inactivated. CC was unable to reach the client.	2015
2015-03-12	2015-03-12	External	2015-03-12	Client's Result Letter (Test Result)	2015-03-12	CC inactivated incorrect address	N/A	2015-03-12	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-03-12	Address inactivated. CC was unable to reach the client.	2015
2015-03-16	2015-03-16	External	2015-03-16	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-03-16	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-03-16	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-03-16	Address inactivated. CC was unable to reach the client.	2015
2015-03-16	2015-03-16	External	2015-03-16	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-03-16	CC inactivated incorrect address	N/A	2015-03-16	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-03-16	Address inactivated. CC was unable to reach the client.	2015

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
2015-03-16	2015-03-16	External	2015-03-16	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-03-16	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-03-16	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-03-16	Address inactivated. CC was unable to reach the client.	2015
2015-03-18	2015-03-18	External	2015-03-18	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-03-18	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-03-18	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-03-18	Address inactivated. CC was unable to reach the client.	2015
2015-03-19	2015-03-19	External	2015-03-19	Client's Result Letter (Test Result)	2015-03-19	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-03-19	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-03-19	Address inactivated. CC was unable to reach the client.	2015
2015-03-20	2015-03-20	External	2015-03-20	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-03-20	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-03-20	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-03-20	Address inactivated. CC was unable to reach the client.	2015
2015-03-20	2015-03-20	External	2015-03-20	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-03-20	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-03-20	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	2015-03-20	CC called the client and updated the address.	2015
2015-03-23	2015-03-23	External	2015-03-23	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-03-23	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-03-23	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-03-23	Address inactivated. CC was unable to reach the client.	2015
2015-03-23	2015-03-23	External	2015-03-23	Client's Result Letter (Test Result)	2015-03-23	CC inactivated incorrect address	N/A	2015-03-23	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-03-23	Address inactivated. CC was unable to reach the client.	2015
2015-03-23	2015-03-23	External	2015-03-23	N/A	2015-03-23	Provider faxed high risk requisition forms to CCO's fax line. CC deleted the fax containing the PHI.	N/A	2015-03-23	Contact Center	Policy breach	N/A	NO	Contact Center	2015-03-23	CC advised sender (referral team at provider's office) to fax the requisition directly to one of the OBSP High Risk referral contacts.	2015
2015-03-24	2015-03-24	External	2015-03-24	Client's Invitation/Reminder Letter (Screening	2015-03-24	CC inactivated address + Unintended Recipient	N/A	2015-03-24	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact	NO	Contact Center	2015-03-24	Address inactivated. CC was unable to	2015

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				Status/Eligibility)		asked to return letter					intended client.				reach the client.	
2015-03-25	2015-03-25	External	2015-03-25	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-03-25	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-03-25	Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-03-25	Address inactivated. CC was unable to reach the client.	2015
2015-03-25	2015-03-25	External	2015-03-25	Client's Result Letter (Test Result)	2015-03-25	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-03-25	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center	2015-03-25	CC called the client and updated the address.	2015
2015-03-25	2015-03-25	External	2015-03-25	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-03-25	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-03-25	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-03-25	Address inactivated. CC was unable to reach the client.	2015
2015-03-25	2015-03-25	External	2015-03-25	Client's Result Letter (Test Result)	2015-03-25	Address inactivated - Letter will not be returned	N/A	2015-03-25	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	2015-03-25	CC called the client and updated the address.	2015
2015-03-25	2015-03-25	External	2015-03-25	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-03-25	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-03-25	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-03-25	Address inactivated. CC was unable to reach the client.	2015
2015-03-26	2015-03-26	Internal	2015-03-26	N/A	2015-03-26	N/A - National Change of Address database error- unclear whether the unintended recipient returned and/or destroyed the letter. Provided Canada Post phone number to the intended recipient. Address inactivated then updated.	N/A	2015-03-26	Contact Center	Privacy breach	N/A - no recommendations logged.	NO	Contact Center	2015-03-26	N/A - no recommendations logged.	2015
2015-03-26	2015-03-26	External	2015-03-26	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-03-26	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-03-26	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-03-26	Address inactivated. CC was unable to reach the client.	2015

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
2015-03-27	2015-03-27	External	2015-03-27	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-03-27	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-03-27	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2015-03-27	Address inactivated. CC was unable to reach the client.	2015
2015-03-30	2015-03-30	External	2015-03-30	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-03-30	CC inactivated incorrect address	N/A	2015-03-30	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-03-30	Address inactivated. CC was unable to reach the client.	2015
2015-03-30	2015-03-30	External	2015-03-30	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-03-30	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-03-30	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	YES	Contact Center & Privacy Specialist	2015-03-30	Address inactivated. CC was unable to reach the client.	2015
2015-03-30	2015-03-30	External	2015-03-30	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-03-30	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-03-30	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2015-03-30	Address inactivated. CC was unable to reach the client.	2015
2015-03-30	2015-03-30	External	2015-03-30	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-03-30	CC inactivated incorrect address	N/A	2015-03-30	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2015-03-30	Address inactivated. CC was unable to reach the client.	2015
2015-03-30	2015-03-30	External	2015-03-30	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-03-30	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-03-30	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-03-30	Address inactivated. CC was unable to reach the client.	2015
2015-03-30	2015-03-30	External	2015-03-30	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-03-30	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-03-30	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-03-30	Address inactivated. CC was unable to reach the client.	2015
2015-03-31	2015-03-31	External	2015-03-31	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-03-31	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-03-31	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2015-03-31	Address inactivated. CC was unable to reach the client.	2015
2015-03-31	2015-03-31	External	2015-03-31	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-03-31	CC inactivated incorrect address	N/A	2015-03-31	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-03-31	Address inactivated. CC was unable to reach the client.	2015
2015-04-01	2015-04-01	External	2015-04-01	Client's Invitation/Reminder Letter (Screening	2015-04-01	CC inactivated the address + Unintended	N/A	2015-04-01	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact	NO	Contact Center	2015-04-01	Address inactivated. CC was unable to	2015

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				Status/Eligibility)		Recipient to destroy letter					intended client.				reach the client.	
2015-04-02	2015-04-02	External	2015-04-02	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-04-02	CC inactivated incorrect address	N/A	2015-04-02	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-04-02	Address inactivated. CC was unable to reach the client.	2015
2015-04-09	2015-04-09	External	2015-04-09	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-04-09	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-04-09	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2015-04-09	Address inactivated. CC was unable to reach the client.	2015
2015-04-10	2015-04-10	External	2015-04-10	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-04-10	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-04-10	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-04-10	Address inactivated. CC was unable to reach the client.	2015
2015-04-10	2015-04-10	External	2015-04-10	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-04-10	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-04-10	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2015-04-10	Address inactivated. CC was unable to reach the client.	2015
2015-04-13	2015-04-13	External	2015-04-13	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-04-13	Address inactivated - Letter will not be returned	N/A	2015-04-13	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-04-13	Address inactivated. CC was unable to reach the client.	2015
2015-04-13	2015-04-13	External	2015-04-13	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-04-13	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-04-13	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-04-13	Address inactivated. CC was unable to reach the client.	2015
2015-04-14	2015-04-14	External	2015-04-14	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-04-14	Address inactivated - Letter will not be returned	N/A	2015-04-14	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-04-14	Address inactivated. CC was unable to reach the client.	2015
2015-04-14	2015-04-14	External	2015-04-14	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-04-14	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-04-14	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-04-14	Address inactivated. CC was unable to reach the client.	2015
2015-04-14	2015-04-14	External	2015-04-14	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-04-14	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-04-14	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-04-14	Address inactivated. CC was unable to reach the client.	2015
2015-04-14	2015-04-14	External	2015-04-14	Client's Invitation/Remi	2015-04-14	CC inactivated address +	N/A	2015-04-14	Contact Center	Privacy breach	Address to be inactivated.	NO	Contact Center	2015-04-14	Address inactivated.	2015

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				nder Letter (Screening Status/Eligibility)		Unintended Recipient asked to return letter					CC to attempt to contact intended client.				CC was unable to reach the client.	
2015-04-14	2015-04-14	External	2015-04-14	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-04-14	CC inactivated incorrect address	N/A	2015-04-14	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-04-14	Address inactivated. CC was unable to reach the client.	2015
2015-04-14	2015-04-14	External	2015-04-14	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-04-14	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-04-14	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-04-14	Address inactivated. CC was unable to reach the client.	2015
2015-04-14	2015-04-14	External	2015-04-14	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-04-14	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-04-14	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-04-14	Address inactivated. CC was unable to reach the client.	2015
2015-04-15	2015-04-15	External	2015-04-15	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-04-15	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-04-15	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-04-15	Address inactivated. CC was unable to reach the client.	2015
2015-04-15	2015-04-15	External	2015-04-15	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-04-15	CC inactivated incorrect address	N/A	2015-04-15	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-04-15	Address inactivated. CC was unable to reach the client.	2015
2015-04-15	2015-04-15	External	2015-04-15	Client's Result Letter (Test Result)	2015-04-15	CC inactivated incorrect address	N/A	2015-04-15	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-04-15	Address inactivated. CC was unable to reach the client.	2015
2015-04-15	2015-04-15	External	2015-04-15	Client's Result Letter (Test Result)	2015-04-15	CC inactivated incorrect address	N/A	2015-04-15	Contact Center & Privacy Specialist	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center & Privacy Specialist	2015-04-15	CC called the client and updated the address.	2015
2015-04-15	2015-04-15	External	2015-04-15	Client's Result Letter (Test Result)	2015-04-15	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-04-15	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2015-04-15	Address inactivated. CC was unable to reach the client.	2015
2015-04-16	2015-04-16	External	2015-04-16	Client's Result Letter (Test Result)	2015-04-16	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-04-16	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-04-16	Address inactivated. CC was unable to reach the client.	2015

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
2015-04-17	2015-04-17	External	2015-04-17	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-04-17	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-04-17	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-04-17	Address inactivated. CC was unable to reach the client.	2015
2015-04-17	2015-04-17	External	2015-04-17	Client's Result Letter (Test Result)	2015-04-17	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-04-17	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2015-04-17	Address inactivated. CC was unable to reach the client.	2015
2015-04-17	2015-04-17	External	2015-04-17	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-04-17	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-04-17	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2015-04-17	Address inactivated. CC was unable to reach the client.	2015
2015-04-20	2015-04-20	External	2015-04-20	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-04-20	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-04-20	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-04-20	Address inactivated. CC was unable to reach the client.	2015
2015-04-20	2015-04-20	External	2015-04-20	Client's Result Letter (Test Result)	2015-04-20	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-04-20	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center	2015-04-20	CC called the client and updated the address.	2015
2015-04-20	2015-04-20	External	2015-04-20	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-04-20	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-04-20	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-04-20	Address inactivated. CC was unable to reach the client.	2015
2015-04-20	2015-04-20	External	2015-04-20	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-04-20	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-04-20	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-04-20	Address inactivated. CC was unable to reach the client.	2015
2015-04-21	2015-04-21	External	2015-04-21	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-04-21	Relative/Spouse opened the letter - address change not required	N/A	2015-04-21	Contact Center	Privacy breach	None Required	NO	Contact Center	2015-04-21	None Required	2015
2015-04-21	2015-04-21	External	2015-04-21	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-04-21	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-04-21	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2015-04-21	Address inactivated. CC was unable to reach the client.	2015
2015-04-21	2015-04-21	External	2015-04-21	Client's Invitation/Reminder Letter (Screening	2015-04-21	CC inactivated address + Unintended Recipient	N/A	2015-04-21	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact	NO	Contact Center	2015-04-21	Address inactivated. CC was unable to	2015

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				Status/Eligibility)		asked to return letter					intended client.				reach the client.	
2015-04-23	2015-04-23	External	2015-04-23	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-04-23	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-04-23	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-04-23	Address inactivated. CC was unable to reach the client.	2015
2015-04-23	2015-04-23	External	2015-04-23	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-04-23	CC inactivated incorrect address	N/A	2015-04-23	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-04-23	Address inactivated. CC was unable to reach the client.	2015
2015-04-27	2015-04-27	External	2015-04-27	Client's Result Letter (Test Result)	2015-04-27	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-04-27	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center	2015-04-27	CC called the client and updated the address.	2015
2015-04-27	2015-04-27	External	2015-04-27	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-04-27	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-04-27	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2015-04-27	Address inactivated. CC was unable to reach the client.	2015
2015-04-27	2015-04-27	External	2015-04-27	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-04-27	CC inactivated incorrect address	N/A	2015-04-27	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-04-27	Address inactivated. CC was unable to reach the client.	2015
2015-04-28	2015-04-28	External	2015-04-28	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-04-28	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-04-28	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-04-28	Address inactivated. CC was unable to reach the client.	2015
2015-04-29	2015-04-29	External	2015-04-29	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-04-29	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-04-29	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-04-29	Address inactivated. CC was unable to reach the client.	2015
2015-05-04	2015-05-04	External	2015-05-04	Client's Result Letter (Test Result)	2015-05-04	CC inactivated incorrect address	N/A	2015-05-04	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-05-04	Address inactivated. CC was unable to reach the client.	2015
2015-05-05	2015-05-05	External	2015-05-05	Client's Result Letter (Test Result)	2015-05-05	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-05-05	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	2015-05-05	CC called the client and updated the address.	2015
2015-05-05	2015-05-05	External	2015-05-05	Client's Invitation/Reminder Letter	2015-05-05	CC inactivated incorrect address	N/A	2015-05-05	Contact Center	Privacy breach	Address to be inactivated. CC to attempt	NO	Contact Center	2015-05-05	Address inactivated. CC was	2015

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				(Screening Status/Eligibility)							to contact intended client.				unable to reach the client.	
2015-05-05	2015-05-05	External	2015-05-05	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-05-05	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-05-05	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-05-05	Address inactivated. CC was unable to reach the client.	2015
2015-05-06	2015-05-06	External	2015-05-06	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-05-06	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-05-06	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-05-06	Address inactivated. CC was unable to reach the client.	2015
2015-05-06	2015-05-06	External	2015-05-06	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-05-06	CC inactivated incorrect address	N/A	2015-05-06	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-05-06	Address inactivated. CC was unable to reach the client.	2015
2015-05-11	2015-05-11	External	2015-05-11	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-05-11	CC inactivated incorrect address	N/A	2015-05-11	Contact Center & Privacy Specialist	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center & Privacy Specialist	2015-05-11	Address inactivated. CC was unable to reach the client.	2015
2015-05-15	2015-05-15	External	2015-05-15	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-05-15	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-05-15	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-05-15	Address inactivated. CC was unable to reach the client.	2015
2015-05-15	2015-05-15	External	2015-05-15	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-05-15	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-05-15	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-05-15	Address inactivated. CC was unable to reach the client.	2015
2015-05-19	2015-05-19	External	2015-05-19	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-05-19	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-05-19	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-05-19	Address inactivated. CC was unable to reach the client.	2015
2015-05-19	2015-05-19	External	2015-05-19	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-05-19	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-05-19	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-05-19	Address inactivated. CC was unable to reach the client.	2015
2015-05-19	2015-05-19	External	2015-05-19	Client's Result Letter (Test Result)	2015-05-19	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-05-19	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-05-19	Address inactivated. CC was unable to reach the client.	2015

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
2015-05-19	2015-05-19	External	2015-05-19	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-05-19	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-05-19	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-05-19	Address inactivated. CC was unable to reach the client.	2015
2015-05-20	2015-05-20	External	2015-05-20	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-05-20	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-05-20	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-05-20	Address inactivated. CC was unable to reach the client.	2015
2015-05-20	2015-05-20	External	2015-05-20	Client's Result Letter (Test Result)	2015-05-20	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-05-20	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-05-20	Address inactivated. CC was unable to reach the client.	2015
2015-05-21	2015-05-21	External	2015-05-21	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-05-21	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-05-21	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-05-21	Address inactivated. CC was unable to reach the client.	2015
2015-05-21	2015-05-21	External	2015-05-21	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-05-21	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-05-21	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-05-21	Address inactivated. CC was unable to reach the client.	2015
2015-05-21	2015-05-21	External	2015-05-21	Client's Result Letter (Test Result)	2015-05-21	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-05-21	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	2015-05-21	CC called the client and updated the address.	2015
2015-05-21	2015-05-21	External	2015-05-21	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-05-21	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-05-21	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-05-21	Address inactivated. CC was unable to reach the client.	2015
2015-05-25	2015-05-25	External	2015-05-25	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-05-25	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-05-25	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-05-25	Address inactivated. CC was unable to reach the client.	2015
2015-05-25	2015-05-25	External	2015-05-25	Client's Result Letter (Test Result)	2015-05-25	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-05-25	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center	2015-05-25	CC called the client and updated the address.	2015
2015-05-25	2015-05-25	External	2015-05-25	Client's Result Letter (Test Result)	2015-05-25	CC inactivated address + Unintended Recipient	N/A	2015-05-25	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact	NO	Contact Center	2015-05-25	Address inactivated. CC was unable to	2015

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
						asked to return letter					intended client.				reach the client.	
2015-05-25	2015-05-25	External	2015-05-25	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-05-25	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-05-25	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-05-25	Address inactivated. CC was unable to reach the client.	2015
2015-05-25	2015-05-25	External	2015-05-25	Client's Result Letter (Test Result)	2015-05-25	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-05-25	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center	2015-05-25	CC called the client and updated the address.	2015
2015-05-26	2015-05-26	External	2015-05-26	Client's Result Letter (Test Result)	2015-05-26	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-05-26	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center	2015-05-26	CC called the client and updated the address.	2015
2015-05-26	2015-05-26	External	2015-05-26	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-05-26	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-05-26	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-05-26	Address inactivated. CC was unable to reach the client.	2015
2015-05-26	2015-05-26	External	2015-05-26	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-05-26	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-05-26	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-05-26	Address inactivated. CC was unable to reach the client.	2015
2015-05-26	2015-05-26	External	2015-05-26	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-05-26	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-05-26	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-05-26	Address inactivated. CC was unable to reach the client.	2015
2015-05-26	2015-05-26	External	2015-05-26	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-05-26	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-05-26	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-05-26	Address inactivated. CC was unable to reach the client.	2015
2015-05-27	2015-05-27	External	2015-05-27	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-05-27	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-05-27	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-05-27	Address inactivated. CC was unable to reach the client.	2015
2015-05-27	2015-05-27	External	2015-05-27	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-05-27	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-05-27	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-05-27	Address inactivated. CC was unable to reach the client.	2015
2015-05-27	2015-05-27	External	2015-05-27	Client's Result Letter (Test Result)	2015-05-27	CC inactivated the address + Unintended	N/A	2015-05-27	Contact Center	Privacy breach	Address to be inactivated. CC to attempt	NO	Contact Center	2015-05-27	Address inactivated. CC was	2015

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
						Recipient to destroy letter					to contact intended client.				unable to reach the client.	
2015-05-29	2015-05-29	External	2015-05-29	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-05-29	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-05-29	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-05-29	Address inactivated. CC was unable to reach the client.	2015
2015-06-01	2015-06-01	External	2015-06-01	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-06-01	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-06-01	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-06-01	Address inactivated. CC was unable to reach the client.	2015
2015-06-02	2015-06-02	External	2015-06-02	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-06-02	None - Provider faxed request for results containing PHI to CCO's fax line - no containment possible.	N/A	2015-06-02	Contact Center	Policy breach	N/A	N/A	Contact Center	2015-06-02	CC advised provider's office to contact the OBSP site for these requests going forward.	2015
2015-06-02	2015-06-02	External	2015-06-02	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-06-02	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-06-02	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	2015-06-02	CC called the client and updated the address.	2015
2015-06-02	2015-06-02	External	2015-06-02	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-06-02	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-06-02	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-06-02	Address inactivated. CC was unable to reach the client.	2015
2015-06-02	2015-06-02	External	2015-06-02	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-06-02	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-06-02	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center	2015-06-02	CC called the client and updated the address.	2015
2015-06-02	2015-06-02	External	2015-06-02	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-06-02	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-06-02	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-06-02	Address inactivated. CC was unable to reach the client.	2015
2015-06-03	2015-06-03	External	2015-06-03	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-06-03	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-06-03	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-06-03	Address inactivated. CC was unable to reach the client.	2015
2015-06-03	2015-06-03	External	2015-06-03	Client's Invitation/Reminder Letter (Screening	2015-06-03	CC inactivated address + Unintended Recipient	N/A	2015-06-03	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact	NO	Contact Center	2015-06-03	Address inactivated. CC was unable to	2015

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				Status/Eligibility)		asked to return letter					intended client.				reach the client.	
2015-06-04	2015-06-04	External	2015-06-04	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-06-04	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-06-04	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-06-04	Address inactivated. CC was unable to reach the client.	2015
2015-06-04	2015-06-04	External	2015-06-04	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-06-04	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-06-04	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-06-04	Address inactivated. CC was unable to reach the client.	2015
2015-06-05	2015-06-05	External	2015-06-05	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-06-05	Address inactivated - Letter will not be returned	N/A	2015-06-05	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-06-05	Address inactivated. CC was unable to reach the client.	2015
2015-06-08	2015-06-08	External	2015-06-08	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-06-08	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-06-08	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-06-08	Address inactivated. CC was unable to reach the client.	2015
2015-06-09	2015-06-09	External	2015-06-09	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-06-09	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-06-09	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-06-09	Address inactivated. CC was unable to reach the client.	2015
2015-06-09	2015-06-09	External	2015-06-09	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-06-09	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-06-09	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-06-09	Address inactivated. CC was unable to reach the client.	2015
2015-06-09	2015-06-09	External	2015-06-09	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-06-09	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-06-09	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-06-09	Address inactivated. CC was unable to reach the client.	2015
2015-06-11	2015-06-11	External	2015-06-11	Client's Result Letter (Test Result)	2015-06-11	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-06-11	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-06-11	Address inactivated. CC was unable to reach the client.	2015
2015-06-11	2015-06-11	External	2015-06-11	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-06-11	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-06-11	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-06-11	Address inactivated. CC was unable to reach the client.	2015
2015-06-11	2015-06-11	External	2015-06-11	Client's Invitation/Remi	2015-06-11	CC inactivated address +	N/A	2015-06-11	Contact Center	Privacy breach	Address to be inactivated.	NO	Contact Center	2015-06-11	Address inactivated.	2015

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				nder Letter (Screening Status/Eligibility)		Unintended Recipient asked to return letter					CC to attempt to contact intended client.				CC was unable to reach the client.	
2015-06-11	2015-06-11	External	2015-06-11	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-06-11	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-06-11	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-06-11	Address inactivated. CC was unable to reach the client.	2015
2015-06-11	2015-06-11	External	2015-06-11	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-06-11	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-06-11	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-06-11	Address inactivated. CC was unable to reach the client.	2015
2015-06-12	2015-06-12	External	2015-06-12	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-06-12	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-06-12	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-06-12	Address inactivated. CC was unable to reach the client.	2015
2015-06-16	2015-06-16	External	2015-06-16	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-06-16	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-06-16	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-06-16	Address inactivated. CC was unable to reach the client.	2015
2015-06-17	2015-06-17	External	2015-06-17	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-06-17	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-06-17	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-06-17	Address inactivated. CC was unable to reach the client.	2015
2015-06-17	2015-06-17	External	2015-06-17	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-06-17	Address inactivated - Letter will not be returned	N/A	2015-06-17	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-06-17	Address inactivated. CC was unable to reach the client.	2015
2015-06-17	2015-06-17	Unclear	2015-06-17	Cannot be determined	2015-06-17	N/A - Unclear why this was classified as a breach.	N/A	2015-06-17	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	N/A	Contact Center	2015-06-17	None Required/Possible (anonymous)	2015
2015-06-18	2015-06-18	External	2015-06-18	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-06-18	Address inactivated - Letter will not be returned	N/A	2015-06-18	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-06-18	Address inactivated. CC was unable to reach the client.	2015
2015-06-18	2015-06-18	External	2015-06-18	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-06-18	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-06-18	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-06-18	Address inactivated. CC was unable to reach the client.	2015

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
2015-06-18	2015-06-18	External	2015-06-18	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-06-18	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-06-18	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-06-18	Address inactivated. CC was unable to reach the client.	2015
2015-06-22	2015-06-22	External	2015-06-22	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-06-22	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-06-22	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-06-22	Address inactivated. CC was unable to reach the client.	2015
2015-06-23	2015-06-23	External	2015-06-23	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-06-23	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-06-23	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-06-23	Address inactivated. CC was unable to reach the client.	2015
2015-06-23	2015-06-23	External	2015-06-23	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-06-23	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-06-23	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-06-23	Address inactivated. CC was unable to reach the client.	2015
2015-06-25	2015-06-25	External	2015-06-25	Client's Result Letter (Test Result)	2015-06-25	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-06-25	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center	2015-06-25	CC called the client and updated the address.	2015
2015-06-25	2015-06-25	External	2015-06-25	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-06-25	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-06-25	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-06-25	Address inactivated. CC was unable to reach the client.	2015
2015-06-26	2015-06-26	External	2015-06-26	Client's Result Letter (Test Result)	2015-06-26	Relative/Spouse opened the letter - address change not required	N/A	2015-06-26	Contact Center	Privacy breach	None Required	NO	Contact Center	2015-06-26	None Required	2015
2015-06-26	2015-06-26	External	2015-06-26	Client's Result Letter (Test Result)	2015-06-26	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-06-26	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-06-26	Address inactivated. CC was unable to reach the client.	2015
2015-07-02	2015-07-02	External	2015-07-02	Client's Result Letter (Test Result)	2015-07-02	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-07-02	Contact Center	Privacy breach	Contact Center could not reach client, address to be inactivated.	NO	Contact Center	2015-07-02	Client did not want to update address	2015
2015-07-06	2015-07-06	External	2015-07-06	Client's Invitation/Reminder Letter (Screening	2015-07-06	CC inactivated address + Unintended Recipient	N/A	2015-07-06	Contact Center	Privacy breach	Contact Center to call client/PCP and	YES	Contact Center	2015-07-06	CC called the client and updated the address.	2015

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				Status/Eligibility)		asked to return letter					update address.					
2015-07-07	2015-07-07	External	2015-07-07	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-07-07	CC inactivated incorrect address	N/A	2015-07-07	Contact Center	Privacy breach	None Required	NO	Contact Center	2015-07-07	None Required	2015
2015-07-08	2015-07-08	External	2015-07-08	Client's Result Letter (Test Result)	2015-07-08	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-07-08	Contact Center	Privacy breach	Contact Center could not reach client, address to be inactivated.	YES	Contact Center	2015-07-08	CC called the client and updated the address.	2015
2015-07-09	2015-07-09	External	2015-07-09	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-07-09	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-07-09	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-07-09	Address inactivated. CC was unable to reach the client.	2015
2015-07-09	2015-07-09	External	2015-07-09	Misdirected Form-sent in error by PCP/Screening Site	2015-07-09	CC to call the sender to inform of their breach + destroy the fax	N/A	2015-07-09	Contact Center	Policy breach	CC to call the sender to inform of their breach + destroy the fax	N/A	Contact Center	2015-07-09	CC informed the sender of the correct place to send the form and destroyed the fax	2015
2015-07-09	2015-07-09	External	2015-07-09	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-07-09	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-07-09	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center	2015-07-09	CC called the client and updated the address.	2015
2015-07-09	2015-07-09	External	2015-07-09	Client's Result Letter (Test Result)	2015-07-09	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-07-09	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-07-09	Address inactivated. CC was unable to reach the client.	2015
2015-07-10	2015-07-10	External	2015-07-10	Misdirected Patient Eligibility Form/Result-sent in error by PCP/Screening Site/lab	2015-07-10	CC to call the sender to inform of their breach + destroy the fax	N/A	2015-07-10	Contact Center	Policy breach	CC to call the sender to inform of their breach + destroy the fax	N/A	Contact Center	2015-07-10	CC informed the sender of the correct place to send the form and destroyed the fax	2015
2015-07-13	2015-07-13	External	2015-07-13	Client's Result Letter (Test Result)	2015-07-13	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-07-13	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	2015-07-13	Client did not want to update address	2015
2015-07-13	2015-07-13	External	2015-07-13	Client's Invitation/Reminder Letter (Screening	2015-07-13	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-07-13	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact	NO	Contact Center	2015-07-13	Address inactivated. CC was unable to	2015

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				Status/Eligibility)							intended client.				reach the client.	
2015-07-14	2015-07-14	External	2015-07-14	Client's Result Letter (Test Result)	2015-07-14	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-07-14	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-07-14	Address inactivated. CC was unable to reach the client.	2015
2015-07-15	2015-07-15	External	2015-07-15	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-07-15	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-07-15	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-07-15	Address inactivated. CC was unable to reach the client.	2015
2015-07-15	2015-07-15	External	2015-07-15	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-07-15	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-07-15	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-07-15	Address inactivated. CC was unable to reach the client.	2015
2015-07-15	2015-07-15	External	2015-07-15	Client's Result Letter (Test Result)	2015-07-15	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-07-15	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-07-15	Address inactivated. CC was unable to reach the client.	2015
2015-07-15	2015-07-15	External	2015-07-15	Client's Result Letter (Test Result)	2015-07-15	Address inactivated - Letter will not be returned	N/A	2015-07-15	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center	2015-07-15	CC called the client and updated the address.	2015
2015-07-16	2015-07-16	External	2015-07-16	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-07-16	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-07-16	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-07-16	Address inactivated. CC was unable to reach the client.	2015
2015-07-20	2015-07-20	External	2015-07-20	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-07-20	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-07-20	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-07-20	Address inactivated. CC was unable to reach the client.	2015
2015-07-20	2015-07-20	External	2015-07-20	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-07-20	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-07-20	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-07-20	Address inactivated. CC was unable to reach the client.	2015
2015-07-20	2015-07-20	External	2015-07-20	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-07-20	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-07-20	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-07-20	Address inactivated. CC was unable to reach the client.	2015
2015-07-22	2015-07-22	External	2015-07-22	Client's Result Letter (Test Result)	2015-07-22	CC inactivated address + Unintended	N/A	2015-07-22	Contact Center	Privacy breach	Contact Center to call client/PCP and	YES	Contact Center	2015-07-22	CC called the client and	2015

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
						Recipient asked to return letter					update address.				updated the address.	
2015-07-22	2015-07-22	External	2015-07-22	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-07-22	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-07-22	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-07-22	Address inactivated. CC was unable to reach the client.	2015
2015-07-22	2015-07-22	External	2015-07-22	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-07-22	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-07-22	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-07-22	Address inactivated. CC was unable to reach the client.	2015
2015-07-23	2015-07-23	External	2015-07-23	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-07-23	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-07-23	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-07-23	Address inactivated. CC was unable to reach the client.	2015
2015-07-23	2015-07-23	External	2015-07-23	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-07-23	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-07-23	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-07-23	Address inactivated. CC was unable to reach the client.	2015
2015-07-23	2015-07-23	External	2015-07-23	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-07-23	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-07-23	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-07-23	Address inactivated. CC was unable to reach the client.	2015
2015-07-28	2015-07-28	External	2015-07-28	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-07-28	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-07-28	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-07-28	Address inactivated. CC was unable to reach the client.	2015
2015-07-29	2015-07-29	External	2015-07-29	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-07-29	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-07-29	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-07-29	Address inactivated. CC was unable to reach the client.	2015
2015-07-29	2015-07-29	External	2015-07-29	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-07-29	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-07-29	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-07-29	Address inactivated. CC was unable to reach the client.	2015
2015-07-29	2015-07-29	External	2015-07-29	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-07-29	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-07-29	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center	2015-07-29	CC called the client and updated the address.	2015

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
2015-07-30	2015-07-30	External	2015-07-30	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-07-30	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-07-30	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-07-30	Address inactivated. CC was unable to reach the client.	2015
2015-07-30	2015-07-30	External	2015-07-30	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-07-30	Address inactivated - Letter will not be returned	N/A	2015-07-30	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	2015-07-30	CC called the client and updated the address.	2015
2015-07-31	2015-07-31	External	2015-07-31	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-07-31	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-07-31	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-07-31	Address inactivated. CC was unable to reach the client.	2015
2015-08-04	2015-08-04	External	2015-08-04	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-08-04	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-08-04	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-08-04	Address inactivated. CC was unable to reach the client.	2015
2015-08-04	2015-08-04	External	2015-08-04	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-08-04	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-08-04	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-08-04	Address inactivated. CC was unable to reach the client.	2015
2015-08-04	2015-08-04	External	2015-08-04	Misdirected Patient Eligibility Form/Result-sent in error by PCP/Screening Site/lab	2015-08-04	CC to call the sender to inform of their breach + destroy the fax	N/A	2015-08-04	Contact Center	Policy breach	CC to call the sender to inform of their breach + destroy the fax	NO	Contact Center	2015-08-04	CC informed the sender of the correct place to send the form and destroyed the fax	2015
2015-08-05	2015-08-05	Internal	2015-08-05	Cannot be determined	2015-08-05	None - unintended recipient notified CC of breach, did not leave their contact information; no containment possible.	N/A	2015-08-05	Contact Center	Privacy breach	CC could not find the client (intended recipient)'s profile in InScreen, no follow-up possible.	NO	Contact Center	2015-08-05	CC could not find the client (intended recipient)'s profile in InScreen, no follow-up possible.	2015
2015-08-07	2015-08-07	External	2015-08-07	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-08-07	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-08-07	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-08-07	Address inactivated. CC was unable to reach the client.	2015
2015-08-07	2015-08-07	External	2015-08-07	Client's Result Letter (Test Result)	2015-08-07	CC inactivated address + Unintended Recipient	N/A	2015-08-07	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact	NO	Contact Center	2015-08-07	Address inactivated. CC was unable to	2015

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
						asked to return letter					intended client.				reach the client.	
2015-08-10	2015-08-10	External	2015-08-10	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-08-10	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-08-10	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-08-10	Address inactivated. CC was unable to reach the client.	2015
2015-08-10	2015-08-10	External	2015-08-10	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-08-10	CC inactivated incorrect address	N/A	2015-08-10	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-08-10	Address inactivated. CC was unable to reach the client.	2015
2015-08-10	2015-08-10	External	2015-08-10	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-08-10	Address inactivated - Letter will not be returned	N/A	2015-08-10	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-08-10	Address inactivated. CC was unable to reach the client.	2015
2015-08-12	2015-08-12	External	2015-08-12	Client's Result Letter (Test Result)	2015-08-12	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-08-12	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	2015-08-12	CC called the client and updated the address.	2015
2015-08-12	2015-08-12	External	2015-08-12	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-08-12	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-08-12	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	2015-08-12	CC called the client and updated the address.	2015
2015-08-12	2015-08-12	External	2015-08-12	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-08-12	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-08-12	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-08-12	Address inactivated. CC was unable to reach the client.	2015
2015-08-12	2015-08-12	External	2015-08-12	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-08-12	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-08-12	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-08-12	Address inactivated. CC was unable to reach the client.	2015
2015-08-14	2015-08-14	Unclear	2015-08-14	Client's Name, DOB and Address discussed with a relative with client present-relative called on behalf of client-	2015-08-14	None - CC provided PHI to a relative of the client who was posing as the client, after completing authentication. No containment possible.	N/A	2015-08-14	Contact Center	Privacy breach	N/A - no recommendations logged.	NO	Contact Center	2015-08-24	N/A - no recommendations logged. CC referred client to provider to discuss concerns, but this is not related to the breach itself.	2015
2015-08-14	2015-08-14	External	2015-08-14	Client's Invitation/Reminder Letter (Screening	2015-08-14	CC inactivated the address + Unintended	N/A	2015-08-14	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact	NO	Contact Center	2015-08-14	Address inactivated. CC was unable to	2015

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				Status/Eligibility)		Recipient to destroy letter					intended client.				reach the client.	
2015-08-14	2015-08-14	External	2015-08-14	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-08-14	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-08-14	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-08-14	Address inactivated. CC was unable to reach the client.	2015
2015-08-17	2015-08-17	External	2015-08-17	Client's Result Letter (Test Result)	2015-08-17	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-08-17	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-08-17	Address inactivated. CC was unable to reach the client.	2015
2015-08-18	2015-08-18	External	2015-08-18	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-08-18	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-08-18	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-08-18	Address inactivated. CC was unable to reach the client.	2015
2015-08-18	2015-08-18	External	2015-08-18	Client's Result Letter (Test Result)	2015-08-18	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-08-18	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-08-18	Address inactivated. CC was unable to reach the client.	2015
2015-08-20	2015-08-20	External	2015-08-20	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-08-20	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-08-20	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-08-20	Address inactivated. CC was unable to reach the client.	2015
2015-08-21	2015-08-21	External	2015-08-21	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-08-21	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-08-21	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-08-21	Address inactivated. CC was unable to reach the client.	2015
2015-08-25	2015-08-25	External	2015-08-25	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-08-25	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-08-25	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-08-25	Address inactivated. CC was unable to reach the client.	2015
2015-08-26	2015-08-26	External	2015-08-26	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-08-26	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-08-26	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-08-26	Address inactivated. CC was unable to reach the client.	2015
2015-08-26	2015-08-26	External	2015-08-26	Misdirected Patient Eligibility Form/Result-sent in error by PCP/Screening Site/lab	2015-08-26	CC to call the sender to inform of their breach + destroy the fax	N/A	2015-08-26	Contact Center	Policy breach	CC to call the sender to inform of their breach + destroy the fax	NO	Contact Center	2015-08-26	CC informed the sender of the correct place to send the form and destroyed the fax	2015

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
2015-08-26	2015-08-26	External	2015-08-26	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-08-26	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-08-26	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-08-26	Address inactivated. CC was unable to reach the client.	2015
2015-08-27	2015-08-27	External	2015-08-27	Misdirected Patient Eligibility Form/Result-sent in error by PCP/Screening Site/lab	2015-08-27	CC to call the sender to inform of their breach + destroy the fax	N/A	2015-08-27	Contact Center	Policy breach	CC to call the sender to inform of their breach + destroy the fax	NO	Contact Center	2015-08-27	CC informed the sender of the correct place to send the form and destroyed the fax	2015
2015-08-28	2015-08-28	External	2015-08-28	Client's Result Letter (Test Result)	2015-08-28	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-08-28	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-08-28	Address inactivated. CC was unable to reach the client.	2015
2015-08-28	2015-08-28	External	2015-08-28	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-08-28	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-08-28	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	2015-08-28	Address inactivated. CC was unable to reach the client.	2015
2015-09-02	2015-09-02	External	2015-09-02	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-09-02	CC inactivated incorrect address	2015-09-09	2015-09-21	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center & Privacy Specialist	N/A	CC called the client and updated the address.	2015
2015-09-03	2015-09-03	External	2015-09-03	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-09-03	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-10-13	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-09-03	2015-09-03	External	2015-09-03	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-09-03	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-10-13	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-09-04	2015-09-04	External	2015-09-04	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-09-04	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-09-04	Contact Center	Privacy breach	None Required	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-09-04	2015-09-04	External	2015-09-04	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-09-04	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-09-04	Contact Center	Privacy breach	None Required	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-09-08	2015-09-08	External	2015-09-08	Client's Invitation/Remi	2015-09-08	CC inactivated address +	2015-09-09	2015-09-21	Contact Center	Privacy breach	Contact Center to call	YES	Contact Center &	N/A	CC called the client and	2015

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				nder Letter (Screening Status/Eligibility)		Unintended Recipient asked to return letter					client/PCP and update address.		Privacy Specialist		updated the address.	
2015-09-08	2015-09-08	External	2015-09-14	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-09-14	CC inactivated the address + Unintended Recipient to destroy letter	2015-10-13	2015-10-13	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center & Privacy Specialist	N/A	CC called the client and updated the address.	2015
2015-09-10	2015-09-10	External	2015-09-10	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-09-10	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-09-22	Contact Center	Privacy breach	None Required	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-09-10	2015-09-10	External	2015-09-04	Client's Result Letter (Test Result)	2015-09-04	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-09-17	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to obtain client's phone number from PCP.	2015
2015-09-10	2015-09-10	External	2015-09-10	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-09-10	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-09-10	Contact Center	Privacy breach	None Required	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-09-15	2015-09-15	External	2015-09-15	Client PHI intended for a CCO screening program was provided to CCO by a PCP, in electronic, voicemail, or paper form.	2015-09-15	The Contact Centre agent uploaded the voicemail to an activity in InScreen, and hard deleted the voicemail from CCO's systems.	N/A	2015-09-16	Contact Center	Policy breach	The Contact Centre agent should call the PCP and inform them of the policy breach. For misdirected requests, the agent should re-direct the PCP to the appropriate recipient of these requests (e.g., Ontario Breast Screening Program High Risk site) and advise them to not send PHI to CCO for such requests.	NO	Contact Center	N/A	The PCP was notified of the policy breach, and about the policy on client PHI maintenance.	2015
2015-09-16	2015-09-16	External	2015-09-16	Client's Invitation/Reminder Letter (Screening	2015-09-16	CC inactivated address + Unintended Recipient	N/A	2015-10-02	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to	2015

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				Status/Eligibility)		asked to return letter									reach the client.	
2015-09-16	2015-09-16	External	2015-09-16	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-09-16	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-09-16	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-09-17	2015-09-17	External	2015-09-17	Client's Result Letter (Test Result)	2015-09-17	CC inactivated address + Unintended Recipient asked to return letter	2015-09-21	2015-10-19	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center & Privacy Specialist	N/A	CC called the client and updated the address.	2015
2015-09-17	2015-09-17	External	2015-09-17	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-09-17	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-09-29	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-09-18	2015-09-18	External	2015-09-18	Client's Result Letter (Test Result)	2015-09-18	CC inactivated address + Unintended Recipient asked to return letter	2015-09-21	2015-10-20	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center & Privacy Specialist	N/A	CC called the client and updated the address.	2015
2015-09-22	2015-09-22	External	2015-09-22	Client's Result Letter (Test Result)	2015-09-22	Address inactivated - Letter will not be returned	2015-10-20	2015-11-06	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center & Privacy Specialist	N/A	CC called the client and updated the address.	2015
2015-09-22	2015-09-22	External	2015-09-22	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-09-22	Address inactivated - Letter will not be returned	N/A	2015-09-22	Contact Center	Privacy breach	None Required	NO	Contact Center	N/A	None Required	2015
2015-09-22	2015-09-22	External	2015-09-22	Client's Result Letter (Test Result)	2015-09-22	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-09-28	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Client did not want to update address.	2015
2015-09-22	2015-09-22	External	2015-09-22	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-09-22	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-09-22	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-09-22	2015-09-22	External	2015-09-22	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-09-22	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-09-22	Contact Center	Privacy breach	None Required	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-09-23	2015-09-23	External	2015-09-23	Client's Invitation/Reminder Letter	2015-09-23	CC inactivated address + Unintended	N/A	2015-09-28	Contact Center	Privacy breach	Contact Center to call client/PCP and	NO	Contact Center	N/A	Address inactivated. CC was	2015

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				(Screening Status/Eligibility)		Recipient asked to return letter					update address.				unable to reach the client.	
2015-09-23	2015-09-23	External	2015-09-23	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-09-23	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-10-05	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-09-23	2015-09-23	External	2015-09-24	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-09-24	CC inactivated the address + Unintended Recipient to destroy letter	2015-09-24	2015-10-13	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	None Required	2015
2015-09-23	2015-09-23	External	2015-09-23	Client's Result Letter (Test Result)	2015-09-23	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-10-06	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-09-24	2015-09-24	External	2015-09-24	Client's Result Letter (Test Result)	2015-09-24	CC inactivated the address + Unintended Recipient to destroy letter	2015-09-25	2015-10-19	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center & Privacy Specialist	N/A	CC called the client and updated the address.	2015
2015-09-24	2015-09-24	External	2015-09-24	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-09-24	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-10-08	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-09-25	2015-09-25	External	2015-09-25	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-09-25	CC inactivated incorrect address	2015-09-25	2015-10-19	Contact Center	Privacy breach	None Required	YES	Contact Center & Privacy Specialist	N/A	CC called the client and updated the address.	2015
2015-09-28	2015-09-28	External	2015-09-28	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-09-28	Address inactivated - Letter will not be returned	N/A	2015-09-28	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-09-28	2015-09-28	External	2015-09-28	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-09-28	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-09-28	Contact Center	Privacy breach	None Required	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-09-28	2015-09-28	External	2015-09-28	Client PHI intended for a CCO screening program was provided to CCO by a PCP, in	2015-09-28	The Contact Centre agent uploaded the fax to an activity in InScreen. The agent then hard deleted	N/A	2015-09-28	Contact Center & Privacy Specialist	Policy breach	The Contact Centre agent should call the PCP and inform them of the policy breach. For misdirected	NO	Contact Center & Privacy Specialist	N/A	The PCP was notified of the policy breach, and about the policy on client PHI maintenance.	2015

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				electronic or paper form.		the fax from CCO's systems.					requests, the agent should re-direct the PCP to the appropriate recipient of these requests (e.g., Ontario Breast Screening Program High Risk site) and advise them to not send PHI to CCO for such requests.					
2015-09-29	2015-09-29	External	2015-09-29	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-09-29	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-09-29	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-09-30	2015-09-30	External	2015-09-30	Client's Result Letter (Test Result)	2015-09-30	CC inactivated incorrect address	2015-09-30	2015-09-30	Contact Center	Privacy breach	None Required	YES	Contact Center & Privacy Specialist	N/A	CC called the client and updated the address.	2015
2015-09-30	2015-09-30	External	2015-09-30	Client's Result Letter (Test Result)	2015-09-30	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-10-28	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to obtain client's phone number from PCP.	2015
2015-09-30	2015-09-30	External	2015-09-30	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-09-30	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-09-30	Contact Center	Privacy breach	None Required	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-09-30	2015-09-30	External	2015-09-30	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-09-30	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-09-30	Contact Center	Privacy breach	None Required	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-10-06	2015-10-06	External	2015-10-06	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-10-06	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-10-28	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to obtain client's phone number from PCP.	2015
2015-10-06	2015-10-06	Internal	2015-10-06	Client's Result Letter (Test Result)	2015-10-06	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-10-29	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
2015-10-09	2015-10-09	External	2015-10-09	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-10-09	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-10-09	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-10-09	2015-10-09	External	2015-10-09	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-09-29	CC inactivated incorrect address	2015-10-09	2015-10-20	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-10-09	2015-10-09	External	2015-10-09	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-10-09	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-10-13	Contact Center	Privacy breach	None Required	NO	Contact Center	N/A	None Required	2015
2015-10-13	2015-10-13	External	2015-10-13	Client's Result Letter (Test Result)	2015-10-13	CC inactivated incorrect address	2015-10-22	2015-11-11	Contact Center	Privacy breach	None Required	YES	Contact Center & Privacy Specialist	N/A	CC called the client and updated the address.	2015
2015-10-13	2015-10-13	External	2015-10-13	Client's Result Letter (Test Result)	2015-10-13	CC inactivated incorrect address	N/A	2015-10-13	Contact Center	Privacy breach	None Required	NO	Contact Center	N/A	CC called the client and updated the address.	2015
2015-10-13	2015-10-13	External	2015-10-13	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-10-13	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-10-13	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-10-15	2015-10-15	External	2015-10-15	Client's Result Letter (Test Result)	2015-10-15	CC inactivated address + Unintended Recipient asked to return letter	2015-10-22	2015-10-28	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center & Privacy Specialist	N/A	CC called the client and updated the address.	2015
2015-10-15	2015-10-15	External	2015-10-15	A representative from the PCP's office who is not registered as a delegate of the PCP is accessing the SAR reports, and calling the Contact Centre on behalf of the PCP.	2015-10-15	The Contact Centre agent immediately ended the discussion regarding the SAR. They informed the representative that the SAR report access constituted a privacy breach.	2015-10-15	2015-10-15	Contact Center	Policy breach	The Contact Centre agent should advise the representative to register for a ONE ID account. They should further advise that the representative must be registered with CCO as a delegate of the PCP prior to accessing the PCP's SAR, or calling CCO about anything	NO	Contact Center	N/A	The Contact Centre agent provided feedback to the representative, who agreed to register for ONE ID. The Contact Centre agent transferred the representative to eHealth, or provided them with the eHealth phone number, so that they could be registered	2015

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
											related to the SAR.				for a ONE ID account.	
2015-10-16	2015-10-16	External	2015-10-16	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-10-16	CC inactivated incorrect address	N/A	2015-10-16	Contact Center	Privacy breach	None Required	NO	Contact Center	N/A	None Required	2015
2015-10-16	2015-10-16	External	2015-10-16	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-10-16	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-10-16	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-10-16	2015-10-16	External	2015-10-16	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-10-16	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-10-16	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-10-16	2015-10-16	Internal	2015-10-16	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	N/A	Unintended recipient left a voicemail describing a breach. No contact information for the unintended recipient available, therefore no containment possible.	N/A	N/A	Contact Center	Privacy breach	CC could not find the client (intended recipient)'s profile in InScreen, no follow-up possible.	N/A	Contact Center	N/A	CC could not find the client (intended recipient)'s profile in InScreen, no follow-up possible.	2015
2015-10-19	2015-10-19	External	2015-10-19	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-10-19	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-11-06	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-10-20	2015-10-20	External	2015-10-20	Client's Result Letter (Test Result)	2015-10-20	CC inactivated address + Unintended Recipient asked to return letter	2015-11-18	2015-11-26	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	YES	Contact Center & Privacy Specialist	N/A	CC called the client and updated the address.	2015
2015-10-20	2015-10-20	External	2015-10-20	Client's Result Letter (Test Result)	2015-10-20	CC inactivated the address + Unintended Recipient to destroy letter	2015-10-20	2015-11-11	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	YES	Contact Center & Privacy Specialist	N/A	CC called the client and updated the address.	2015
2015-10-20	2015-10-20	External	2015-10-20	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-10-20	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-11-09	Contact Center	Privacy breach	None Required	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
2015-10-21	2015-10-21	External	2015-10-21	Client's Result Letter (Test Result)	2015-10-21	Address inactivated - Letter will not be returned	N/A	2015-10-21	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-10-21	2015-10-21	External	2015-10-21	Client's Result Letter (Test Result)	2015-10-21	CC inactivated the address + Unintended Recipient to destroy letter	2015-11-18	2015-11-26	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center & Privacy Specialist	N/A	CC called the client and updated the address.	2015
2015-10-22	2015-10-22	External	2015-10-22	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-10-22	Address inactivated - Letter will not be returned	2015-10-29	2015-11-06	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center & Privacy Specialist	N/A	CC called the client and updated the address.	2015
2015-10-22	2015-10-22	External	2015-10-22	Client's Result Letter (Test Result)	2015-09-14	CC inactivated incorrect address	2015-11-13	2015-11-26	Contact Center	Privacy breach	None Required	YES	Contact Center & Privacy Specialist	N/A	CC called the client and updated the address.	2015
2015-10-26	2015-10-26	External	2015-10-26	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-10-26	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-10-27	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-10-27	2015-10-27	External	2015-10-27	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-10-27	Address inactivated - Letter will not be returned	N/A	2015-11-13	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to obtain client's phone number from PCP.	2015
2015-10-27	2015-10-27	External	2015-10-27	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-10-27	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-11-06	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-10-27	2015-10-27	External	2015-10-27	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-10-27	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-10-27	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-10-27	2015-10-27	External	2015-10-27	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-10-27	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-11-05	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-10-28	2015-10-28	External	2015-10-28	Client's Result Letter (Test Result)	2015-09-21	CC inactivated incorrect address	2015-11-26	2015-11-26	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center & Privacy Specialist	N/A	CC called the client and updated the address.	2015

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
2015-10-28	2015-10-28	External	2015-10-28	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-10-23	CC inactivated incorrect address	N/A	2015-11-06	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-10-28	2015-10-28	Internal	2015-10-28	Client's Result Letter (Test Result)	N/A	CC received returned letter, which had been opened. No contact information for the unintended recipient available, therefore no containment possible.	N/A	N/A	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center	2015-11-06	CC did not contact client because they saw that the client's address had already been updated post breach.	2015
2015-10-30	2015-10-30	External	2015-10-30	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-10-30	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-12-01	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-11-02	2015-11-02	External	2015-11-02	Client's Result Letter (Test Result)	2015-11-02	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-11-23	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-11-02	2015-11-02	External	2015-11-02	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-11-02	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-01-06	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-11-02	2015-11-02	External	2015-11-02	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-11-02	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-11-03	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-11-05	2015-11-05	External	2015-11-05	Client's Result Letter (Test Result)	2015-11-05	CC inactivated address + Unintended Recipient asked to return letter	2015-11-06	2015-12-02	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center & Privacy Specialist	N/A	CC called the client and updated the address.	2015
2015-11-06	2015-11-06	External	2015-11-06	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-11-06	CC inactivated incorrect address	N/A	2015-12-29	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-11-06	2015-11-06	External	2015-11-06	Client's Invitation/Reminder Letter (Screening	2015-11-06	CC inactivated the address + Unintended	N/A	2015-11-06	Contact Center	Privacy breach	None Required	NO	Contact Center	N/A	Address inactivated. CC was unable to	2015

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				Status/Eligibility)		Recipient to destroy letter									reach the client.	
2015-11-09	2015-11-09	External	2015-11-09	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-11-09	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-11-24	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-11-11	2015-11-11	External	2015-11-11	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-11-11	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-12-01	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-11-13	2015-11-13	Internal	2015-11-13	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-11-16	National Change of Address database error. Intended recipient did finally receive the letter. Client also faxed a reminder letter to CCO with an address correction marked; no containment possible.	2015-11-20	2015-11-26	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center & Privacy Specialist	N/A	CC called the client and updated the address.	2015
2015-11-13	2015-11-13	Unclear	2015-11-13	Client PHI intended for a CCO screening program was provided to CCO by a PCP, in electronic, voicemail, or paper form.	2015-11-13	Privacy uploaded the fax to an activity in InScreen. Privacy had been the original recipient of the PHI, and had hard deleted the fax containing PHI from CCO's systems.	2015-11-13	2015-12-01	Contact Center & Privacy Specialist	Policy breach	The Contact Centre agent should call the PCP and inform them of the policy breach. For misdirected requests, the agent should re-direct the PCP to the appropriate recipient of these requests (e.g., Ontario Breast Screening Program High Risk site) and advise them to not send PHI to CCO for such requests.	NO	Contact Center & Privacy Specialist	N/A	The PCP was notified of the policy breach, and about the policy on client PHI maintenance.	2015
2015-11-16	2015-11-16	External	2015-11-16	Client's Result Letter (Test Result)	2015-11-16	CC inactivated address + Unintended	N/A	2015-12-01	Contact Center	Privacy breach	Contact Center to call client/PCP and	NO	Contact Center	N/A	Address inactivated. CC was	2015

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
						Recipient asked to return letter					update address.				unable to obtain client's phone number from PCP.	
2015-11-16	2015-11-16	External	2015-11-16	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-11-16	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-12-02	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-11-16	2015-11-16	External	2015-11-16	Client's Result Letter (Test Result)	2015-11-16	CC inactivated the address + Unintended Recipient to destroy letter	2015-11-18	2015-11-26	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center & Privacy Specialist	N/A	CC called the client and updated the address.	2015
2015-11-16	2015-11-16	External	2015-11-16	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-11-16	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-11-16	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-11-16	2015-11-16	External	2015-11-16	Client's Result Letter (Test Result)	2015-11-16	Canada Post delivery error. The intended recipient finally received the letter, opened.	N/A	2015-11-16	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	2015-11-16	CC contacted the client and updated the address.	2015
2015-11-17	2015-11-17	External	2015-11-17	Client's Result Letter (Test Result)	2015-11-17	CC inactivated incorrect address	2015-11-17	2015-11-26	Contact Center	Privacy breach	None Required	YES	Contact Center & Privacy Specialist	N/A	CC called the client and updated the address.	2015
2015-11-17	2015-11-17	External	2015-11-17	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-11-18	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-12-07	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-11-19	2015-11-19	External	2015-11-19	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-11-19	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-11-23	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-11-19	2015-11-19	External	2015-11-19	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-11-19	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-12-07	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	N/A	Client did not want to update address.	2015
2015-11-19	2015-11-19	External	2015-11-19	Client's Result Letter (Test Result)	2015-11-19	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-11-19	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-11-20	2015-11-20	External	2015-11-20	Client's Invitation/Reminder Letter	2015-11-20	CC inactivated address + Unintended	N/A	2015-12-04	Contact Center	Privacy breach	Contact Center to call client/PCP and	NO	Contact Center	N/A	Address inactivated. CC was	2015

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				(Screening Status/Eligibility)		Recipient asked to return letter					update address.				unable to obtain client's phone number from PCP.	
2015-11-20	2015-11-20	External	2015-11-20	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-11-20	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-12-07	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-11-23	2015-11-23	External	2015-11-23	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-11-23	Address inactivated - Letter will not be returned	N/A	2015-12-07	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-11-23	2015-11-23	External	2015-11-23	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-11-23	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-11-24	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-11-23	2015-11-23	External	2015-11-23	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-11-23	CC inactivated incorrect address	N/A	2015-12-07	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-11-23	2015-11-23	External	2015-11-23	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-11-23	Relative/Spouse opened the letter - address change not required	N/A	2015-11-25	Contact Center	Privacy breach	None Required	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-11-24	2015-11-24	External	2015-11-24	Client's Result Letter (Test Result)	2015-11-24	CC inactivated address + Unintended Recipient asked to return letter	N/A	2015-12-08	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-11-24	2015-11-24	External	2015-11-24	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-11-24	CC inactivated incorrect address	N/A	2015-12-07	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-11-25	2015-11-25	External	2015-11-25	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-11-25	CC inactivated incorrect address	2015-11-25	2015-11-26	Contact Center	Privacy breach	None Required	YES	Contact Center & Privacy Specialist	N/A	None Required	2015
2015-11-25	2015-11-25	External	2015-11-25	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-11-13	CC inactivated incorrect address	2015-11-26	2015-12-04	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center & Privacy Specialist	N/A	CC called the client and updated the address.	2015

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
2015-11-25	2015-11-25	External	2015-11-25	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-11-13	CC inactivated incorrect address	N/A	2015-11-27	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-11-25	2015-11-25	External	2015-11-25	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-11-25	CC inactivated incorrect address	N/A	2015-11-25	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-11-25	2015-11-25	External	2015-11-25	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-11-25	CC inactivated incorrect address	N/A	2015-11-27	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-11-25	2015-11-25	Internal	2015-11-25	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-11-25	Unintended recipient faxed misdirected mail to CC with a note that the intended recipient had moved. No contact info on file for the unintended recipient; no containment possible.	N/A	2016-01-06	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	2016-01-06	Address inactivated. CC was unable to reach the client.	2015
2015-11-26	2015-11-26	External	2015-11-26	Client's Result Letter (Test Result)	2015-11-26	Address inactivated - Letter will not be returned	N/A	2015-12-08	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-11-27	2015-11-27	External	2015-11-27	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-11-27	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-11-27	Contact Center	Privacy breach	None Required	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-11-30	2015-11-30	External	2015-11-30	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-11-17	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-12-01	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-12-01	2015-12-01	External	2015-12-01	Client's Result Letter (Test Result)	2015-11-27	CC inactivated incorrect address	2015-12-03	2015-12-04	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center & Privacy Specialist	N/A	CC called the client and updated the address.	2015

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
2015-12-01	2015-12-01	External	2015-12-01	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-11-27	CC inactivated incorrect address	N/A	2015-12-08	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-12-01	2015-12-01	External	2015-12-01	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-11-27	CC inactivated incorrect address	N/A	2015-12-01	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-12-01	2015-12-01	External	2015-12-01	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-11-27	CC inactivated incorrect address	N/A	2015-12-01	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-12-03	2015-12-03	External	2015-12-03	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-12-03	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2016-01-12	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to obtain client's phone number from PCP.	2015
2015-12-07	2015-12-07	External	2015-12-07	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-12-07	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2016-01-12	Contact Center	Privacy breach	None Required	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-12-09	2015-12-09	External	2015-12-09	Client's Result Letter (Test Result)	2015-12-09	CC inactivated incorrect address	2015-12-10	2015-12-16	Contact Center	Privacy breach	None Required	YES	Contact Center & Privacy Specialist	N/A	CC called the client and updated the address.	2015
2015-12-10	2015-12-10	External	2015-12-10	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-12-10	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2015-12-10	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-12-15	2015-12-15	External	2015-12-15	Client's Result Letter (Test Result)	2015-12-15	CC inactivated address + Unintended Recipient asked to return letter	N/A	2016-01-27	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-12-16	2015-12-16	External	2015-12-16	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-12-12	CC inactivated incorrect address	N/A	2016-02-24	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-12-16	2015-12-16	External	2015-12-16	Client's Invitation/Reminder Letter (Screening	2015-12-12	CC inactivated incorrect address	N/A	2015-12-22	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to	2015

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				Status/Eligibility)											reach the client.	
2015-12-16	2015-12-16	External	2015-12-16	Client's Result Letter (Test Result)	2015-12-12	CC inactivated incorrect address	N/A	2015-12-17	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-12-17	2015-12-17	External	2015-12-17	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-12-17	CC inactivated incorrect address	2015-12-17	2015-12-17	Contact Center	Privacy breach	None Required	YES	Contact Center & Privacy Specialist	N/A	CC called the client and updated the address.	2015
2015-12-21	2015-12-21	External	2015-12-21	Client's Result Letter (Test Result)	2015-12-18	CC inactivated incorrect address	2016-01-22	2016-02-03	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center & Privacy Specialist	N/A	CC called the client and updated the address.	2015
2015-12-21	2015-12-21	External	2015-12-21	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-12-12	CC inactivated incorrect address	N/A	2016-01-20	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-12-21	2015-12-21	External	2015-12-21	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-12-12	CC inactivated incorrect address	N/A	2016-01-21	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-12-21	2015-12-21	External	2015-12-21	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2015-12-18	CC inactivated incorrect address	N/A	2016-01-21	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-12-21	2015-12-21	External	2015-12-21	Client's Result Letter (Test Result)	2015-12-18	CC inactivated incorrect address	N/A	2016-01-20	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-12-21	2015-12-21	External	2015-12-21	Client's Result Letter (Test Result)	2015-12-21	CC inactivated incorrect address	N/A	2016-01-14	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2015
2015-12-21	2015-12-21	External	2015-12-21	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-01-20	CC inactivated incorrect address	N/A	2016-01-20	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	CC called the client and updated the address.	2015
2015-12-21	2015-12-21	External	2015-12-21	Client's Invitation/Reminder Letter	2016-01-18	CC inactivated incorrect address	N/A	2016-01-20	Contact Center	Privacy breach	Contact Center to call client/PCP and	NO	Contact Center	N/A	Client did not want to update address.	2015

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				(Screening Status/Eligibility)							update address.					
2016-01-05	2016-01-05	External	2016-01-05	A representative from the PCP's office who is not registered as a delegate of the PCP is accessing the SAR reports, and calling the Contact Centre on behalf of the PCP.	2016-01-05	The Contact Centre agent immediately ended the discussion regarding the SAR. They informed the representative that the SAR report access constituted a privacy breach.	2016-01-05	2016-01-05	Contact Center	Policy breach	The Contact Centre agent should advise the representative to register for a ONE ID account. They should further advise that the representative must be registered with CCO as a delegate of the PCP prior to accessing the PCP's SAR, or calling CCO about anything related to the SAR.	NO	Contact Center	N/A	The Contact Centre agent provided feedback to the representative, who agreed to register for ONE ID. The Contact Centre agent transferred the representative to eHealth, or provided them with the eHealth phone number, so that they could be registered for a ONE ID account.	2016
2016-01-05	2016-01-05	External	2016-01-05	Lab reports containing PHI (pathology, diagnostics, screening, treatment) related to CCO programs were sent to CCO.	2016-01-05	Privacy uploaded the fax to an activity in InScreen. Privacy had been the original recipient of the PHI, and had hard deleted the fax containing PHI from CCO's systems.	2016-01-05	2016-01-05	Contact Center & Privacy Specialist	Policy breach	The Manager of Laboratory Services should contact the program partner/lab and notify them of the PHI that was sent via an unauthorized method. The Contact Centre or Privacy should then shred the PHI.	NO	Contact Center & Privacy Specialist	N/A	The applicable program was notified, and relevant safeguards were put in place to protect incoming PHI. The Contact Centre agent notified the sender of the policy breach.	2016
2016-01-05	2016-01-05	External	2016-01-05	Screening-related status/confirmation of PHI (i.e., policy breaches where the Contact Centre agent did not authenticate as per standard operating procedures)	2016-01-05	Privacy uploaded the fax to an activity in InScreen. Privacy had been the original recipient of the PHI, and had hard deleted the fax containing PHI from CCO's systems.	2016-01-05	2016-01-05	Contact Center & Privacy Specialist	Policy breach	The Contact Centre agent should call the PCP and inform them of the policy breach. For client requests through the PCP (withdraw, address updates, anything screening related), the	NO	Contact Center & Privacy Specialist	N/A	The PCP was notified of the policy breach, and about the policy on client PHI maintenance.	2016

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
											agent should direct the PCP to have the client call CCO directly for the request.					
2016-01-07	2016-01-07	External	2016-01-07	Client's Result Letter (Test Result)	2016-01-07	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2016-01-14	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-01-08	2016-01-08	External	2016-01-08	Client's Result Letter (Test Result)	2016-01-08	CC inactivated incorrect address	2016-01-27	2016-02-01	Contact Center	Privacy breach	None Required	YES	Contact Center & Privacy Specialist	N/A	CC called the client and updated the address.	2016
2016-01-08	2016-01-08	External	2016-01-08	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-01-13	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2016-01-18	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-01-08	2016-01-08	Unclear	2016-01-08	Lab reports containing PHI (pathology, diagnostics, screening, treatment) related to CCO programs were sent to CCO.	2016-01-08	The Manager of Laboratory Services notified the program partner/lab of the policy breach.	N/A	2016-01-08	Contact Center & Privacy Specialist	Policy breach	The Manager of Laboratory Services should contact the program partner/lab and notify them of the PHI that was sent via an unauthorized method. The Contact Centre or Privacy should then shred the PHI.	NO	Contact Center & Privacy Specialist	N/A	The Manager of Laboratory Services has confirmed that their partner has been notified of the policy breach. The Contact Centre or Privacy then shredded the PHI.	2016
2016-01-08	2016-01-08	Unclear	2016-01-08	Lab reports containing PHI (pathology, diagnostics, screening, treatment) related to CCO programs were sent to CCO.	2016-01-08	The Manager of Laboratory Services notified the program partner/lab of the policy breach.	N/A	2016-01-08	Contact Center & Privacy Specialist	Policy breach	The Manager of Laboratory Services should contact the program partner/lab and notify them of the PHI that was sent via an unauthorized method. The Contact Centre or Privacy should then shred the PHI.	NO	Contact Center & Privacy Specialist	N/A	The Manager of Laboratory Services has confirmed that their partner has been notified of the policy breach. The Contact Centre or Privacy then shredded the PHI.	2016
2016-01-08	2016-01-08	Unclear	2016-01-08	Lab reports containing PHI	2016-01-08	The Manager of Laboratory	N/A	2016-01-08	Contact Center &	Policy breach	The Manager of Laboratory	NO	Contact Center &	N/A	The Manager of Laboratory	2016

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				(pathology, diagnostics, screening, treatment) related to CCO programs were sent to CCO.		Services notified the program partner/lab of the policy breach.			Privacy Specialist		Services should contact the program partner/lab and notify them of the PHI that was sent via an unauthorized method. The Contact Centre or Privacy should then shred the PHI.		Privacy Specialist		Services has confirmed that their partner has been notified of the policy breach. The Contact Centre or Privacy then shredded the PHI.	
2016-01-08	2016-01-08	Unclear	2016-01-08	Lab reports containing PHI (pathology, diagnostics, screening, treatment) related to CCO programs were sent to CCO.	2016-01-08	The Manager of Laboratory Services notified the program partner/lab of the policy breach.	N/A	2016-01-08	Contact Center & Privacy Specialist	Policy breach	The Manager of Laboratory Services should contact the program partner/lab and notify them of the PHI that was sent via an unauthorized method. The Contact Centre or Privacy should then shred the PHI.	NO	Contact Center & Privacy Specialist	N/A	The Manager of Laboratory Services has confirmed that their partner has been notified of the policy breach. The Contact Centre or Privacy then shredded the PHI.	2016
2016-01-11	2016-01-11	External	2016-01-11	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-01-11	CC inactivated address + Unintended Recipient asked to return letter	N/A	2016-01-28	Contact Center	Privacy breach	None Required	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-01-11	2016-01-11	External	2016-01-11	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-01-11	CC inactivated the address + Unintended Recipient to destroy letter	2016-01-11	2016-01-11	Contact Center	Privacy breach	None Required	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-01-12	2016-01-12	External	2016-01-12	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-01-12	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2016-03-01	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-01-12	2016-01-12	External	2016-01-12	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-01-12	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2016-01-12	Contact Center	Privacy breach	None Required	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-01-14	2016-01-14	External	2016-01-14	Client's Invitation/Remi	2016-01-14	CC inactivated the address +	N/A	2016-01-19	Contact Center	Privacy breach	Contact Center to call	NO	Contact Center	N/A	Address inactivated.	2016

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				nder Letter (Screening Status/Eligibility)		Unintended Recipient to destroy letter					client/PCP and update address.				CC was unable to reach the client.	
2016-01-14	2016-01-14	External	2016-01-14	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-01-14	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2016-01-14	Contact Center	Privacy breach	None Required	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-01-18	2016-01-18	External	2016-01-18	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-01-18	CC inactivated address + Unintended Recipient asked to return letter	N/A	2016-02-02	Contact Center	Privacy breach	None Required	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-01-18	2016-01-18	External	2016-01-18	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-01-18	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2016-03-04	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-01-18	2016-01-18	External	2016-01-18	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-01-18	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2016-01-18	Contact Center	Privacy breach	None Required	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-01-19	2016-01-19	External	2016-01-19	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-01-19	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2016-02-03	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-01-19	2016-01-19	External	2016-01-19	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-01-19	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2016-01-29	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-01-19	2016-01-19	External	2016-01-19	Client's Result Letter (Test Result)	2016-01-19	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2016-02-03	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-01-20	2016-01-20	External	2016-01-20	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-01-20	CC inactivated address + Unintended Recipient asked to return letter	N/A	2016-02-01	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-01-20	2016-01-20	External	2016-01-20	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-01-20	CC inactivated address + Unintended Recipient asked to return letter	N/A	2016-02-18	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
2016-01-22	2016-01-22	External	2016-01-22	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-01-22	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2016-01-27	Contact Center	Privacy breach	None Required	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-01-22	2016-01-22	External	2016-01-22	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-01-22	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2016-01-22	Contact Center	Privacy breach	None Required	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-01-26	2016-01-26	External	2016-01-26	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-01-26	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2016-01-28	Contact Center	Privacy breach	None Required	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-01-26	2016-01-26	Internal	2016-01-26	Client's Result Letter (Test Result)	2016-01-26	National Change of Address database error. The intended recipient finally received the letter, opened.	2016-01-28	2016-01-29	Contact Center	Privacy breach	None Required	YES	Contact Center & Privacy Specialist	2016-01-29	CC called the client and updated the address.	2016
2016-01-27	2016-01-27	External	2016-01-27	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-01-27	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2016-03-07	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-01-27	2016-01-27	External	2016-01-27	Client's Result Letter (Test Result)	2016-01-27	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2016-02-03	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-01-28	2016-01-28	External	2016-01-28	Client's Result Letter (Test Result)	2016-01-28	CC inactivated incorrect address	2016-02-01	2016-02-01	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center & Privacy Specialist	N/A	CC called the client and updated the address.	2016
2016-01-29	2016-01-29	External	2016-01-29	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-01-29	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2016-02-01	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-02-01	2016-02-01	External	2016-02-01	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-02-20	CC inactivated address + Unintended Recipient asked to return letter	N/A	2016-02-22	Contact Center	Privacy breach	None Required	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-02-01	2016-02-01	External	2016-02-01	Client's Invitation/Remi	2016-02-01	CC inactivated the address +	N/A	2016-04-06	Contact Center	Privacy breach	None Required	NO	Contact Center	N/A	Address inactivated.	2016

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				nder Letter (Screening Status/Eligibility)		Unintended Recipient to destroy letter									CC was unable to reach the client.	
2016-02-02	2016-02-02	External	2016-02-02	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-02-02	CC inactivated incorrect address	2016-02-02	2016-02-18	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center & Privacy Specialist	N/A	CC called the client and updated the address.	2016
2016-02-02	2016-02-02	External	2016-02-02	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-01-22	CC inactivated incorrect address	N/A	2016-04-04	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-02-02	2016-02-02	External	2016-02-02	Client's Result Letter (Test Result)	2016-01-29	CC inactivated incorrect address	N/A	2016-02-12	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-02-02	2016-02-02	External	2016-02-02	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-02-05	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2016-02-12	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-02-02	2016-02-02	External	2016-02-02	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-02-02	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2016-02-02	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-02-03	2016-02-03	External	2016-02-03	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-01-29	CC inactivated incorrect address	2016-02-03	2016-02-18	Contact Center	Privacy breach	None Required	YES	Contact Center & Privacy Specialist	N/A	None Required	2016
2016-02-03	2016-02-03	External	2016-02-03	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-01-22	CC inactivated incorrect address	N/A	2016-02-11	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-02-03	2016-02-03	Unclear	2016-02-03	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-02-03	Client called in to inform CC of breach. Client received the letter opened.	2016-02-03	2016-02-03	Contact Center	Privacy breach	None Required	YES	Contact Center & Privacy Specialist	2016-02-03	CC called the client and updated the address.	2016
2016-02-04	2016-02-04	External	2016-02-04	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-02-04	CC inactivated address + Unintended Recipient asked to return letter	N/A	2016-02-18	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
2016-02-04	2016-02-04	External	2016-02-04	Client's Result Letter (Test Result)	2016-02-09	CC inactivated incorrect address	2016-02-09	2016-02-18	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center & Privacy Specialist	N/A	CC called the client and updated the address.	2016
2016-02-05	2016-02-05	External	2016-02-05	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-02-19	CC inactivated incorrect address	N/A	2016-02-11	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-02-08	2016-02-08	External	2016-02-08	Client's Result Letter (Test Result)	2016-02-19	CC inactivated address + Unintended Recipient asked to return letter	2016-02-22	2016-03-04	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center & Privacy Specialist	N/A	Address updated. CC was able to contact the client via number provided by their PCP.	2016
2016-02-08	2016-02-08	External	2016-02-08	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-02-08	CC inactivated address + Unintended Recipient asked to return letter	N/A	2016-02-24	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-02-17	2016-02-17	External	2016-02-17	Lab reports containing PHI (pathology, diagnostics, screening, treatment) related to CCO programs were sent to CCO.	2016-02-17	The Manager of Laboratory Services notified the program partner/lab of the policy breach.	N/A	2016-02-17	Contact Center	Policy breach	The Manager of Laboratory Services should contact the program partner/lab and notify them of the PHI that was sent via an unauthorized method. The Contact Centre or Privacy should then shred the PHI.	NO	Contact Center	N/A	The Manager of Laboratory Services has confirmed that their partner has been notified of the policy breach. The Contact Centre or Privacy then shredded the PHI.	2016
2016-02-17	2016-02-17	External	2016-02-17	Lab reports containing PHI (pathology, diagnostics, screening, treatment) related to CCO programs were sent to CCO.	2016-02-17	The Manager of Laboratory Services notified the program partner/lab of the policy breach.	N/A	2016-02-17	Contact Center	Policy breach	The Manager of Laboratory Services should contact the program partner/lab and notify them of the PHI that was sent via an unauthorized method. The Contact Centre or Privacy should	NO	Contact Center	N/A	The Manager of Laboratory Services has confirmed that their partner has been notified of the policy breach. The Contact Centre or Privacy then shredded the PHI.	2016

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
											then shred the PHI.					
2016-02-18	2016-02-18	External	2016-02-18	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-02-12	CC inactivated incorrect address	N/A	2016-02-19	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-02-18	2016-02-18	External	2016-02-18	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-02-12	CC inactivated incorrect address	N/A	2016-02-29	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-02-18	2016-02-18	External	2016-02-18	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-02-12	CC inactivated incorrect address	N/A	2016-03-07	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-02-18	2016-02-18	External	2016-02-18	Client's Result Letter (Test Result)	2016-02-12	CC inactivated incorrect address	N/A	2016-02-23	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	CC called the client and updated the address.	2016
2016-03-02	2016-03-02	External	2016-03-02	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-03-02	CC inactivated address + Unintended Recipient asked to return letter	2016-04-20	2016-05-02	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center & Privacy Specialist	N/A	CC called the client and updated the address.	2016
2016-03-03	2016-03-03	External	2016-03-03	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-03-09	Address inactivated - Letter will not be returned	2016-03-09	2016-03-18	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center & Privacy Specialist	N/A	CC called the client and updated the address.	2016
2016-03-03	2016-03-03	External	2016-03-03	Client's Result Letter (Test Result)	2016-03-03	CC inactivated the address + Unintended Recipient to destroy letter	2016-03-07	2016-04-20	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center & Privacy Specialist	N/A	CC called the client and updated the address.	2016
2016-03-04	2016-03-04	External	2016-03-04	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-03-04	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2016-03-14	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-03-04	2016-03-04	External	2016-03-04	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-03-04	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2016-03-14	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-03-07	2016-03-07	External	2016-03-07	Client's Invitation/Reminder Letter (Screening	2016-03-07	CC inactivated address + Unintended Recipient	N/A	2016-03-21	Contact Center	Privacy breach	Contact Center to call client/PCP and	NO	Contact Center	N/A	Address inactivated. CC was unable to	2016

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				Status/Eligibility)		asked to return letter					update address.				reach the client.	
2016-03-07	2016-03-07	External	2016-03-07	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-03-04	CC inactivated incorrect address	N/A	2016-03-23	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-03-08	2016-03-08	External	2016-03-08	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-03-08	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2016-04-21	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-03-09	2016-03-09	External	2016-03-09	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-03-09	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2016-03-09	Contact Center	Privacy breach	None Required	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-03-10	2016-03-10	External	2016-03-10	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-03-10	Address inactivated - Letter will not be returned	N/A	2016-03-17	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-03-14	2016-03-14	External	2016-03-14	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-03-14	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2016-03-21	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-03-15	2016-03-15	External	2016-03-15	Lab reports containing PHI (pathology, diagnostics, screening, treatment) related to CCO programs were sent to CCO.	2016-03-15	The Manager of Laboratory Services notified the program partner/lab of the policy breach.	N/A	2016-03-15	Contact Center	Policy breach	The Manager of Laboratory Services should contact the program partner/lab and notify them of the PHI that was sent via an unauthorized method. The Contact Centre or Privacy should then shred the PHI.	NO	Contact Center	N/A	The Manager of Laboratory Services has confirmed that their partner has been notified of the policy breach. The Contact Centre or Privacy then shredded the PHI.	2016
2016-03-16	2016-03-16	External	2016-03-16	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-03-16	CC inactivated address + Unintended Recipient asked to return letter	N/A	2016-03-31	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-03-17	2016-03-17	External	2016-03-17	Client's Invitation/Reminder Letter	2016-04-01	CC inactivated address + Unintended	N/A	2016-04-01	Contact Center	Privacy breach	Contact Center to call client/PCP and	NO	Contact Center	N/A	Address inactivated. CC was	2016

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				(Screening Status/Eligibility)		Recipient asked to return letter					update address.				unable to reach the client.	
2016-03-18	2016-03-18	External	2016-03-18	Client's Result Letter (Test Result)	2016-03-18	CC inactivated incorrect address	2016-03-21	2016-04-21	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center & Privacy Specialist	N/A	CC called the client and updated the address.	2016
2016-03-18	2016-03-18	External	2016-03-18	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-03-28	CC inactivated incorrect address	N/A	2016-03-18	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-03-18	2016-03-18	External	2016-03-18	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-03-18	CC inactivated incorrect address	N/A	2016-03-22	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-03-18	2016-03-18	External	2016-03-18	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-03-18	CC inactivated incorrect address	N/A	2016-03-22	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-03-18	2016-03-18	External	2016-03-18	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-03-18	CC inactivated incorrect address	N/A	2016-03-21	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Client did not want to update address.	2016
2016-03-18	2016-03-18	External	2016-03-18	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-03-18	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2016-04-07	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-03-18	2016-03-18	External	2016-03-18	A representative from the PCP's office who is not registered as a delegate of the PCP is accessing the SAR reports, and calling the Contact Centre on behalf of the PCP.	2016-03-18	The Contact Centre agent immediately ended the discussion regarding the SAR. They informed the representative that the SAR report access constituted a privacy breach.	N/A	2016-03-18	Contact Center	Policy breach	The Contact Centre agent should advise the representative to register for a ONE ID account. They should further advise that the representative must be registered with CCO as a delegate of the PCP prior to accessing the PCP's SAR, or calling CCO about anything	NO	Contact Center	N/A	The Contact Centre agent provided feedback to the representative, who agreed to register for ONE ID. The Contact Centre agent transferred the representative to eHealth, or provided them with the eHealth phone number, so that they could be registered	2016

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
											related to the SAR.				for a ONE ID account.	
2016-03-21	2016-03-21	External	2016-03-21	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-03-16	CC inactivated incorrect address	N/A	2016-03-23	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-03-21	2016-03-21	External	2016-03-21	Client's Result Letter (Test Result)	2016-03-16	CC inactivated incorrect address	N/A	2016-03-24	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-03-22	2016-03-22	External	2016-03-22	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-03-22	CC inactivated address + Unintended Recipient asked to return letter	N/A	2016-03-24	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-03-22	2016-03-22	External	2016-03-22	Client's Result Letter (Test Result)	2016-03-22	CC inactivated the address + Unintended Recipient to destroy letter	N/A	N/A	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	N/A	Contact Center	N/A	CC called the client and updated the address.	2016
2016-03-23	2016-03-23	External	2016-03-23	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-03-23	CC inactivated address + Unintended Recipient asked to return letter	N/A	2016-04-26	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-03-23	2016-03-23	External	2016-03-23	Client's Result Letter (Test Result)	2016-03-23	CC inactivated incorrect address	N/A	2016-03-28	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-03-23	2016-03-23	External	2016-03-23	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-03-24	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2016-03-24	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-03-23	2016-03-23	External	2016-03-23	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-03-24	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2016-03-24	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-03-24	2016-03-24	External	2016-03-24	Client PHI intended for a CCO screening program was provided to CCO by a PCP, in electronic,	2016-03-24	Privacy uploaded the fax to an activity in InScreen. Privacy had been the original recipient of the	N/A	2016-04-12	Contact Center & Privacy Specialist	Policy breach	The Contact Centre agent should call the PCP and inform them of the policy breach. For misdirected requests, the	NO	Contact Center & Privacy Specialist	N/A	The PCP was notified of the policy breach, and about the policy on client PHI maintenance.	2016

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				voicemail, or paper form.		PHI, and had hard deleted the fax containing PHI from CCO's systems.					agent should re-direct the PCP to the appropriate recipient of these requests (e.g., Ontario Breast Screening Program High Risk site) and advise them to not send PHI to CCO for such requests.					
2016-03-28	2016-03-28	External	2016-03-28	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-03-29	CC inactivated address + Unintended Recipient asked to return letter	N/A	2016-04-05	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-03-28	2016-03-28	External	2016-03-28	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-03-28	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2016-04-05	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-03-28	2016-03-28	External	2016-03-28	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-03-28	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2016-04-05	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-03-30	2016-03-30	External	2016-03-30	Lab reports containing PHI (pathology, diagnostics, screening, treatment) related to CCO programs were sent to CCO.	2016-03-30	Privacy uploaded the fax to an activity in InScreen. Privacy had been the original recipient of the PHI, and had hard deleted the fax containing PHI from CCO's systems.	N/A	2016-04-22	Contact Center & Privacy Specialist	Policy breach	The Contact Centre agent should inform the relevant CCO Program Manager of the policy breach right away. They should work with the CCO program and Privacy team to determine whether there is an alternative secure fax option, and whether safeguards are in place to protect incoming PHI. The Contact	NO	Contact Center & Privacy Specialist	N/A	The applicable program was notified, and relevant safeguards were put in place to protect incoming PHI. The Contact Centre agent notified the sender of the policy breach.	2016

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
											Centre agent should also notify the sender of the policy breach, and request that the Lab Manager or the agent call the lab.					
2016-03-30	2016-03-30	External	2016-03-30	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-03-30	CC inactivated the address + Unintended Recipient to destroy letter	2016-04-05	2016-04-05	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center & Privacy Specialist	N/A	CC called the client and updated the address.	2016
2016-04-01	2016-04-01	External	2016-04-01	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-04-01	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2016-04-11	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-04-04	2016-04-04	Internal	2016-04-04	Client's Result Letter (Test Result)	2016-04-04	CC received returned letter, which had been opened. No contact information for the unintended recipient available, therefore no containment possible. CC destroyed letter.	N/A	N/A	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center	2016-05-30	Address updated. CC was able to contact the client via number provided by their PCP.	2016
2016-04-04	2016-04-04	External	2016-04-13	Screening-related status/confirmation of PHI (i.e., policy breaches where the Contact Centre agent did not authenticate as per standard operating procedures)	2016-04-13	The Contact Centre agent logged the internal policy breach in InScreen.	N/A	2016-04-13	Contact Center	Policy breach	The Contact Centre Management should coach the relevant agent on standard operating procedures for authenticating clients and for PHI disclosure.	NO	Contact Center	N/A	The Contact Centre agent received appropriate coaching from the Contact Centre Management.	2016
2016-04-04	2016-04-04	External	2016-04-04	Client's Result Letter (Test Result)	2016-04-04	CC inactivated the address + Unintended Recipient to destroy letter	2016-04-06	2016-04-14	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center & Privacy Specialist	N/A	CC called the client and updated the address.	2016
2016-04-06	2016-04-06	External	2016-04-06	Client's Invitation/Remi	2016-04-06	CC inactivated address +	N/A	2016-04-08	Contact Center	Privacy breach	Contact Center to call	NO	Contact Center	N/A	Address inactivated.	2016

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				nder Letter (Screening Status/Eligibility)		Unintended Recipient asked to return letter					client/PCP and update address.				CC was unable to reach the client.	
2016-04-07	2016-04-07	External	2016-04-07	Client PHI intended for a CCO screening program was provided to CCO by a PCP, in electronic, voicemail, or paper form.	2016-04-07	Privacy uploaded the fax to an activity in InScreen. Privacy had been the original recipient of the PHI, and had hard deleted the fax containing PHI from CCO's systems.	N/A	2016-04-11	Contact Center & Privacy Specialist	Policy breach	The Contact Centre agent should call the PCP and inform them of the policy breach. For misdirected requests, the agent should re-direct the PCP to the appropriate recipient of these requests (e.g., Ontario Breast Screening Program High Risk site) and advise them to not send PHI to CCO for such requests.	NO	Contact Center & Privacy Specialist	N/A	The PCP was notified of the policy breach, and about the policy on client PHI maintenance.	2016
2016-04-07	2016-04-07	External	2016-04-07	Client's Result Letter (Test Result)	2016-04-08	CC inactivated incorrect address	2016-04-08	2016-04-19	Contact Center	Privacy breach	None Required	YES	Contact Center & Privacy Specialist	N/A	CC called the client and updated the address.	2016
2016-04-08	2016-04-08	External	2016-04-08	Client PHI intended for a CCO screening program was provided to CCO by a PCP, in electronic, voicemail, or paper form.	2016-04-08	Privacy uploaded the fax to an activity in InScreen. Privacy had been the original recipient of the PHI, and had hard deleted the fax containing PHI from CCO's systems.	N/A	2016-04-08	Contact Center & Privacy Specialist	Policy breach	The Contact Centre agent should call the PCP and inform them of the policy breach. For misdirected requests, the agent should re-direct the PCP to the appropriate recipient of these requests (e.g., Ontario Breast Screening Program High Risk site) and advise them to not send PHI to CCO for such requests.	NO	Contact Center & Privacy Specialist	N/A	The PCP was notified of the policy breach, and about the policy on client PHI maintenance.	2016
2016-04-08	2016-04-08	External	2016-04-08	Client's Invitation/Remi	2016-04-08	CC inactivated the address +	N/A	2016-04-08	Contact Center	Privacy breach	Contact Center to call	NO	Contact Center	N/A	Address inactivated.	2016

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				nder Letter (Screening Status/Eligibility)		Unintended Recipient to destroy letter					client/PCP and update address.				CC was unable to reach the client.	
2016-04-12	2016-04-12	External	2016-04-12	Client's Result Letter (Test Result)	2016-04-12	CC inactivated address + Unintended Recipient asked to return letter	N/A	2016-04-27	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-04-13	2016-04-13	External	2016-04-13	Client PHI intended for a CCO screening program was provided to CCO by a PCP, in electronic, voicemail, or paper form.	2016-04-13	The Contact Centre agent uploaded the voicemail to an activity in InScreen, and hard deleted the voicemail from CCO's systems.	N/A	2016-04-13	Contact Center	Policy breach	The Contact Centre agent should call the PCP and inform them of the policy breach. For misdirected requests, the agent should re-direct the PCP to the appropriate recipient of these requests (e.g., Ontario Breast Screening Program High Risk site) and advise them to not send PHI to CCO for such requests.	NO	Contact Center	N/A	The PCP was notified of the policy breach, and about the policy on client PHI maintenance.	2016
2016-04-15	2016-04-15	External	2016-04-15	Client's Result Letter (Test Result)	2016-04-15	CC inactivated incorrect address	2016-04-15	2016-04-15	Contact Center	Privacy breach	None Required	YES	Contact Center & Privacy Specialist	N/A	CC called the client and updated the address.	2016
2016-04-15	2016-04-18	External	2016-04-18	Screening-related status/confirmation of PHI (i.e., policy breaches where the Contact Centre agent did not authenticate as per standard operating procedures)	2016-04-18	The Contact Centre agent logged the internal policy breach in InScreen.	N/A	2016-04-18	Contact Center	Policy breach	The Contact Centre Management should coach the relevant agent on standard operating procedures for authenticating clients and for PHI disclosure.	NO	Contact Center	N/A	The Contact Centre agent received appropriate coaching from the Contact Centre Management.	2016
2016-04-15	2016-04-18	External	2016-04-18	Screening-related status/confirmation of PHI (i.e., policy	2016-04-18	The Contact Centre agent logged the internal policy	N/A	2016-04-18	Contact Center	Policy breach	The Contact Centre Management should coach the relevant	NO	Contact Center	N/A	The Contact Centre agent received appropriate coaching from	2016

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				breaches where the Contact Centre agent did not authenticate as per standard operating procedures)		breach in InScreen.					agent on standard operating procedures for authenticating clients and for PHI disclosure.				the Contact Centre Management.	
2016-04-19	2016-04-19	External	2016-04-19	Client's Result Letter (Test Result)	2016-04-20	CC inactivated address + Unintended Recipient asked to return letter	2016-04-20	2016-05-13	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center & Privacy Specialist	N/A	CC called the client and updated the address.	2016
2016-04-20	2016-04-20	External	2016-04-20	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-04-15	CC inactivated incorrect address	N/A	2016-04-27	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-04-20	2016-04-20	External	2016-04-20	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-04-15	CC inactivated incorrect address	N/A	2016-05-04	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-04-20	2016-04-20	External	2016-04-20	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-04-15	CC inactivated incorrect address	N/A	2016-05-19	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-04-20	2016-04-20	External	2016-04-20	Client's Result Letter (Test Result)	2016-04-15	CC inactivated incorrect address	N/A	2016-05-04	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-04-20	2016-04-20	External	2016-04-20	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-04-21	CC inactivated incorrect address	N/A	2016-04-21	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Client did not want to update address.	2016
2016-04-22	2016-04-22	External	2016-04-22	Client PHI intended for a CCO screening program was provided to CCO by a PCP, in electronic, voicemail, or paper form.	2016-04-22	Privacy uploaded the fax to an activity in InScreen. Privacy had been the original recipient of the PHI, and had hard deleted the fax	N/A	2016-04-22	Contact Center	Policy breach	The Contact Centre agent should call the PCP and inform them of the policy breach. For misdirected requests, the agent should re-direct the PCP to the	NO	Contact Center	N/A	The PCP was notified of the policy breach, and about the policy on client PHI maintenance.	2016

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
						containing PHI from CCO's systems.					appropriate recipient of these requests (e.g., Ontario Breast Screening Program High Risk site) and advise them to not send PHI to CCO for such requests.					
2016-04-22	2016-04-22	External	2016-04-22	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-05-30	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2016-04-28	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-04-29	2016-04-29	External	2016-04-29	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-04-29	CC inactivated address + Unintended Recipient asked to return letter	N/A	2016-05-10	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-04-29	2016-04-29	External	2016-04-29	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-04-29	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2016-04-28	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-05-02	2016-05-02	External	2016-05-02	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-05-02	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2016-05-09	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-05-02	2016-05-02	Internal	2016-05-02	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	N/A	Unintended recipient notified CC of breach. They opened the letter. They refused to shred or mail the misdirected correspondence back to CCO. The CC Agent had to hang up on the recipient due to verbal abuse.	2016-05-02	2016-05-06	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center & Privacy Specialist	N/A	CC called the client and updated the address.	2016
2016-05-03	2016-05-03	External	2016-05-03	Client's Result Letter (Test Result)	2016-04-20	CC inactivated address + Unintended Recipient	2016-05-03	2016-05-13	Contact Center	Privacy breach	Contact Center to call client/PCP and	NO	Contact Center	N/A	CC called the client and updated the address.	2016

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
						asked to return letter					update address.					
2016-05-05	2016-05-05	External	2016-05-05	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-05-16	CC inactivated address + Unintended Recipient asked to return letter	N/A	2016-05-19	Contact Center	Privacy breach	None Required	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-05-05	2016-05-05	External	2016-05-05	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-04-26	CC inactivated incorrect address	2016-05-17	2016-05-26	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center	N/A	CC called the client and updated the address.	2016
2016-05-05	2016-05-05	External	2016-05-05	Client's Result Letter (Test Result)	2016-04-26	CC inactivated incorrect address	N/A	2016-05-10	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Client did not want to update address.	2016
2016-05-05	2016-05-05	External	2016-05-05	Client's Result Letter (Test Result)	2016-04-26	CC inactivated the address + Unintended Recipient to destroy letter	2016-05-05	2016-05-06	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center & Privacy Specialist	N/A	CC called the client and updated the address.	2016
2016-05-05	2016-05-05	Internal	2016-05-05	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-05-05	Unintended recipient notified CC that the client moved. They had opened the letter. The CC Agent forgot to ask the unintended recipient to shred or return the correspondence, but did not have the unintended recipient's contact information on file. Further containment is not possible.	N/A	2016-05-05	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client. CC Agent was reminded of standard operating procedures.	2016
2016-05-06	2016-05-06	External	2016-05-06	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-05-06	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2016-05-19	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-05-09	2016-05-09	External	2016-05-09	Screening-related status/confirmation of PHI (i.e., policy	2016-05-09	The Contact Centre agent logged the internal policy	N/A	2016-05-09	Contact Center	Policy breach	The Contact Centre Management should coach the relevant	NO	Contact Center	N/A	The Manager of Laboratory Services has confirmed that their partner	2016

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				breaches where the Contact Centre agent did not authenticate as per standard operating procedures)		breach in InScreen.					agent on standard operating procedures for authenticating clients and for PHI disclosure.				has been notified of the policy breach. The Contact Centre or Privacy then shredded the PHI.	
2016-05-09	2016-05-09	External	2016-05-09	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-05-09	CC inactivated address + Unintended Recipient asked to return letter	N/A	2016-05-16	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-05-09	2016-05-09	External	2016-05-09	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-05-09	CC inactivated address + Unintended Recipient asked to return letter	N/A	2016-05-25	Contact Center	Privacy breach	None Required	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-05-10	2016-05-10	External	2016-05-10	Lab reports containing PHI (pathology, diagnostics, screening, treatment) related to CCO programs were sent to CCO.	2016-05-10	The Contact Centre agent logged the internal policy breach in InScreen.	N/A	2016-05-10	Contact Center	Policy breach	The Contact Centre Management should coach the relevant agent on standard operating procedures for authenticating clients and for PHI disclosure.	NO	Contact Center	N/A	The Contact Centre agent received appropriate coaching from the Contact Centre Management.	2016
2016-05-10	2016-05-10	External	2016-05-10	Client's Result Letter (Test Result)	2016-05-10	CC inactivated address + Unintended Recipient asked to return letter	N/A	2016-05-24	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-05-10	2016-05-10	External	2016-05-10	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-05-04	CC inactivated incorrect address	N/A	2016-05-13	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-05-10	2016-05-10	External	2016-05-10	Client's Result Letter (Test Result)	2016-05-04	CC inactivated incorrect address	N/A	2016-05-13	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-05-12	2016-05-12	External	2016-05-12	Screening-related status/confirmation of PHI (i.e., policy	2016-05-12	The Contact Centre agent logged the internal policy	N/A	2016-05-12	Contact Center	Policy breach	The Contact Centre Management should coach the relevant	NO	Contact Center	N/A	The Contact Centre agent received appropriate coaching from	2016

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				breaches where the Contact Centre agent did not authenticate as per standard operating procedures)		breach in InScreen.					agent on standard operating procedures for authenticating clients and for PHI disclosure.				the Contact Centre Management.	
2016-05-12	2016-05-12	External	2016-05-12	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-04-26	CC inactivated incorrect address	2016-05-13	2016-05-30	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center & Privacy Specialist	N/A	CC called the client and updated the address.	2016
2016-05-12	2016-05-12	External	2016-05-12	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-05-12	CC inactivated incorrect address	N/A	2016-05-24	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-05-12	2016-05-12	External	2016-05-12	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-04-21	CC inactivated incorrect address	N/A	2016-05-17	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-05-13	2016-05-13	External	2016-05-13	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-04-21	CC inactivated incorrect address	N/A	2016-06-02	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-05-16	2016-05-16	External	2016-05-16	Screening-related status/confirmation of PHI (i.e., policy breaches where the Contact Centre agent did not authenticate as per standard operating procedures)	2016-05-18	The Contact Centre agent logged the internal policy breach in InScreen.	N/A	2016-05-18	Contact Center	Policy breach	The Contact Centre Management should coach the relevant agent on standard operating procedures for authenticating clients and for PHI disclosure.	NO	Contact Center	N/A	The Contact Centre agent received appropriate coaching from the Contact Centre Management.	2016
2016-05-16	2016-05-16	External	2016-05-16	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-09-02	CC inactivated incorrect address	N/A	2016-05-16	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
2016-05-16	2016-05-16	External	2016-05-16	Client's Result Letter (Test Result)	2016-05-04	CC inactivated incorrect address	N/A	2016-05-20	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	CC called the client and updated the address.	2016
2016-05-16	2016-05-16	External	2016-05-16	Client's Result Letter (Test Result)	2016-03-22	CC inactivated incorrect address	N/A	2016-05-24	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Client did not want to update address.	2016
2016-05-16	2016-05-16	External	2016-05-17	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-05-17	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2016-05-17	Contact Center	Privacy breach	None Required	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-05-17	2016-05-17	External	2016-05-17	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-05-17	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2016-05-17	Contact Center	Privacy breach	None Required	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-05-17	2016-06-02	External	2016-06-02	Screening-related status/confirmation of PHI (i.e., policy breaches where the Contact Centre agent did not authenticate as per standard operating procedures)	2016-06-02	The Contact Centre agent logged the internal policy breach in InScreen.	N/A	2016-06-02	Contact Center	Policy breach	The Contact Centre Management should coach the relevant agent on standard operating procedures for authenticating clients and for PHI disclosure.	NO	Contact Center	N/A	The Contact Centre agent received appropriate coaching from the Contact Centre Management.	2016
2016-05-18	2016-05-18	External	2016-05-18	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-05-18	CC inactivated incorrect address	N/A	2016-05-18	Contact Center	Privacy breach	None Required	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-05-18	2016-05-18	External	2016-05-18	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-05-18	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2016-06-02	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-05-19	2016-05-19	External	2016-05-19	Client's Result Letter (Test Result)	2016-05-10	CC inactivated address + Unintended Recipient asked to return letter	N/A	2016-05-30	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	CC called the client and updated the address.	2016
2016-05-25	2016-05-25	External	2016-05-25	Client's Result Letter (Test Result)	2016-05-18	CC inactivated incorrect address	2016-05-25	2016-05-30	Contact Center	Privacy breach	Contact Center to call client/PCP and	YES	Contact Center &	N/A	CC called the client and	2016

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
											update address.		Privacy Specialist		updated the address.	
2016-05-25	2016-05-25	External	2016-05-25	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-05-20	CC inactivated incorrect address	2016-05-26	2016-05-27	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center & Privacy Specialist	N/A	CC called the client and updated the address.	2016
2016-05-25	2016-05-25	External	2016-05-25	Client's Result Letter (Test Result)	2016-05-18	CC inactivated incorrect address	N/A	2016-05-27	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-05-25	2016-05-25	External	2016-05-25	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-05-18	CC inactivated incorrect address	N/A	2016-05-25	Contact Center	Privacy breach	None Required	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-05-25	2016-05-25	External	2016-05-25	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-05-25	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2016-06-02	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-05-30	2016-05-30	External	2016-05-30	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-05-31	CC inactivated incorrect address	2016-06-01	2016-06-03	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center & Privacy Specialist	N/A	CC called the client and updated the address.	2016
2016-05-30	2016-05-30	External	2016-05-30	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-05-20	CC inactivated incorrect address	N/A	2016-06-15	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-05-30	2016-05-30	External	2016-05-30	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-05-30	CC inactivated incorrect address	N/A	2016-05-30	Contact Center	Privacy breach	None Required	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-06-01	2016-06-01	External	2016-06-01	Screening-related status/confirmation of PHI (i.e., policy breaches where the Contact Centre agent did not authenticate as per standard	2016-06-01	The Contact Centre agent logged the internal policy breach in InScreen.	2016-06-01	2016-06-01	Contact Center	Policy breach	The Contact Centre Management should coach the relevant agent on standard operating procedures for authenticating clients and for PHI disclosure.	NO	Contact Center	N/A	The Contact Centre agent received appropriate coaching from the Contact Centre Management.	2016

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				operating procedures)												
2016-06-01	2016-06-01	External	2016-06-01	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-05-18	CC inactivated incorrect address	N/A	2016-06-08	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-06-02	2016-06-02	External	2016-06-02	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-06-02	CC inactivated incorrect address	2016-06-02	2016-06-20	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center & Privacy Specialist	N/A	CC called the client and updated the address.	2016
2016-06-02	2016-06-02	External	2016-06-02	Client's Result Letter (Test Result)	2016-06-02	CC inactivated incorrect address	2016-06-03	2016-06-03	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center & Privacy Specialist	N/A	CC called the client and updated the address.	2016
2016-06-02	2016-06-02	External	2016-06-02	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-06-02	CC inactivated incorrect address	N/A	2016-06-14	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to obtain client's phone number from PCP.	2016
2016-06-02	2016-06-02	External	2016-06-02	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-06-02	CC inactivated incorrect address	N/A	2016-06-09	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-06-02	2016-06-02	External	2016-06-02	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-06-02	CC inactivated incorrect address	N/A	2016-06-02	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-06-02	2016-06-02	External	2016-06-02	Client's Result Letter (Test Result)	2016-05-04	CC inactivated incorrect address	N/A	2016-06-08	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-06-03	2016-06-03	External	2016-06-03	Screening-related status/confirmation of PHI (i.e., policy breaches where the Contact Centre agent did not authenticate as per standard	2016-06-03	The Contact Centre agent logged the internal policy breach in InScreen.	N/A	2016-06-03	Contact Center	Policy breach	The Contact Centre Management should coach the relevant agent on standard operating procedures for authenticating clients and for PHI disclosure.	NO	Contact Center	N/A	The Contact Centre agent received appropriate coaching from the Contact Centre Management.	2016

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				operating procedures)												
2016-06-06	2016-06-06	External	2016-06-06	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-06-02	CC inactivated incorrect address	N/A	2016-06-07	Contact Center	Privacy breach	None Required	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-06-08	2016-06-08	External	2016-06-08	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-06-08	CC inactivated address + Unintended Recipient asked to return letter	N/A	2016-06-17	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to obtain client's phone number from PCP.	2016
2016-06-08	2016-06-08	External	2016-06-08	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-06-08	CC inactivated address + Unintended Recipient asked to return letter	N/A	2016-06-21	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-06-08	2016-06-08	External	2016-06-08	Client's Result Letter (Test Result)	2016-06-08	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2016-06-15	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Client did not want to update address.	2016
2016-06-13	2016-06-13	External	2016-06-13	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-06-13	CC inactivated address + Unintended Recipient asked to return letter	N/A	2016-08-19	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-06-13	2016-06-13	External	2016-06-13	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-06-13	CC inactivated address + Unintended Recipient asked to return letter	N/A	2016-06-28	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-06-14	2016-06-14	External	2016-06-14	Client's Result Letter (Test Result)	2016-06-14	CC inactivated address + Unintended Recipient asked to return letter	N/A	2016-07-27	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-06-16	2016-06-16	External	2016-06-16	Client's Invitation/Reminder Letter (Screening	2016-06-30	CC inactivated the address + Unintended	N/A	2016-07-18	Contact Center	Privacy breach	Contact Center to call client/PCP and	NO	Contact Center	N/A	CC called the client and updated the address.	2016

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				Status/Eligibility)		Recipient to destroy letter					update address.					
2016-06-22	2016-06-22	External	2016-06-22	Client PHI intended for a CCO screening program was provided to CCO by a PCP, in electronic, voicemail, or paper form.	2016-06-28	Privacy uploaded the fax to an activity in InScreen. Privacy had been the original recipient of the PHI, and had hard deleted the fax containing PHI from CCO's systems.	N/A	2016-06-22	Contact Center & Privacy Specialist	Policy breach	The Contact Centre agent should call the PCP and inform them of the policy breach. For misdirected requests, the agent should re-direct the PCP to the appropriate recipient of these requests (e.g., Ontario Breast Screening Program High Risk site) and advise them to not send PHI to CCO for such requests.	NO	Contact Center	N/A	The PCP was notified of the policy breach, and about the policy on client PHI maintenance.	2016
2016-06-22	2016-06-22	External	2016-06-22	Client PHI intended for a CCO screening program was provided to CCO by a PCP, in electronic, voicemail, or paper form.	2016-06-28	Privacy uploaded the fax to an activity in InScreen. Privacy had been the original recipient of the PHI, and had hard deleted the fax containing PHI from CCO's systems.	N/A	2016-06-28	Contact Center & Privacy Specialist	Policy breach	The Contact Centre agent should call the PCP and inform them of the policy breach. For misdirected requests, the agent should re-direct the PCP to the appropriate recipient of these requests (e.g., Ontario Breast Screening Program High Risk site) and advise them to not send PHI to CCO for such requests.	NO	Contact Center	N/A	The PCP was notified of the policy breach, and about the policy on client PHI maintenance.	2016
2016-06-22	2016-06-22	External	2016-06-24	Client PHI intended for a CCO screening program was provided to	2016-06-24	Privacy uploaded the fax to an activity in InScreen. Privacy had	N/A	2016-06-24	Contact Center & Privacy Specialist	Policy breach	The Contact Centre agent should call the PCP and inform them of the policy	NO	Contact Center	N/A	The PCP was notified of the policy breach, and about the policy on client	2016

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				CCO by a PCP, in electronic, voicemail, or paper form.		been the original recipient of the PHI, and had hard deleted the fax containing PHI from CCO's systems.					breach. For misdirected requests, the agent should re-direct the PCP to the appropriate recipient of these requests (e.g., Ontario Breast Screening Program High Risk site) and advise them to not send PHI to CCO for such requests.				PHI maintenance.	
2016-06-23	2016-06-23	External	2016-06-23	Client PHI intended for a CCO screening program was provided to CCO by a PCP, in electronic, voicemail, or paper form.	2016-06-23	Privacy uploaded the fax to an activity in InScreen. Privacy had been the original recipient of the PHI, and had hard deleted the fax containing PHI from CCO's systems.	N/A	2016-06-23	Contact Center & Privacy Specialist	Policy breach	The Contact Centre agent should call the PCP and inform them of the policy breach. For misdirected requests, the agent should re-direct the PCP to the appropriate recipient of these requests (e.g., Ontario Breast Screening Program High Risk site) and advise them to not send PHI to CCO for such requests.	NO	Contact Center	N/A	The PCP was notified of the policy breach, and about the policy on client PHI maintenance.	2016
2016-06-24	2016-06-24	External	2016-06-24	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-06-24	CC inactivated address + Unintended Recipient asked to return letter	N/A	2016-08-10	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-06-29	2016-06-29	External	2016-06-29	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-06-29	CC inactivated address + Unintended Recipient asked to return letter	2016-07-06	2016-08-16	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center & Privacy Specialist	N/A	CC called the client and updated the address.	2016
2016-07-04	2016-07-04	External	2016-07-04	Client's Invitation/Reminder Letter (Screening	2016-07-04	CC inactivated address + Unintended Recipient	N/A	2016-07-11	Contact Center	Privacy breach	Contact Center to call client/PCP and	NO	Contact Center	N/A	Address inactivated. CC was unable to	2016

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				Status/Eligibility)		asked to return letter					update address.				reach the client.	
2016-07-05	2016-07-05	External	N/A	An Ontario Breast Screening Program high risk requisition form was faxed to CCO's main fax line.	2016-07-05	Privacy uploaded the fax to an activity in InScreen. Privacy had been the original recipient of the PHI, and had hard deleted the fax containing PHI from CCO's systems.	N/A	2017-06-06	Contact Center	Policy breach	The Contact Centre agent should call the PCP and inform them of the policy breach. For misdirected requests, the agent should re-direct the PCP to the appropriate recipient of these requests (e.g., Ontario Breast Screening Program High Risk site) and advise them to not send PHI to CCO for such requests.	NO	Contact Center	N/A	CC followed up with the PCP.	2016
2016-07-08	2016-07-08	Internal	2016-07-08	Cannot be determined	2016-07-08	PHI was disclosed through an insecure method. Records of the conversation with identifying information have not been retained.	N/A	2016-07-08	Contact Center	Policy breach	The Contact Centre Management should coach the relevant agent on standard operating procedures for authenticating clients and for PHI disclosure. Privacy Specialist should be more cautious going forward as well. If there is a possibility that PHI may be discussed they should use a secure medium of communication.	NO	Contact Center	N/A	The Contact Centre agent received appropriate coaching from the Contact Centre Management. Privacy Specialist will try to be more careful, and will try not to ask questions that would lead to inadvertent disclosure of PHI over an insecure medium.	2016

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
2016-07-13	2016-07-13	External	2016-07-13	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-07-13	CC inactivated incorrect address	2016-07-13	2016-07-19	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center & Privacy Specialist	N/A	CC called the client and updated the address.	2016
2016-07-13	2016-07-13	External	2016-07-13	Client's Result Letter (Test Result)	2016-07-13	CC inactivated incorrect address	2016-07-22	2016-07-29	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	YES	Contact Center & Privacy Specialist	N/A	CC called the client and updated the address.	2016
2016-07-13	2016-07-13	External	2016-07-13	Client's Result Letter (Test Result)	2016-07-13	CC inactivated incorrect address	N/A	2016-07-15	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-07-13	2016-07-13	External	2016-07-13	Client's Result Letter (Test Result)	2016-07-13	CC inactivated incorrect address	N/A	2016-07-13	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	CC called the client and updated the address.	2016
2016-07-14	2016-07-14	External	2016-07-14	Client PHI intended for a CCO screening program was provided to CCO by a PCP, in electronic, voicemail, or paper form.	2016-07-14	Privacy uploaded the fax to an activity in InScreen. Privacy had been the original recipient of the PHI, and had hard deleted the fax containing PHI from CCO's systems.	N/A	2016-07-14	Contact Center	Policy breach	The Contact Centre agent should call the PCP and inform them of the policy breach. For misdirected requests, the agent should re-direct the PCP to the appropriate recipient of these requests (e.g., Ontario Breast Screening Program High Risk site) and advise them to not send PHI to CCO for such requests.	NO	Contact Center	N/A	The PCP was notified of the policy breach, and about the policy on client PHI maintenance.	2016
2016-07-14	2016-07-14	External	2016-07-14	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-07-14	CC inactivated incorrect address	N/A	2016-07-21	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-07-14	2016-07-14	External	2016-07-14	Client's Invitation/Reminder Letter (Screening	2016-07-14	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2016-07-14	Contact Center	Privacy breach	None Required	NO	Contact Center	N/A	Address inactivated. CC was unable to	2016

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				Status/Eligibility)											reach the client.	
2016-07-15	2016-07-15	External	2016-07-15	Client's Result Letter (Test Result)	2016-07-18	Address inactivated - Letter will not be returned	2016-07-15	2016-08-15	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center & Privacy Specialist	N/A	CC called the client and updated the address.	2016
2016-07-19	2016-07-19	External	2016-07-19	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-07-18	CC inactivated incorrect address	N/A	2016-07-18	Contact Center	Privacy breach	None Required	NO	Contact Center	N/A	Address updated. CC was able to contact the client via number provided by their PCP.	2016
2016-07-21	2016-07-21	External	2016-07-21	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-07-25	CC inactivated address + Unintended Recipient asked to return letter	N/A	2016-08-15	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-07-21	2016-07-21	Unclear	2016-07-21	Client's Result Letter (Test Result)	2016-07-21	Client notified CC of breach. An unintended recipient found their letter opened, and returned it to them.	N/A	2016-07-21	Contact Center	Privacy breach	None Required	NO	Contact Center	N/A	None Required	2016
2016-07-25	2016-07-25	External	2016-07-25	A representative from the PCP's office who is not registered as a delegate of the PCP is accessing the SAR reports, and calling the Contact Centre on behalf of the PCP.	2016-07-25	The Contact Centre agent immediately ended the discussion regarding the SAR. They informed the representative that the SAR report access constituted a privacy breach.	N/A	2016-07-29	Contact Center	Privacy breach	The Contact Centre agent should advise the representative to register for a ONE ID account. They should further advise that the representative must be registered with CCO as a delegate of the PCP prior to accessing the PCP's SAR, or calling CCO about anything related to the SAR.	NO	Contact Center	N/A	The Contact Centre agent provided feedback to the representative, who agreed to register for ONE ID. The Contact Centre agent transferred the representative to eHealth, or provided them with the eHealth phone number, so that they could be registered for a ONE ID account.	2016
2016-07-26	2016-07-26	External	2016-07-26	Client's Result Letter (Test Result)	2016-07-26	CC inactivated incorrect address	N/A	2016-07-26	Contact Center	Privacy breach	None Required	NO	Contact Center	N/A	None Required	2016

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
2016-07-29	2016-07-29	External	2016-07-29	Client PHI intended for a CCO screening program was provided to CCO by a PCP, in electronic, voicemail, or paper form.	2016-07-29	Privacy uploaded the fax to an activity in InScreen. Privacy had been the original recipient of the PHI, and had hard deleted the fax containing PHI from CCO's systems.	N/A	2016-07-29	Contact Center & Privacy Specialist	Policy breach	The Contact Centre agent should call the PCP and inform them of the policy breach. For misdirected requests, the agent should re-direct the PCP to the appropriate recipient of these requests (e.g., Ontario Breast Screening Program High Risk site) and advise them to not send PHI to CCO for such requests.	NO	Contact Center & Privacy Specialist	N/A	The PCP was notified of the policy breach, and about the policy on client PHI maintenance.	2016
2016-07-29	2016-07-29	External	2016-07-29	Client's Result Letter (Test Result)	2016-07-29	CC inactivated incorrect address	N/A	2016-08-15	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to obtain client's phone number from PCP.	2016
2016-08-02	2016-08-02	External	2016-08-02	Client's Result Letter (Test Result)	2016-08-02	CC inactivated incorrect address	N/A	2016-08-02	Contact Center	Privacy breach	None Required	NO	Contact Center	N/A	CC called the client and updated the address.	2016
2016-08-04	2016-08-04	External	2016-08-04	Client's Result Letter (Test Result)	2016-08-04	CC inactivated address + Unintended Recipient asked to return letter	N/A	2016-08-16	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-08-09	2016-08-09	External	2016-08-09	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-08-09	CC inactivated address + Unintended Recipient asked to return letter	N/A	2016-08-15	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-08-09	2016-08-09	External	2016-08-11	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-08-09	CC inactivated address + Unintended Recipient asked to return letter	N/A	2016-08-11	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to obtain client's phone number from PCP.	2016

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
2016-08-09	2016-08-09	External	2016-08-09	A representative from the PCP's office who is not registered as a delegate of the PCP is accessing the SAR reports, and calling the Contact Centre on behalf of the PCP.	2016-08-09	The Contact Centre agent immediately ended the discussion regarding the SAR. They informed the representative that the SAR report access constituted a privacy breach.	N/A	2016-08-09	Contact Center	Privacy breach	The Contact Centre agent should advise the representative to register for a ONE ID account. They should further advise that the representative must be registered with CCO as a delegate of the PCP prior to accessing the PCP's SAR, or calling CCO about anything related to the SAR.	NO	Contact Center	N/A	The Contact Centre agent provided feedback to the representative, who agreed to register for ONE ID. The Contact Centre agent transferred the representative to eHealth, or provided them with the eHealth phone number, so that they could be registered for a ONE ID account.	2016
2016-08-09	2016-08-09	External	2016-08-09	A representative from the PCP's office who is not registered as a delegate of the PCP is accessing the SAR reports, and calling the Contact Centre on behalf of the PCP.	2016-08-09	The Contact Centre agent immediately ended the discussion regarding the SAR. They informed the representative that the SAR report access constituted a privacy breach.	N/A	2016-08-09	Contact Center	Privacy breach	The Contact Centre agent should advise the representative to register for a ONE ID account. They should further advise that the representative must be registered with CCO as a delegate of the PCP prior to accessing the PCP's SAR, or calling CCO about anything related to the SAR.	NO	Contact Center	N/A	The Contact Centre agent provided feedback to the representative, who agreed to register for ONE ID. The Contact Centre agent transferred the representative to eHealth, or provided them with the eHealth phone number, so that they could be registered for a ONE ID account.	2016
2016-08-10	2016-08-10	External	2016-08-10	A representative from the PCP's office who is not registered as a delegate of the PCP is accessing the SAR reports, and calling the Contact Centre on	2016-08-10	The Contact Centre agent immediately ended the discussion regarding the SAR. They informed the representative that the SAR report access constituted a privacy breach.	N/A	2016-08-10	Contact Center	Privacy breach	The Contact Centre agent should advise the representative to register for a ONE ID account. They should further advise that the representative must be registered with CCO as a	NO	Contact Center	N/A	The Contact Centre agent provided feedback to the representative, who did not wish to be registered for ONE ID. The Contact Centre agent reiterated the authentication	2016

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				behalf of the PCP.							delegate of the PCP prior to accessing the PCP's SAR, or calling CCO about anything related to the SAR.				requirements and let the representative know that they must have delegate status in order to access the SAR. The Contact Centre agent followed up with the PCP to inform them of the breach.	
2016-08-11	2016-08-11	External	2016-08-11	Client's Result Letter (Test Result)	2016-08-11	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2016-08-11	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-08-11	2016-08-11	External	2016-08-11	A representative from the PCP's office who is not registered as a delegate of the PCP is accessing the SAR reports, and calling the Contact Centre on behalf of the PCP.	2016-08-11	The Contact Centre agent immediately ended the discussion regarding the SAR. They informed the representative that the SAR report access constituted a privacy breach.	N/A	2016-08-11	Contact Center	Privacy breach	The Contact Centre agent should advise the representative to register for a ONE ID account. They should further advise that the representative must be registered with CCO as a delegate of the PCP prior to accessing the PCP's SAR, or calling CCO about anything related to the SAR.	NO	Contact Center	N/A	The Contact Centre agent provided feedback to the representative, who agreed to register for ONE ID. The Contact Centre agent transferred the representative to eHealth, or provided them with the eHealth phone number, so that they could be registered for a ONE ID account.	2016
2016-08-15	2016-08-15	External	2016-08-15	Client's Result Letter (Test Result)	2016-08-15	CC inactivated address + Unintended Recipient asked to return letter	N/A	2016-08-16	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	N/A	Client did not want to update address.	2016
2016-08-15	2016-08-15	External	2016-08-15	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-08-15	CC inactivated address + Unintended Recipient asked to return letter	N/A	2016-09-30	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center & Privacy Specialist	N/A	Address inactivated. CC was unable to reach the client.	2016

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
2016-08-15	2016-08-15	External	2016-08-15	A representative from the PCP's office who is not registered as a delegate of the PCP is accessing the SAR reports, and calling the Contact Centre on behalf of the PCP.	2016-08-15	The Contact Centre agent immediately ended the discussion regarding the SAR. They informed the representative that the SAR report access constituted a privacy breach.	N/A	2016-08-15	Contact Center	Privacy breach	None Required	NO	Contact Center	N/A	The Contact Centre agent provided feedback to the representative, who agreed to register for ONE ID. The Contact Centre agent transferred the representative to eHealth, or provided them with the eHealth phone number, so that they could be registered for a ONE ID account.	2016
2016-08-16	2016-08-16	Internal	2016-08-16	Client's Result Letter (Test Result)	2016-08-16	Unintended recipient notified CC of breach. Letter was opened. Unintended recipient was asked to return letter but they did not do this. Reminder voicemail left for unintended recipient to return the letter. No further containment measures possible.	N/A	N/A	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center	2016-09-07	CC did not contact client because they saw that the client's address had already been updated post breach.	2016
2016-08-18	2016-08-18	External	2016-08-18	Client PHI intended for a CCO screening program was provided to CCO by a PCP, in electronic, voicemail, or paper form.	N/A	Privacy uploaded the fax to an activity in InScreen. Privacy had been the original recipient of the PHI, and had hard deleted the fax containing PHI from CCO's systems.	N/A	2016-08-23	Contact Center & Privacy Specialist	Policy breach	The Contact Centre agent should call the PCP and inform them of the policy breach. For misdirected requests, the agent should re-direct the PCP to the appropriate recipient of these requests	NO	Contact Center & Privacy Specialist	N/A	The PCP was notified of the policy breach, and about the policy on client PHI maintenance.	2016

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
											(e.g., Ontario Breast Screening Program High Risk site) and advise them to not send PHI to CCO for such requests.					
2016-08-19	2016-08-19	External	2016-08-19	Client's Result Letter (Test Result)	2016-08-22	CC inactivated incorrect address	2016-08-22	2016-08-26	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	YES	Contact Center & Privacy Specialist	N/A	CC called the client and updated the address.	2016
2016-08-19	2016-08-19	External	2016-08-19	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-08-09	CC inactivated incorrect address	2016-08-25	2016-08-26	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	YES	Contact Center & Privacy Specialist	N/A	CC called the client and updated the address.	2016
2016-08-19	2016-08-19	External	2016-08-19	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-08-19	CC inactivated incorrect address	2016-09-07	2016-09-12	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center & Privacy Specialist	N/A	Address updated. CC was able to contact the client via number provided by their PCP.	2016
2016-08-19	2016-08-19	External	2016-08-19	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-07-27	CC inactivated incorrect address	N/A	2016-08-24	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-08-19	2016-08-19	External	2016-08-19	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-08-19	CC inactivated incorrect address	N/A	2016-08-24	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-08-19	2016-08-19	External	2016-08-19	Client's Result Letter (Test Result)	2016-08-19	CC inactivated incorrect address	N/A	2016-08-19	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-08-19	2016-08-19	External	2016-08-19	Client's Invitation/Reminder Letter (Screening	2016-08-19	CC inactivated the address + Unintended Recipient to destroy letter	N/A	2016-08-19	Contact Center	Privacy breach	None Required	NO	Contact Center	N/A	None Required	2016

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				Status/Eligibility)												
2016-08-22	2016-08-22	External	2016-08-22	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-08-22	CC inactivated incorrect address	N/A	2016-08-25	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-08-23	2016-08-23	External	2016-08-23	Client's Result Letter (Test Result)	2016-08-23	CC inactivated incorrect address	2016-08-23	2016-08-25	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	YES	Contact Center & Privacy Specialist	N/A	CC called the client and updated the address.	2016
2016-08-23	2016-08-23	External	2016-08-26	Client's Result Letter (Test Result)	2016-08-23	CC inactivated incorrect address	2016-08-24	2016-08-26	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	YES	Contact Center & Privacy Specialist	N/A	CC called the client and updated the address.	2016
2016-08-23	2016-08-23	External	2016-08-23	Client's Result Letter (Test Result)	2016-08-23	CC inactivated incorrect address	2016-08-29	2016-08-29	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center & Privacy Specialist	N/A	CC called the client and updated the address.	2016
2016-08-23	2016-08-23	External	2016-08-23	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-08-23	CC inactivated incorrect address	N/A	2016-08-29	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-08-23	2016-08-23	External	2016-08-23	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-08-23	CC inactivated incorrect address	N/A	2016-08-29	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-08-23	2016-08-23	External	2016-08-23	Client PHI intended for a CCO screening program was provided to CCO by a PCP, in electronic, voicemail, or paper form.	2016-08-23	Privacy uploaded the fax to an activity in InScreen. Privacy had been the original recipient of the PHI, and had hard deleted the fax containing PHI from CCO's systems.	N/A	2016-08-29	Contact Center & Privacy Specialist	Policy breach	The Contact Centre agent should call the PCP and inform them of the policy breach. For misdirected requests, the agent should re-direct the PCP to the appropriate recipient of these requests (e.g., Ontario Breast Screening Program High	NO	Contact Center & Privacy Specialist	N/A	The PCP was notified of the policy breach, and about the policy on client PHI maintenance.	2016

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
											Risk site) and advise them to not send PHI to CCO for such requests.					
2016-08-23	2016-08-23	External	2016-08-23	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-08-23	CC inactivated incorrect address	N/A	2016-08-23	Contact Center	Privacy breach	None Required	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-08-23	2016-08-23	Internal	2016-08-23	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-08-23	CC received returned letter, which had been opened. No contact information for the unintended recipient available, therefore no containment possible. CC indicated that they will destroy the letter.	N/A	2016-08-23	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-08-25	2016-08-25	External	2016-08-25	Client PHI intended for a CCO screening program was provided to CCO by a PCP, in electronic, voicemail, or paper form.	2016-08-25	Privacy uploaded the fax to an activity in InScreen. Privacy had been the original recipient of the PHI, and had hard deleted the fax containing PHI from CCO's systems.	N/A	2016-08-25	Contact Center & Privacy Specialist	Policy breach	The Contact Centre agent should call the PCP and inform them of the policy breach. For misdirected requests, the agent should re-direct the PCP to the appropriate recipient of these requests (e.g., Ontario Breast Screening Program High Risk site) and advise them to not send PHI	NO	Contact Center & Privacy Specialist	N/A	The PCP was notified of the policy breach, and about the policy on client PHI maintenance.	2016

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
											to CCO for such requests.					
2016-08-25	2016-08-25	External	2016-08-26	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-09-09	CC inactivated incorrect address	2016-09-06	2016-09-13	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center & Privacy Specialist	N/A	CC called the client and updated the address.	2016
2016-08-25	2016-08-25	External	2016-08-25	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-09-09	CC inactivated the address + Unintended Recipient to destroy letter	2016-09-06	2016-09-13	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	YES	Contact Center & Privacy Specialist	N/A	CC called the client and updated the address.	2016
2016-08-26	2016-08-26	External	2016-08-26	Client PHI intended for a CCO screening program was provided to CCO by a PCP, in electronic, voicemail, or paper form.	2016-08-26	Privacy uploaded the fax to an activity in InScreen. Privacy had been the original recipient of the PHI, and had hard deleted the fax containing PHI from CCO's systems.	N/A	2016-08-31	Contact Center & Privacy Specialist	Policy breach	The Contact Centre agent should call the PCP and inform them of the policy breach. For client requests through the PCP (withdraw, address updates, anything screening related), the agent should direct the PCP to have the client call CCO directly for the request.	NO	Contact Center & Privacy Specialist	N/A	The PCP was notified of the policy breach, and about the policy on client PHI maintenance.	2016
2016-08-26	2016-08-26	External	2016-08-26	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-08-26	CC inactivated incorrect address	N/A	2016-08-26	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-08-26	2016-08-26	External	2016-08-26	Client's Result Letter (Test Result)	2016-08-26	CC inactivated incorrect address	N/A	2016-08-31	Contact Center	Privacy breach	Address to be inactivated. CC to attempt	NO	Contact Center	N/A	Address inactivated. CC was	2016

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
											to contact intended client.				unable to reach the client.	
2016-08-29	2016-08-29	External	2016-08-29	Client's Result Letter (Test Result)	2016-08-29	CC inactivated address + Unintended Recipient asked to return letter	2016-09-07	2016-09-12	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	YES	Contact Center & Privacy Specialist	N/A	CC called the client and updated the address.	2016
2016-08-29	2016-08-29	External	2016-08-29	A representative from the PCP's office who is not registered as a delegate of the PCP is accessing the SAR reports, and calling the Contact Centre on behalf of the PCP.	2016-08-29	The Contact Centre agent immediately ended the discussion regarding the SAR. They informed the representative that the SAR report access constituted a privacy breach.	N/A	2016-08-29	Contact Center	Privacy breach	The Contact Centre agent should advise the representative to register for a ONE ID account. They should further advise that the representative must be registered with CCO as a delegate of the PCP prior to accessing the PCP's SAR, or calling CCO about anything related to the SAR.	NO	Contact Center	N/A	The Contact Centre agent provided feedback to the representative, who did not wish to be registered for ONE ID. The Contact Centre agent reiterated the authentication requirements and let the representative know that they must have delegate status in order to access the SAR. The Contact Centre agent followed up with the PCP to inform them of the breach.	2016
2016-08-30	2016-08-30	External	2016-08-30	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-08-30	CC inactivated address + Unintended recipient asked to return letter	N/A	2016-09-23	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
2016-08-31	2016-08-31	External	2016-08-31	Lab reports containing PHI (pathology, diagnostics, screening, treatment) related to CCO programs were sent to CCO.	2016-08-31	Privacy uploaded the fax to an activity in InScreen. Privacy had been the original recipient of the PHI, and had hard deleted the fax containing PHI from CCO's systems.	N/A	2016-08-31	Contact Center & Privacy Specialist	Policy breach	The Contact Centre agent should call the PCP and inform them of the policy breach. For misdirected requests, the agent should re-direct the PCP to the appropriate recipient of these requests (e.g., Ontario Breast Screening Program High Risk site) and advise them to not send PHI to CCO for such requests.	NO	Contact Center & Privacy Specialist	N/A	The PCP was notified of the policy breach, and about the policy on client PHI maintenance.	2016
2016-08-31	2016-08-31	External	2016-08-31	Client's Result Letter (Test Result)	2016-08-31	CC inactivated address + Unintended recipient asked to return letter	N/A	2016-08-29	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-08-31	2016-08-31	External	2016-08-30	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-08-30	CC inactivated the address + Unintended recipient to destroy letter	N/A	2016-09-08	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-09-02	2016-09-02	External	2016-09-02	Client's Result Letter (Test Result)	2016-09-02	CC inactivated the address + Unintended recipient to destroy letter	2016-09-07	2016-09-07	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	YES	Contact Center & Privacy Specialist	N/A	Address updated. CC was able to contact the client via number provided by their PCP.	2016
2016-09-06	2016-09-06	External	2016-09-06	Client's Result Letter (Test Result)	2016-09-06	CC inactivated address + Unintended recipient asked to return letter	2016-09-12	2016-09-14	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	YES	Contact Center & Privacy Specialist	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-09-08	2016-09-08	External	2016-09-08	Client's Result Letter (Test Result)	2016-09-08	CC inactivated incorrect address	2016-09-16	2016-09-29	Contact Center	Privacy breach	None Required	YES	Contact Center & Privacy Specialist	N/A	CC called the client and updated the address.	2016
2016-09-09	2016-09-09	External	2016-09-09	Client's Invitation/Reminder Letter (Screening	2016-09-09	CC inactivated incorrect address	2016-09-19	2016-09-29	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact	YES	Contact Center & Privacy Specialist	N/A	CC called the client and updated the address.	2016

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				Status/Eligibility)							intended client.					
2016-09-12	2016-09-12	External	2016-09-15	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-09-12	CC inactivated incorrect address	N/A	2016-09-15	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-09-13	2016-09-13	External	2016-09-13	Client's Result Letter (Test Result)	2016-09-13	CC inactivated the address + Unintended recipient to destroy letter	N/A	2016-09-13	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to obtain client's phone number from PCP.	2016
2016-09-14	2016-09-14	External	2016-09-14	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-09-14	CC inactivated address + Unintended recipient asked to return letter	N/A	2016-09-29	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-09-16	2016-09-16	External	2016-09-16	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-09-16	CC inactivated the address + Unintended recipient to destroy letter	N/A	2016-09-30	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-09-16	2016-09-16	External	2016-09-16	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-09-16	CC inactivated address + Unintended recipient asked to return letter	N/A	2016-09-16	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-09-16	2016-09-16	External	2016-09-16	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-09-22	CC inactivated the address + Unintended recipient to destroy letter	N/A	2016-09-22	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	N/A	CC called the client and updated the address.	2016
2016-09-19	2016-09-19	External	2016-09-19	Client's Result Letter (Test Result)	2016-09-19	CC inactivated the address + Unintended recipient to destroy letter	N/A	2016-09-23	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-09-19	2016-09-19	External	2016-09-19	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-09-19	CC inactivated the address + Unintended recipient to destroy letter	N/A	2016-09-21	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-09-20	2016-09-20	External	2016-09-20	Client's Invitation/Reminder Letter (Screening	2016-09-20	CC inactivated the address + Unintended recipient to destroy letter	N/A	2016-09-29	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact	NO	Contact Center	N/A	Address inactivated. CC was unable to	2016

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
				Status/Eligibility)							intended client.				reach the client.	
2016-09-21	2016-09-21	External	2016-09-21	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-09-28	CC inactivated address + Unintended recipient asked to return letter	N/A	2016-09-28	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-09-23	2016-09-23	External	2016-09-23	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-09-23	CC inactivated address + Unintended recipient asked to return letter	N/A	2016-09-23	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-09-23	2016-09-23	External	2016-09-23	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-09-23	CC inactivated the address + Unintended recipient to destroy letter	N/A	2016-09-27	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-09-23	2016-09-23	External	2016-09-23	Client's Result Letter (Test Result)	2016-09-23	cc inactivated incorrect address	N/A	2016-09-23	Contact Center	Privacy breach	None Required	NO	Contact Center	N/A	None Required	2016
2016-09-26	2016-09-26	External	2016-09-26	Client PHI intended for a CCO screening program was provided to CCO by a PCP, in electronic, voicemail, or paper form.	2016-09-23	Privacy uploaded the fax to an activity in InScreen. Privacy had been the original recipient of the PHI, and had hard deleted the fax containing PHI from CCO's systems.	N/A	2016-09-29	Contact Center & Privacy Specialist	Policy breach	The Contact Centre agent should call the PCP and inform them of the policy breach. For misdirected requests, the agent should re-direct the PCP to the appropriate recipient of these requests (e.g., Ontario Breast Screening Program High Risk site) and advise them to not send PHI to CCO for such requests.	NO	Contact Center & Privacy Specialist	N/A	The PCP was notified of the policy breach.	2016
2016-09-26	2016-09-26	Internal	2016-09-26	Cannot be determined	2016-09-26	The Contact Centre agent logged the internal policy breach in InScreen.	N/A	2016-09-26	Contact Center	Policy breach	The Contact Centre Management should coach the relevant agent on standard operating procedures for	NO	Contact Center	N/A	The Contact Centre agent received appropriate coaching from the Contact Centre Management.	2016

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
											authenticating clients and for PHI disclosure.					
2016-09-28	2016-09-28	External	2016-09-28	Client's Result Letter (Test Result)	2016-09-28	CC inactivated the address + Unintended recipient to destroy letter	2016-09-28	2016-10-04	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	YES	Contact Center & Privacy Specialist	N/A	CC called the client and updated the address.	2016
2016-09-29	2016-09-29	External	2016-09-29	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-09-28	CC inactivated address + Unintended recipient asked to return letter	N/A	2016-10-11	Contact Center	Privacy breach	None Required	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-09-30	2016-09-30	External	2016-09-30	Client's Result Letter (Test Result)	2016-09-30	cc inactivated incorrect address	2016-09-30	2016-10-18	Contact Center	Privacy breach	None Required	YES	Contact Center & Privacy Specialist	N/A	CC called the client and updated the address.	2016
2016-10-03	2016-10-03	External	2016-10-03	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-10-03	CC inactivated the address + Unintended Recepient to destroy letter	N/A	2016-10-03	Contact Center	Privacy breach	None Required	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-10-04	2016-10-04	External	2016-10-04	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-10-04	The Contact Centre agent scanned the paper document to an activity in InScreen, then destroyed the paper document.	N/A	2016-10-04	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address updated. CC was able to contact the client via number provided by their PCP.	2016
2016-10-04	2016-10-04	External	2016-10-04	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-10-04	CC inactivated incorrect adderess	N/A	2016-10-04	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-10-05	2016-10-05	External	2016-10-05	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-10-05	CC inactivated address + Unintended Recepient asked to return letter	N/A	2016-10-11	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-10-05	2016-10-05	External	2016-10-05	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-10-05	CC inactivated address + Unintended Recepient asked to return letter	N/A	2016-10-06	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
2016-10-07	2016-10-07	External	2016-10-07	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-10-07	CC inactivated address + Unintended Recepient asked to return letter	N/A	2016-10-17	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-10-12	2016-10-12	External	2016-10-12	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-10-12	CC inactivated address + Unintended Recepient asked to return letter	N/A	2016-10-21	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	N/A	Address updated. CC was able to contact the client via number provided by their PCP.	2016
2016-10-12	2016-10-12	External	2016-10-12	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-10-12	CC inactivated the address + Unintended Recepient to destroy letter	N/A	2016-10-12	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-10-12	2016-10-16	External	2016-10-12	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-10-12	CC inactivated address + Unintended Recepient asked to return letter	N/A	2016-10-17	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-10-13	2016-10-13	External	2016-10-13	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-10-14	CC inactivated address + Unintended Recepient asked to return letter	N/A	2016-10-14	Contact Center	Privacy breach	None Required	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-10-13	2016-10-13	External	2016-10-13	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-10-13	CC inactivated address + Unintended Recepient asked to return letter	N/A	2016-10-27	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-10-18	2016-10-18	External	2016-10-18	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-10-18	CC inactivated the address + Unintended Recepient to destroy letter	N/A	2016-10-18	Contact Center	Privacy breach	None Required	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-10-18	2016-10-18	External	2016-10-18	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-10-18	CC inactivated address + Unintended Recepient asked to return letter	N/A	2016-10-18	Contact Center	Privacy breach	None Required	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-10-18	2016-10-18	External	2016-10-18	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-10-18	CC inactivated the address + Unintended Recepient to destroy letter	N/A	2016-10-18	Contact Center	Privacy breach	None Required	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
2016-10-19	2016-10-19	External	2016-10-19	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-10-19	CC inactivated address + Unintended Recepient asked to return letter	N/A	2016-11-01	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-10-21	2016-10-21	External	2016-10-21	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-10-21	CC inactivated address + Unintended Recepient asked to return letter	N/A	2016-11-16	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-10-24	2016-10-24	External	2016-10-24	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-10-24	The Contact Centre agent scanned the paper document to an activity in InScreen, then destroyed the paper document.	N/A	2016-11-03	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	N/A	Address inactivated. CC was unable to obtain client's phone number from PCP.	2016
2016-10-25	2016-10-25	External	2016-10-25	Client's Result Letter (Test Result)	2016-10-25	CC inactivated the address + Unintended Recepient to destroy letter	2016-10-25	2016-10-31	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	YES	Contact Center & Privacy Specialist	N/A	CC called the client and updated the address.	2016
2016-10-26	2016-10-26	External	2016-10-26	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-10-26	CC inactivated the address + Unintended Recepient to destroy letter	N/A	2016-11-02	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-10-26	2016-10-26	External	2016-10-26	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-10-26	The Contact Centre agent scanned the paper document to an activity in InScreen, then destroyed the paper document.	N/A	2016-10-28	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-10-26	2016-10-26	External	2016-10-26	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-10-26	The Contact Centre agent scanned the paper document to an activity in InScreen, then destroyed the paper document.	N/A	2016-11-11	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	N/A	Address inactivated. CC was unable to obtain client's phone number from PCP.	2016

Date breach was identified or suspected	Date breach was identified or suspected2	Internal/External	Date Senior Management was Notified (date range provided)	Nature of PHI	Date of Containment	Containment Measure	Date Notification Provided to HICs/Other Orgs	Date Investigation Completed	Agent to conduct investigation	Policy or privacy breach?	Recommendations	Breach Notification Letter sent to client	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed	Year
2016-10-27	2016-10-27	External	2016-10-27	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-10-26	The Contact Centre agent scanned the paper document to an activity in InScreen, then destroyed the paper document.	N/A	2016-10-28	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-10-27	2016-10-27	External	2016-10-27	Client's Result Letter (Test Result)	2016-10-27	CC inactivated the address + Unintended Recepient to destroy letter	N/A	2016-10-27	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-10-28	2016-10-28	External	2016-10-28	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-10-28	CC inactivated address + Unintended Recepient asked to return letter	N/A	N/A	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-10-31	2016-10-31	External	2016-10-31	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-11-04	The Contact Centre agent scanned the paper document to an activity in InScreen, then destroyed the paper document.	N/A	2016-11-04	Contact Center	Privacy breach	Contact Center to call client/PCP and update address.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016
2016-10-31	2016-10-31	External	2016-10-31	Client's Invitation/Reminder Letter (Screening Status/Eligibility)	2016-10-31	The Contact Centre agent scanned the paper document to an activity in InScreen, then destroyed the paper document.	N/A	2016-11-04	Contact Center	Privacy breach	Address to be inactivated. CC to attempt to contact intended client.	NO	Contact Center	N/A	Address inactivated. CC was unable to reach the client.	2016

Appendix I.1: Indicators- Summary from the Log of Security Audits

The nature and type of the security audit conducted	System / Product	The date that the security audit was completed	The agent(s) responsible for completing the security audit	The recommendations arising from the security audit	The agent(s) responsible for addressing each recommendation
Technical Vulnerability Assessment	iPort	11/17/2013	EISO	Deployment Procedural and Ongoing Operations 3rd Party Components and Integration	Product team
Security Architecture Assessment	McKesson Data Encryption Tool	12/6/2013	EISO	Software Development	Vendor
Technical Vulnerability Assessment	eProcurement	2/2/2014	EISO	Software Development Ongoing Configuration (Hardware & Software) Deployment 3rd Party Components and Integration	IT Operations Product team
Technical Vulnerability Assessment	ICBP (International Cancer Benchmarking Partnership)	2/6/2014	EISO	Procedural and Ongoing Operations	Product team
Technical Vulnerability Assessment	WTIS R17 - Baseline	2/13/2014	EISO	Procedural and Ongoing Operations Design Deployment	IT Operations Product team
Technical Vulnerability Assessment	EPICOR Finance Users	2/13/2014	EISO	Procedural and Ongoing Operations 3rd Party Components and Integration	Product team
Technical Vulnerability Assessment	ATP Tracking and Recording - Production	2/18/2014	EISO	Ongoing Configuration (Hardware/Software)	IT Operations
Threat and Risk Assessment	eLAB -ORN	2/28/2014	EISO	Procedural and Ongoing Operations Data Sharing, Archiving, and Disposal Account Management	IT Operations Product team
Threat and Risk Assessment	ICS eReports PCSAR	3/17/2014	External	Design Deployment Procedural and Ongoing Operations Data Access and Data Management Data Sharing, Archiving, and Disposal	Product team
Threat and Risk Assessment	ISAAC Delta (TRA Addendum)	3/20/2014	EISO	Ongoing Configuration (Hardware/Software) Account Management	IT Operations Product team
Technical Vulnerability Assessment; **Penetration Testing**	Epicor and eProcurement	4/2/2014	External	Design Ongoing Configuration (Hardware/Software) Software Development Procedural and Ongoing Operations Data Access and Data Management	IT Operations Product team

The nature and type of the security audit conducted	System / Product	The date that the security audit was completed	The agent(s) responsible for completing the security audit	The recommendations arising from the security audit	The agent(s) responsible for addressing each recommendation
Technical Vulnerability Assessment	MIVS	5/12/2014	EISO	Account Management Deployment Ongoing Configuration (Hardware/Software) Procedural and Ongoing Operations	IT Operations Product team
Technical Vulnerability Assessment	OCSMC	6/9/2014	EISO	Deployment Procedural and Ongoing Operations	Product team
Technical Vulnerability Assessment	WTIS R18 - Baseline	7/15/2014	EISO	Deployment Design Ongoing Configuration (Hardware/Software) Procedural and Ongoing Operations	IT Operations Product team
Technical Vulnerability Assessment	eLAB -ORN	7/21/2014	EISO	Ongoing Configuration (Hardware/Software) Procedural and Ongoing Operations Deployment	IT Operations Product team
Technical Vulnerability Assessment	Siebel Upgrade	7/29/2014	EISO	Procedural and Ongoing Operations	Product team
Technical Vulnerability Assessment	SSO IS	7/31/2014	EISO	Procedural and Ongoing Operations	Product team
Threat and Risk Assessment	MyCancerIQ (OCRAT)	8/8/2014	External	Design Software Development Deployment 3rd Party Components and Integration Ongoing Configuration (Hardware/Software) Account Management Procedural and Ongoing Operations Data Access and Data Management Data Sharing, Archiving, and Disposal	IT Operations Product team
Threat and Risk Assessment	ISAAC for AHAC	8/28/2014	EISO	Procedural and Ongoing Operations Deployment Software Development Account Management Data Access and Data Management	IT Operations Product team
Technical Vulnerability Assessment; **Penetration Testing**	OCRAT	9/19/2014	External	Ongoing Configuration (Hardware/Software)	Product team
Technical Vulnerability Assessment; **Penetration Testing**	PCSAR R2	11/18/2014	External	Procedural and Ongoing Operations Data Access and Data Management	Product team
Technical Vulnerability Assessment	Drug Formulary	11/24/2014	EISO	Software Development Deployment Ongoing Configuration (Hardware/Software)	Product team
Technical Vulnerability Assessment	MIVS	11/25/2014	EISO	Deployment Procedural and Ongoing Operations	IT Operations

The nature and type of the security audit conducted	System / Product	The date that the security audit was completed	The agent(s) responsible for completing the security audit	The recommendations arising from the security audit	The agent(s) responsible for addressing each recommendation
Technical Vulnerability Assessment	Informatica	11/26/2014	EISO	Procedural and Ongoing Operations 3rd Party Components and Integration	Product team
Technical Vulnerability Assessment	ORRS (completion)	12/11/2014	EISO	Deployment Procedural and Ongoing Operations Ongoing Configuration (Hardware/Software)	Product team
Technical Vulnerability Assessment	iPort	1/20/2015	EISO	Procedural and Ongoing Operations 3rd Party Components and Integration	Product team
Technical Vulnerability Assessment	ISAAC for AHAC	1/21/2015	EISO	None	
Threat and Risk Assessment	EDS	4/9/2015	EISO	Procedural and Ongoing Operations Deployment Account Management Ongoing Configuration (Hardware/Software) Data Access and Data Management Design Data Sharing, Archiving, and Disposal	IT Operations Product team
Technical Vulnerability Assessment	WTIS R18 - Baseline	4/21/2015	EISO	Design Procedural and Ongoing Operations	IT Operations Product team
Technical Vulnerability Assessment	RNFS	4/30/2015	EISO	Procedural and Ongoing Operations Ongoing Configuration (Hardware/Software)	IT Operations Product team
Technical Vulnerability Assessment	WTIS R18	5/13/2015	EISO	Procedural and Ongoing Operations	Product team
Threat and Risk Assessment	Windows Server 2003 End of Life	6/11/2015	EISO	Ongoing Configuration (Hardware/Software)	IT Operations
Technical Vulnerability Assessment	GI Endo	7/30/2015	EISO	Ongoing Configuration (Hardware & Software) Procedural and Ongoing Operations	IT Operations Product team
Technical Vulnerability Assessment	ISAAC Higher Availability QA	8/31/2015	EISO	Software Development Deployment Procedural and Ongoing Operations	Product team
Technical Vulnerability Assessment	IPEHOC	9/21/2015	EISO	Ongoing Configuration (Hardware/Software) Account Management Procedural and Ongoing Operations	IT Operations Product team
Threat and Risk Assessment	ePREM (Electronic Patient Reported Experience Measures)	10/1/2015	External	Account Management Ongoing Configuration (Hardware/Software)	IT Operations Product team
Technical Vulnerability Assessment	DAP-EPS Higher Availability	10/13/2015	EISO	Ongoing Configuration (Hardware/Software) Procedural and Ongoing Operations	IT Operations Product team
Threat and Risk Assessment	Enterprise Social Network Solution (Yammer)	11/17/2015	External	Procedural and Ongoing Operations Data Access and Data Management	IT Operations Product team

The nature and type of the security audit conducted	System / Product	The date that the security audit was completed	The agent(s) responsible for completing the security audit	The recommendations arising from the security audit	The agent(s) responsible for addressing each recommendation
Threat and Risk Assessment	Patient Experience RTM	11/24/2015	External	Design Deployment Ongoing Configuration (Hardware/Software) Procedural and Ongoing Operations Data Access and Data Management Account Management Data Sharing, Archiving, and Disposal	IT Operations Product team

2016 With Additional Columns Added

The nature and type of the security audit conducted	System / Product	The date that the security audit was completed	The agent(s) responsible for completing the security audit	The recommendations arising from the security audit	The agent(s) responsible for addressing each recommendation	Target mitigation date	Mitigation date	The manner in which each recommendation was or is expected to be addressed
Baseline Phishing Susceptibility Assessments **Ethical Hacking / Penetration Test**	All staff	9/15/2015 – 9/25/2016	EISO	Improve awareness Improve CCO endpoint protection	EISO, IT Operations, Communications, Technology Services	FY 16-17	Oct-16 May-17	Due to the confidential nature of the details of the analysis, CCO has excluded a description of the analysis from the public version of this report; however, these details have been provided to the IPC.
Threat and Risk Assessment	ICMS	1/14/2016	External	Design Software Development Procedural and Ongoing Operations Account Management	IT Operations Product team	Q3-16	Jan-17	TVA completed
Technical Vulnerability Assessment;	ICMS	1/26/2016	External	Ongoing Configuration (Hardware/Software) Procedural and Ongoing Operations	IT Operations Product team	Q3-16	Jan-17	The project was put on hold. Due to the confidential nature of the details of the analysis, CCO has excluded a description of the analysis from the public version of this report; however, these details have been provided to the IPC.
Security Assessment	HCMS	3/4/2016	External	Software Development	Product team	Mar-16	Mar-16	The vendor addressed the vulnerability identified and provided an updated report.
Security Assessment	HCMS & MIM Integration	9/27/2016	EISO	Procedural and Ongoing Operations	IT Operations Product team	Q3-16	Jan-17	Due to the confidential nature of the details of the analysis, CCO has excluded a description of the analysis from the public version of this report; however, these details have been provided to the IPC.
Threat and Risk Assessment	WTIS R19 (Release Cancelled)	5/10/2016	External	Design Deployment Procedural and Ongoing Operations	Product team	N/A	N/A	Release 19 was cancelled.
Security Assessment	Corporate Scorecard	6/3/2016	EISO	Deployment	Product team	Dec 2016	Dec-16	Hardware configuration issues addressed.
Security Assessment	Siebel Upgrade & SODD Integration	6/20/2016	EISO	Ongoing Configuration (Hardware/Software)	Product team	Jun-16	Jun-16	Due to the confidential nature of the details of the analysis, CCO has excluded a description of the analysis from the public version of this report; however, these details have been provided to the IPC.
Security Assessment	LIRT and CIRT	8/26/2016	EISO	Design Deployment Ongoing Configuration (Hardware/Software) Procedural and Ongoing Operations Data Access and Data Management Account Management Data Sharing, Archiving, and Disposal	IT Operations Product team	Q2-16	Sep-16	Due to the confidential nature of the details of the analysis, CCO has excluded a description of the analysis from the public version of this report; however, these details have been provided to the IPC.
						Aug-16	Aug-16	Product migrated to supported product.
						Q2-17	May-17	Due to the confidential nature of the details of the analysis, CCO has excluded a description of the analysis from the public version of this report; however, these details have been provided to the IPC.
						Jun-17	n/a	Due to the confidential nature of the details of the analysis, CCO has excluded a description of the analysis from the public version of this report; however, these details have been provided to the IPC.

Technical Vulnerability Assessment; **Ethical Hacking**	LIRT and CIRT	9/29/2016	EISO	Software Development Deployment Ongoing Configuration (Hardware/Software) Procedural and Ongoing Operations	IT Operations Product team	Q4-16	Nov-16	IT Operations addressed all technical vulnerabilities for both LIRT and CIRT
Security Assessment	GI Endoscopy phase 2	9/21/2016	EISO	Design Procedural and Ongoing Operations Deployment Data Access and Data Management	IT Operations Product team	Dec-16	Dec-16	TVA completed
						Oct-17		Due to the confidential nature of the details of the analysis, CCO has excluded a description of the analysis from the public version of this report; however, these details have been provided to the IPC.
						Dec-16		Due to the confidential nature of the details of the analysis, CCO has excluded a description of the analysis from the public version of this report; however, these details have been provided to the IPC.

Appendix I.2: Indicators – Summary from the Log of Security Audits

Incident Category	Date of Incident Occurrence	Discovered /Reported	Sensitivity of Information Involved	Security Breach	Containment Measures	Containment	Snr Mgmt Notification	External Notification	Investigation Complete	Investigated by	Recommendations	Manner of Recommendations Implementation	Recommendations Implemented	Implementer
Other Policy Violation	2/7/2014		PHI	No	deleted all emails containing PHI	2/13/2014	2/11/2014		2/13/2014	LPO	User Education.	One-on-one training with the User	3/1/2014	
Malicious Logic or Code	4/26/2014		Not Applicable	No	Computer was reimaged	4/27/2014	4/26/2014		4/26/2014	EISO	User education	One-on-one training with the User	4/27/2014	
Other Policy Violation	4/27/2014		PHI	Yes	Emails related to the case deleted. Breached account was deactivated. Victim was notified	4/30/2014	4/28/2014		4/30/2014	LPO	Process improvement	Process was reviewed and improved	6/1/2014	
Malicious Logic or Code	6/23/2014		Not Applicable	No	Computer was reimaged	6/23/2014	6/23/2014		6/23/2014	EISO	User education	One-on-one training with the User	6/24/2014	
Inappropriate Use	9/3/2014		Not Applicable	No	Determined offending user, computer, and software. Blocked protocol at the firewall level.	9/3/2014	9/3/2014		9/3/2014	EISO	User education	HR/Management action taken. HR and management follow up for reasonable discipline. Test and block Bit torrent file sharing protocol on corporate network.	5/9/2014	
Malicious Logic or Code	10/8/2014		Not Applicable	No	AV updated, internet access removed. Victims notified. Spam message removed from users and server. Infected computers were reimaged	10/8/2014	10/8/2014		10/14/2014	EISO	User education	Reimaging computers. New rules in place to block email attachments. Block email executable attachments at the perimeter, before they reach end users	12/9/2014	
Other Policy Violation	11/8/2014		PHI	No	Email deleted. Personnel notified of the current policies	11/10/2014	11/10/2014		11/10/2014	LPO	User education	Annual refresher for Privacy and Security. Retrain employees on a regular basis on Breach Management	12/15/2014	
Lost or Stolen Device	1/15/2015	1/15/2015	Business	No	Credentials changed	1/15/2015	1/15/2015		1/15/2015	EISO	Verify policy enforcement. User education	Password changed.	1/15/2015	EISO
Malicious Logic or Code	1/22/2015	1/22/2015	Business	No	Spam message removed from users and server. Infected computer was reimaged	1/22/2015	1/22/2015		1/22/2015	EISO	User education	One-on-One Training	1/22/2015	EISO

Incident Category	Date of Incident Occurrence	Discovered /Reported	Sensitivity of Information Involved	Security Breach	Containment Measures	Containment	Snr Mgmt Notification	External Notification	Investigation Complete	Investigated by	Recommendations	Manner of Recommendations Implementation	Recommendations Implemented	Implementer
Lost or Stolen Device	1/28/2015	1/28/2015	Business Confidential	No	User changed password. Computer account disabled. Laptop recovered 1 day later. Machine was reimaged.	1/28/2015	1/28/2015		1/29/2015	EISO	User education	One-on-One Training	1/29/2015	EISO
Malicious Logic or Code	2/2/2015	2/2/2015	PI	No	Employee recognized it was a scam and reported the email to EISO. No Further action is required as Employee did not reply or click anything in the email.	2/2/2015	2/2/2015		2/4/2015	EISO	User Education	One-on-One Training	2/4/2015	EISO
Other Policy Violation	2/5/2015	2/12/2015	Business	No	TPM was reenabled by Onsite support team.	5/22/2015	2/18/2015		5/22/2015	EISO		Follow Monitoring Process	5/22/2015	EISO
Other Policy Violation	2/12/2015	2/12/2015	PHI	No	A Solution was identified and confirmed with the third party provider. Solution was deployed in the production environment after QA was completed.	2/17/2016	2/18/2015		2/18/2015	EISO	Establish security test cases	Due to the confidential nature of the details of the analysis, CCO has excluded a description of the analysis from the public version of this report; however, these details have been provided to the IPC.	2/18/2015	EISO
Malicious Logic or Code	3/11/2015	3/11/2015	Business	No	Spam message removed from users. Malware was removed.	3/11/2015	3/11/2015		3/11/2015	EISO	User education	One-on-One Training	3/11/2015	EISO
Malicious Logic or Code	3/13/2015	3/13/2015	Business	No	Emails deleted from all inboxes by ITOps	3/14/2015	3/14/2015		3/27/2015	EISO	User education	One-on-One Training	3/27/2015	EISO
Malicious Logic or Code	3/17/2015	3/17/2015	Business	No	Malware was successfully removed.	3/17/2015	3/17/2015		3/17/2015	EISO	User education	One-on-One Training	3/24/2015	EISO
Lost or Stolen Device	3/21/2015	3/21/2015	Business	No	User changed her password. Computer account disabled.	3/23/2015	3/23/2015		3/23/2015	EISO	User education	One-on-One Training	3/24/2015	EISO
Malicious Logic or Code	4/20/2015	4/20/2015	Business	No	Ticket was created to reimage the Laptop. Malware was successfully removed.	4/20/2015	4/20/2015		4/20/2015	EISO	User education	One-on-One Training	4/25/2015	EISO
Malicious Logic or Code	4/21/2015	4/21/2015	Business	No	User changed her password. Malware was	4/21/2015	4/21/2015		4/21/2015	EISO	User education	One-on-One Training	4/26/2015	EISO

Incident Category	Date of Incident Occurrence	Discovered /Reported	Sensitivity of Information Involved	Security Breach	Containment Measures	Containment	Snr Mgmt Notification	External Notification	Investigation Complete	Investigated by	Recommendations	Manner of Recommendations Implementation	Recommendations Implemented	Implementer
					successfully removed.									
Other Policy Violation	4/24/2015	4/24/2015	Business Confidential	No	Account was sucecssfully disabled.	4/24/2015	4/24/2015		4/24/2015	EISO	Service desk education	Team Training	5/1/2015	EISO
Other Policy Violation	4/29/2015	5/7/2015	Business	No	Account was successfully disabled.	5/7/2015			5/7/2015	EISO	Team Training	Team Training	5/7/2015	EISO
Other Policy Violation	5/29/2015	6/1/2015	PHI	No	The file was deleted from the P drive.	6/2/2015	6/2/2015		6/1/2015	EISO	User education	User Education, One on One Training	6/5/2015	EISO
Other Policy Violation	6/1/2015	6/2/2015	PHI	No	Disabled IIS on both OAT and QA/UAT servers. Thus disabling the sites from being accessed.	6/1/2015	6/1/2015		6/1/2015	EISO		User Education, Due to the confidential nature of the details of the analysis, CCO has excluded a description of the analysis from the public version of this report; however, these details have been provided to the IPC.	6/15/2015	EISO
Lost or Stolen Device	7/15/2015	7/16/2015	Business	No	Account disabled. Laptop was found and retrieved by employee the next day. Machine was reimaged and passwords were reset.	7/16/2015	7/15/2015		7/16/2015	EISO	User education	Reset Passwords. Reimage machine	7/16/2015	EISO
Other Policy Violation	8/13/2015	8/13/2015	PHI	No	Helpdesk reversed the RA registration and has reverted back to Lifelab's original RA until August 28.	8/13/2015	8/13/2015		8/13/2015	EISO	Team education	Team Training	8/13/2015	EISO
Multiple Component	8/20/2015	8/20/2015	Business	No	Ticket was created to reimage the Laptop. New image of Windows 8.1 with latest security updates to be installed	8/22/2015	8/21/2015		8/22/2015	EISO	User education	User education. Helpdesk education. Reimage Machine	8/27/2015	EISO
Lost or Stolen Device	9/9/2015	9/9/2015	Business	No	Computer account disabled. Laptop recovered same day. Machine was reimaged.	9/9/2015	9/9/2015		9/9/2015	EISO	User education	One-on-One Training	9/9/2015	EISO
Reconnaissance Activity	9/14/2015	9/14/2015	Not Applicable	No	Firewall successfully	9/15/2015	9/14/2015		9/15/2015	EISO		EISO will work with ITOps to create a regular	9/15/2015	EISO

Incident Category	Date of Incident Occurrence	Discovered /Reported	Sensitivity of Information Involved	Security Breach	Containment Measures	Containment	Snr Mgmt Notification	External Notification	Investigation Complete	Investigated by	Recommendations	Manner of Recommendations Implementation	Recommendations Implemented	Implementer
					blocked all attacks							process to monitor these type of attacks.		
Other Policy Violation	9/28/2015	9/28/2015	PHI	No	The attachment was deleted from the work item. The work item was deleted as well as per EISO's recommendation.	9/28/2015	9/28/2015		10/1/2015	EISO	User education	EISO provided recommendations to delete the work item to make sure that no links to the attachment is accessible. User Education, One on One Training	10/1/2015	EISO
Lost or Stolen Device	1/15/2016	2/3/2016	Not Applicable	No	The tablet was used internally and no PHI has ever been loaded. The investigation has also been conducted to make sure the kiosk ID has not been re-assigned	2/3/2016	2/3/2016		2/4/2016	EISO	User education; Team education	Password changed.	2/4/2016	EISO
Malicious Logic or Code	1/31/2016	1/31/2016	Not Applicable	No	Received Configuration Manager Endpoint Protection Report indicating a malware was detected on the user's machine. Due to the confidential nature of the details of the analysis, CCO has excluded a description of the analysis from the public version of this report; however, these details have been provided to the IPC.	2/1/2016	2/1/2016		2/1/2016	EISO	User education	One on one training	2/1/2016	EISO
Inappropriate Use	2/8/2016	2/9/2016	Not Applicable	No	The User removed one item (with High alert type) from the history. The User started a full AV scan. A Tier2 specialist removed the laptop and provide the loaner. The infected laptop	2/10/2016	2/10/2016		2/10/2016	EISO	User education; Escalate to User's Manager	User education. Advised on being very cautious and run a full scan if anything suspicious happens. Director discussed issue with Manager. 2nd occurrence will result in HR notification	2/9/2016	EISO

Incident Category	Date of Incident Occurrence	Discovered /Reported	Sensitivity of Information Involved	Security Breach	Containment Measures	Containment	Snr Mgmt Notification	External Notification	Investigation Complete	Investigated by	Recommendations	Manner of Recommendations Implementation	Recommendations Implemented	Implementer
					will be re-imaged.									
Inappropriate Use	2/16/2016	2/17/2016	Not Applicable	No	EISO requested to remove the access to the network to the infected employee and to reimage the PC. EISO spoke with the manager to keep User offline till a replacement laptop is issued.	2/17/2016	2/17/2016		2/17/2016	EISO	User education; Escalate to User's Manager	Discussion with User's manager. A repeat of behaviour will involve HR.	4/20/2016	EISO
Lost or Stolen Device	5/16/2016	5/16/2016	Not Applicable	No	EISO reached out to the user and requested him to reset his password while he was using a loaner laptop.	5/16/2016	5/16/2016		5/17/2016	EISO	User education	Due to the confidential nature of the details of the analysis, CCO has excluded a description of the analysis from the public version of this report; however, these details have been provided to the IPC.	5/16/2016	EISO
Inappropriate Use	6/5/2016	6/5/2016	Not Applicable	No	Quarantined by SCEP	6/5/2016	6/7/2016		6/7/2016	EISO	User education; Escalate to User's Manager	Advised User's Manager of contravention of acceptable use policy. A second incident will see HR involvement.	6/22/2016	EISO
Lost or Stolen Device	6/14/2016	6/14/2016	Business	No	EISO sent an e-mail to IT Asset Manager to issue a remote wipe command for the missing laptop as per the 'Reporting Lost Device in CCO' process flow document.	6/14/2016	6/14/2016		6/16/2016	EISO	User education	The users password was reset, the missing device was disabled in Active Directory	6/14/2016	EISO
Inappropriate Use	6/15/2016	6/15/2016	Not Applicable	No	Helpdesk to disable CCODS account Helpdesk to disable the laptop in question Due to the confidential nature of the details of the analysis, CCO has excluded a description of the analysis from the public version of	6/15/2016	6/15/2016		6/16/2016	EISO	User education; Escalate to User's Manager	Due to the confidential nature of the details of the analysis, CCO has excluded a description of the analysis from the public version of this report; however, these details have been provided to the IPC.		EISO

Incident Category	Date of Incident Occurrence	Discovered /Reported	Sensitivity of Information Involved	Security Breach	Containment Measures	Containment	Snr Mgmt Notification	External Notification	Investigation Complete	Investigated by	Recommendations	Manner of Recommendations Implementation	Recommendations Implemented	Implementer
					this report; however, these details have been provided to the IPC.User's domain account password reset.									
Lost or Stolen Device	6/19/2016	6/20/2016	Business	No	EISO sent an e-mail to IT Asset Manager to follow with the user for any laptop replacement activities as per the 'Reporting Lost Device in CCO' process flow document	6/20/2016	6/21/2016		6/21/2016	EISO	User education	Recommendations implemented by service desk	6/20/2016	EISO
Lost or Stolen Device	6/20/2016	6/21/2016	Business Confidential	No	SD disabled laptop access and user's AD account.	6/21/2016	6/22/2016		6/22/2016	EISO	User education	Confirmed no log-in attempts from June 20-22. Laptop was recovered and re-imaged	6/22/2016	EISO
Inappropriate Use	6/22/2016	6/22/2016	Not Applicable	No	Quaranteened by SCEP	6/22/2016			6/22/2016	EISO	User education; Escalate to User's Manager	User education (re-take online security training) to ensure that CCO devices are not being used to carry potential malware and/or 'hacking' software. EISO also recommends that Service Management team lead speak with the user about this incident.	6/22/2016	EISO
Inappropriate Use	6/22/2016	6/22/2016	Not Applicable	No	Quaranteened by SCEP	6/22/2016	6/22/2016		6/23/2016	EISO	User education; Escalate to User's Manager	User education (re-take online security training) to ensure that CCO devices are not being used to carry potential malware and/or 'hacking' software. EISO also recommends that Service Management team lead speak with the user about this incident;	6/23/2016	EISO

Incident Category	Date of Incident Occurrence	Discovered /Reported	Sensitivity of Information Involved	Security Breach	Containment Measures	Containment	Snr Mgmt Notification	External Notification	Investigation Complete	Investigated by	Recommendations	Manner of Recommendations Implementation	Recommendations Implemented	Implementer
												however, the user was leaving the organization that week.		
Multiple Component	6/28/2016	7/7/2016	PHI	No	Files were removed..	7/7/2016	7/7/2016		7/22/2016	EISO	User education; Escalate to User's Manager	Discussion with employee and employee's manager what the issues were and expectations for future.	8/3/2016	EISO
Malicious Logic or Code	7/22/2016	7/26/2016	Business	No	Detective controls: - SCEP Alerts - Full malware scan via SCEP à results confirmed that the malware was not present on the users CCO issued device PREVENTITIVE Controls: - Once alert was received laptop was disabled in Active Directory (AD), network access was removed, preventing any potential spread of malware.	7/25/2016	7/22/2016		7/26/2016	EISO	User education	Education on safe browsing	7/26/2016	EISO
Malicious Logic or Code	8/4/2016	8/5/2016	PHI	No	Laptop and user account was disabled, also spoke to user to run a full malware scan. Results confirmed that there is no malware on the users laptop and does not require reimaging	8/5/2016	8/5/2016		8/5/2016	EISO	User education; Escalate to User's Manager		8/5/2016	
Malicious Logic or Code	8/5/2016	8/8/2016	Business	No	Laptop and user account was disabled, also spoke to user to run a full malware scan. Scan results confirmed that the identified malware in the alert was not clean, and therefore EISO advised that the	8/5/2016	8/5/2016		8/8/2016	EISO	User education; Escalate to User's Manager			

Incident Category	Date of Incident Occurrence	Discovered /Reported	Sensitivity of Information Involved	Security Breach	Containment Measures	Containment	Snr Mgmt Notification	External Notification	Investigation Complete	Investigated by	Recommendations	Manner of Recommendations Implementation	Recommendations Implemented	Implementer
					users CCO issued laptop be reimaged.									
Malicious Logic or Code	8/5/2016	8/8/2016	Business	No	Laptop and user account was disabled, also spoke to user to run a full malware scan. Scan results confirmed that the identified malware in the alert was not clean, and therefore EISO advised that the users CCO issued laptop be reimaged.	8/5/2016	8/5/2016		8/8/2016	EISO	User education; Escalate to User's Manager			
Lost or Stolen Device	8/10/2016	8/10/2016	Business Confidential	No	User password has been reset, the lost laptop is disabled in Active Directory. Also the harddrive is encrypted (MBAM)	8/10/2016	8/10/2016	8/11/2016	8/11/2016	EISO	User education; User to file a police report	Verbal discussion on protecting CCO laptop	8/10/2016	EISO
Malicious Logic or Code	8/17/2016	8/18/2016	Business	No	EISO Manager physically walked into Service Desk to request disabling (User laptop) and account due to a malware infection alert. Agent contacted user to run a full malware SCEP scan. SCEP successfully removed malicious files without issue. User laptop does not require reimaging. User has confirmed malware has been contained and removed as per his follow up screenshot and email.	8/17/2016	8/17/2016		8/18/2016	EISO	User education	User Education		EISO
Multiple Component	8/22/2016	8/25/2016	Not Applicable	Yes	User account confirmed disabled. Remove asset from access under discussion.	8/22/2016	8/25/2016			EISO	File criminal charges with police			

Incident Category	Date of Incident Occurrence	Discovered /Reported	Sensitivity of Information Involved	Security Breach	Containment Measures	Containment	Snr Mgmt Notification	External Notification	Investigation Complete	Investigated by	Recommendations	Manner of Recommendations Implementation	Recommendations Implemented	Implementer
Multiple Component	8/22/2016	8/22/2016	Business	No	User had plugged in an external USB containing zip file of English studying material. USB was removed from laptop and user was educated on corporate policy.	8/23/2016			8/23/2016	EISO	User education	Educated user on corporate security policy regarding USB drives.	8/23/2016	EISO
Inappropriate Use	8/27/2016	8/27/2016	Business	No	Communicated to user to run a full SCEP scan of his PC after alert was discovered. Screenshot of results indicate the PC is clean.	8/29/2016			8/29/2016	EISO	User education	Due to the confidential nature of the details of the analysis, CCO has excluded a description of the analysis from the public version of this report; however, these details have been provided to the IPC.Resulting scan was clean.	8/29/2016	EISO
Malicious Logic or Code	8/27/2016	8/27/2016	Business	No	Received alert regarding cached files under Google Chrome - appears to be a drive by download. Instructed user to run a full SCEP scan on her PC. Screenshot of the results came back clean.	8/29/2016			8/29/2016	EISO	User education	Routinely clear browser cache.	8/29/2016	EISO
Inappropriate Use	8/31/2016	8/31/2016	Not Applicable	No	SCEP found partial Chrome download file . Due to the confidential nature of the details of the analysis, CCO has excluded a description of the analysis from the public version of this report; however, these details have been provided to the IPC.	9/6/2016			9/6/2016	EISO	User education	Run a full SCEP scan Due to the confidential nature of the details of the analysis, CCO has excluded a description of the analysis from the public version of this report; however, these details have been provided to the IPC..	9/6/2016	EISO
Inappropriate Use	9/19/2016	9/19/2016	Not Applicable	No	User received an unsolicited email bounce back from an address	9/19/2016				EISO	User education	Recommended user to mark suspicious email as spam.	9/19/2016	EISO

Incident Category	Date of Incident Occurrence	Discovered /Reported	Sensitivity of Information Involved	Security Breach	Containment Measures	Containment	Snr Mgmt Notification	External Notification	Investigation Complete	Investigated by	Recommendations	Manner of Recommendations Implementation	Recommendations Implemented	Implementer
					she had not contacted. A malicious entity has been using her CCO email address as the "from" address. Advised to mark this as spam within the Outlook client. No further actions required.									
Malicious Logic or Code	9/21/2016	9/21/2016	Not Applicable	No	Malicious file identified as a cached html file on laptop. Instructed user's assistant to run a full SCEP scan. Results screenshot come back clean.	9/21/2016			9/21/2016	EISO	User education		9/21/2016	EISO
Inappropriate Use	9/25/2016	9/25/2016	Business	No	SCEP removed malicious file upon USB being plugged in to PC.	9/25/2016			9/26/2016	EISO	User education	Educated user via email to not use personal USBs with CCO assets as that can introduce malware. Due to the confidential nature of the details of the analysis, CCO has excluded a description of the analysis from the public version of this report; however, these details have been provided to the IPC.	10/6/2016	EISO
Malicious Logic or Code	9/29/2016	9/29/2016	Not Applicable	No	Malicious file identified in alert was quarantined. Requested user to run a full SCEP for good measure. Resulting screenshot was clean.	9/29/2016			9/30/2016	EISO	User education	Requested user to run a full SCEP for good measure. Resulting screenshot was clean.	9/30/2016	EISO
Malicious Logic or Code	9/30/2016	9/30/2016	Business	No	Instructed user to run a full SCEP scan.	10/3/2016			10/3/2016	EISO	User education	User had run a full SCEP scan as instructed.	10/3/2016	EISO
Malicious Logic or Code	10/11/2016	10/11/2016	Business	No	Notified user immediately of malicious cached file on his system and created a	10/11/2016			10/11/2016	EISO	User education	Run full SCEP scan to verify host file clean up & manually navigate to the	10/11/2016	EISO

Incident Category	Date of Incident Occurrence	Discovered /Reported	Sensitivity of Information Involved	Security Breach	Containment Measures	Containment	Snr Mgmt Notification	External Notification	Investigation Complete	Investigated by	Recommendations	Manner of Recommendations Implementation	Recommendations Implemented	Implementer
					ticket through Service Desk. Instructed user to run full SCEP scan and return results.							file to confirm removal of malicious file.		
Unauthorized Access	10/17/2016	10/17/2016	Business	No	Investigated. Research indicated that calendar permissions can end up corrupted if the meeting invite recipient is accessing the meeting invite through a mobile device. User had confirmed offender had accessed the meeting invite on his mobile device. No further meeting invites have been cancelled since.	10/17/2016			10/17/2016	EISO	User education	Recommended user to implement a disclaimer in meeting invites to avoid such an issue.	10/17/2016	EISO
Inappropriate Use	10/18/2016	10/18/2016	Not Applicable	No	Suspicious email reported by user is CCO's EISO Internal Phishing Campaign.	10/18/2016			10/18/2016	EISO	User education	Suspicious email reported by user is CCO's EISO Internal Phishing Campaign.		EISO
Malicious Logic or Code	10/20/2016	10/20/2016	Business	No	Notified affected user of malicious file not cleaned by SCEP and instructed him to run a full SCEP scan and to provide a screenshot. User had run a full SCEP scan as instructed but did not provide a screenshot. User re-ran scan and provided screenshot as proof.	10/21/2016			11/24/2016	EISO	User education	Full SCEP scan was run confirmed with screenshot and manually confirmed the file's removal.	10/21/2016	EISO

Appendix J: Indicators – Log of Statements of Purpose

Prescribed Entity

Data Holding	(1) Statement of Purpose & (2) Need for PHI	Data	Source
Brachytherapy Funding Program	1. The purpose of this data holding is to (1) maintain data related to reimbursement for prostate cancer patients in accordance with program guidelines for CCO's prescribed entity purpose and (2) to provide reimbursement for eligible prostate cancer patients that meet program guidelines on behalf of the MOHLTC 2. PHI is required to (1) conduct analyses and reporting to the MOHLTC on the Brachytherapy Program for health system planning purposes and (2) to reimburse eligible patients.	This dataset contains: • Clinical data • Demographic data	Referring physicians
Canadian Community Health Survey (CCHS)	1. The CCHS is a Statistics Canada Survey that collects information related to health status, heath care utilization, and health determinants for the Canadian population, for the purpose of monitoring the impact of prevention programs and policies. 2. CCO requires the data to monitor and report on the prevalence of cancer risk factors in Ontario and in particular subpopulations (*e.g.,* First Nations, Inuit, Metis populations). The data are also used to monitor factors that influence exposure to cancer risk factors (*e.g.,* socio-demographic characteristics, implementation of household smoking bans, etc.) and to quantify the burden of various cancers.	This dataset contains: • Demographic data (*e.g.,* birth date, sex, health problems, occupation and Ontario geographic codes • Health-related self-ratings (*e.g.,* re: healthy behaviours, health services utilization)	MOHLTC Ontario Sharing Files were provided by Statistics Canada and modified by MOHLTC before being shared with CCO.
Cancer Activity Level Reporting (ALR)	1. ALR data is collected for reporting and analysis purposes. It represents the basic set of data elements required to produce the quality, cost and performance indicators for the cancer system. 2. The PHI collected supports multiple programs at CCO, including the following: Radiation; Systematic; Psychosocial Oncology; Palliative; Smoking Cessation; Symptom Management; and the OCR.	This dataset contains: • Clinical data • Patient-level data	RCCs, hospitals and other healthcare delivery organizations
Case-By-Case Review Program (CBCRP)	1. The CBCRP database stores patient and treatment information about systemic therapy drug utilization at Ontario hospitals, for which reimbursement is being sought through the CBCRP according to strict eligibility criteria for both CCO's prescribed entity purpose and in order to process reimbursements on behalf of the MOHLTC . 2. PHI is required to (1) conduct analysis and reporting to the MOHLTC on the CBCRP for health system planning purposes and (2) to reimburse eligible patients.	This dataset contains: • Administrative Data • Clinical Data (eligibility criteria • Demographic Data	Hospitals
Collaborative Staging	1. The Collaborative Staging dataset is a standardized set of data elements that describe how far a cancer has spread at the time of diagnosis. It contains patient, tumour and additional disease-site specific factors that together derive the stage of the patient at the time of diagnosis. 2. CCO submits provincial stage data annually to NAACCR and Statistics Canada. Along with data from the OCR, cancer stage data is necessary to support cancer system surveillance, planning and management. PHI is necessary to enable comprehensive analysis and for linking to the OCR, screening, and treatment data.	The dataset contains: • Administrative data • Clinical data • Demographic data • Facility data	OCR Pathology Data Mart Hospital patient health records
Complex Continuing Care Reporting and Complex Continuing Care (CCRS) – Institute for Clinical Evaluative Studies (ICES)	1. The CCRS is used to support standardized reporting in LTCHs, personal care homes, and nursing homes. 2. CCO requires the data to support 4 business streams: a. ATC: develop patient flow models for Ontario, support evaluation of Ministry-led initiatives, and support the Ontario's Seniors Strategy b. ORN: conduct analyses to understand how CKD patients interact with the healthcare system. c. Strategic Analysis & Modelling: develop patient flow models	This dataset contains: • Administrative data • Clinical data • Demographic data	Institute for Clinical Evaluative Science (ICES)

Data Holding	(1) Statement of Purpose & (2) Need for PHI	Data	Source
	d. Cancer Program: explore barriers in palliative care access		
Complex Continuing Care Reporting and Complex Continuing Care (CCRS) – Ministry of Health and Long Term Care (MOHLTC)	1. This data is used for the purpose of patient-based funding analysis. 2. CCO requires the data to carry out patient-based funding analysis	Data elements include health card number, sex, and birth date and client postal code.	MOHLTC
Mortality Data	1. The purpose of this data holding is for CCO to receive mortality data which contains the date of death and cause of death for Ontario residents who have died in Ontario for planning and management purposes. 2. PHI is collected to measure cancer survival.	The dataset contains: • Administrative data • Demographic data	Ministry of Government Services Office of the Registrar General
Diagnostic Assessment Program – Electronic Pathway Solution (DAP-EPS)	1. The purpose of the data holding is to securely store data (including PHI) collected from all regional cancer programs for DAP oversight. 2. PHI is collected to evaluate the impact DAPs have on patients in the diagnostic phase of the cancer journey.	This data holding contains the following categories of data: • Administrative data • Clinical data • Demographic data • Usage data • Wait Times data	Hospitals
Diagnostic Assessment Program – Diagnostic Data Upload Tool (DAP – DDUT)	1. The purpose of the data holding is to securely store data (including PHI) collected from all regional cancer programs for DAP oversight. 2. PHI is collected to evaluate the impact DAPs have on patients in the diagnostic phase of the cancer journey.	This data holding contains the following categories of data: • Administrative data • Clinical data • Demographic data • Usage data • Wait times data	Hospitals
Discharge Abstract Database (DAD)	DAD contains summary diagnostic and treatment information about patients who have received healthcare services as an inpatient (including acute care, chronic care and rehabilitation care) in Ontario hospitals.	The dataset contains: • Administrative data • Clinical data • Demographic data	CIHI
Dyspnea Management Program	1. The purpose of the data holding is to securely store data (including PHI) collected from 6 hospital sites for the dyspnea management pilot project. 2. PHI is collected to evaluate the impact that dyspnea management has on lung cancer patients, whether a subset of patients benefit from counselling and to determine if counselling results in any secondary impacts on the health system.	This dataset contains: • Clinical data • Demographic data	Hospitals
Emergency Department (ED) Patient Satisfaction Survey Data	1. To assist with patient satisfaction reporting. All P4R hospitals were required to conduct patient satisfaction surveys and ATC reported back on the results across the province. 2. ATC did not need the PHI for the operational reporting there have been ad-hoc requests that involve linking data to other administrate databases (*i.e.,* NACRS).	Demographic information (age, postal code, gender), visit information (chart # reg #, site, timestamps)	Hospitals

Data Holding	(1) Statement of Purpose & (2) Need for PHI	Data	Source
Emergency Room National Ambulatory Reporting System Initiative (ERNI)	1. The purpose of this data holding is to evaluate ER wait times for provincial ER/ALC Strategy, including but not limited to return on investment, performance improvement, Ministry LHIN Performance Agreements and data quality assessment. 2. PHI is collected to determine and remove duplicate data entry errors from the analysis as well as to calculate percentage of patients returning to an ER within a specified time period as a measure of quality of care and potential negative impact of ER focus.	The dataset contains: • Clinical data • Demographic data	Hospital sites submit to CIHI NACRS. Extract of file is transferred securely from CIHI to ATC Informatics within CCO using Tumbleweed
eOutcomes – Head & Neck Cancer	1. The purpose of the data holding is to capture and monitor outcomes data for patients with head and neck cancer treated with radiotherapy in a provincial, systematic way. 2. PHI is collected to ensure accurate capture of patients' outcomes post-radiotherapy, and to facilitate the identification of inadvertent duplicate cases.	This dataset contains: • Clinical data (*e.g.,* outcomes, diagnosis, radiotherapy details) • Demographic data (patient name, MRN)	Physicians/Data Managers (outcomes) ALR Data (diagnosis, radiotherapy details)
ePath	1. The Pathology Database is comprised of patient and tumour information for cancer and cancer-related pathology reports (tissue, cytology), submitted from public hospital (and some commercial) laboratories. ePath documents patient, facility, and report identifiers, and tumour identifiers, such as site, histology and behaviour. 2. PHI is used to support management decision-making, planning, disease surveillance and research, as well as contributing to resolved incidence case data in the OCSR.	The dataset contains: • Administrative data • Clinical data • Demographic data • Facility data	Hospitals Some commercial laboratories
Evidence-Based Program (EBP)	1. The EBP database stores patient and treatment information about systemic therapy drug utilization at Ontario hospitals. 2. PHI is required to conduct analysis and reporting to the MOHLTC on the EBP for health system planning purposes. a.	This dataset contains: • Administrative Data • Clinical Data (eligibility criteria) • Demographic Data	Hospitals
Health Based Allocation Model (HBAM) Impatient Group (HIG)	1. The purpose of this dataset is to inform the funding methodology being used for cancer quality-based procedures. 2. This data is needed to determine funding at a patient level for cancer quality-based procedures.	This dataset contains replica components of DAD and NACRS data	CIHI
Incident Case Level Stage Data	1. This linked data set indicates staging data created from OCRIS and ALR source records using SAS and is a characteristic of cases of cancer in the OCR. 2. This PHI is needed to accurately attribute the correct stage to its case, and accurately present the real person, case and stage for granular analysis (*e.g.,* one hospital, one local, one cancer type, patient contact studies, etc.). Note that "person" is only defined by a machine generated ID number.	The dataset contains • Clinical data • Patient-level data	OCRIS and ALR
Interim Annotated Tumour Project (ATP) Database	1. The Interim ATP Database provides an integrated set of data, combining tumour information from the Ontario Institute for Cancer Research (**OICR**)'s Tumour Bank with CCO's OCSR, for the purpose of increasing the accuracy and utility of the information for both researchers and CCO planners. 2. PHI is used by researchers to study the association between genetics and response to cancer drugs. CCO also uses the PHI in this data holding to create clinical guidelines for the care and treatment of cancer patients in Ontario.	The dataset contains: • Administrative data • Clinical data • Demographic data	OICR CCO's Cancer Registry

Data Holding	(1) Statement of Purpose & (2) Need for PHI	Data	Source
Magnetic Resonance Imaging (MRI)	1. The MRI Efficiency data is used to produce the MRI Efficiency Program Dashboard to understand wait times for MRI procedures in Ontario hospitals. 2. MRN number is used to calculate MRI wait times for each unique patient.	The Dataset contains: • MRN • Patient Type • Procedure Name	Hospitals
Multidisciplinary Cancer Conference (MCC)	1. The purpose of the data holding is to obtain a better understanding of the outcome of individuals being discussed at MCCs (*e.g.,* other patient conditions, or other patient treatments), as well as to analyze patient movement within and between facilities. 2. PHI is collected to conduct analysis and provide operational advice with respect to MCC initiatives in Ontario, to the MOHLTC, the MCC facilities, and the LHINs.	This dataset contains: • Administrative data • Clinical data	Hospitals
National Ambulatory Care Reporting System (NACRS)	NACRS contains summary diagnostic and treatment information about patients who have received outpatient surgery or selected other treatments (chemotherapy, emergency department visits, dialysis and cardiology) in Ontario hospitals.	The dataset contains: • Administrative data • Clinical data • Demographic data	CIHI
National Rehabilitation Reporting System (NRS)	1. NRS contains client data collected from participating adult inpatient rehabilitation facilities and programs across Canada. 2. CCO requires the data to support 4 business streams: a. ATC: develop patient flow models for Ontario, support evaluation of Ministry-led initiatives, and support the Ontario's Seniors Strategy. b. ORN: conduct analyses to understand how CKD patients interact with the healthcare system. c. Strategic Analysis & Modelling: develop patient flow models. d. Cancer Program: explore barriers in palliative care access.	Data elements include: • Administrative data • Clinical data • Demographic data	Institute for Clinical Evaluative Sciences (ICES) Participating adult inpatient rehabilitation facilities and programs across Canada (*e.g.,* hospital rehabilitation units, designated rehabilitation beds)
New Drug Funding Program (NDFP)	1. The NDFP database stores patient and treatment information about systemic therapy drug utilization at Ontario hospitals. 2. . PHI is required to conduct analysis and reporting to the MOHLTC on the NDFP for health system planning purposes.	This dataset contains: • Administrative data • Clinical data (eligibility criteria) • Demographic data	Hospitals
Ontario Drug Benefit (ODB)	1. The ODB database stores patient and treatment information about systemic therapy drug utilization at Ontario hospitals. 2. CCO (in particular the NDFP and PDRP) need information about the volumes of oral chemotherapy drug units that are dispensed.	Data elements include: • Drug identifier • LTC indicator • Patient pharmacy • Physician identifiers Each record is a separate drug claim.	Institute for Clinical Evaluative Sciences (ICES) The pharmacist submits a claim for each prescribed drug that is covered under the ODB formulary, and each dispensed claim forms a record in the ODB database.
Ontario Association of Community Care Access Centres (OACCAC): **- Home Care Database** **- Resident Assessment Instrument (RAI) – Home Care** **- RAI – Contact Assessment** **- RAI – Palliative Care**	1. The OACCAC contains data on Ontario's 14 CCACs, and includes four data holdings. The data is used for the purpose of home care, care in the community, and hospice and palliative care. 2. Purposes are divided into 4 business streams, per below: a. Health System Funding Reform: analyze service utilization and enhance quality-based funding model based on the findings. b. ATC: pathway modelling for ALC patients c. ORN: understand wait times for LTC and dialysis service utilization by patients with end-stage renal disease;	Data elements include: • Demographic data (*e.g.,* HIN, sex, birth date, geography) • Clinical data (*e.g.,* outcomes of RAI assessment in home care, receipt of health services) • Administrative data (*e.g.,* HIN, admission and discharge date for home care)	Ontario's CCACs

Data Holding	(1) Statement of Purpose & (2) Need for PHI	Data	Source
	understand community service utilization for patients with CKD; using this knowledge to identify potential areas for coordination of care d. Cancer Clinical Programs: understand end-of-life care for cancer patients.		
Ontario Cancer Registry Information System (OCRIS)	1. The OCR is a computerized database of information on all Ontario residents who have been newly diagnosed with cancer ("incidence") or who have died of cancer ("mortality"). All new cases of cancer are registered, except non-melanoma skin cancer. This information is used to support management decision-making, planning, disease surveillance and research. 2. PHI is collected to link records and establish which records belong to which patient. The PHI is frequently required by internal and external researchers. The Canadian Cancer Registry MOU contains the requirement that PHI be included in CCO annual submissions of newly diagnosed patients.	The dataset contains: • Administrative data • Clinical data • Demographic data	CIHI (DAD, NACRS) ALR (RCC and PMH reporting through Databook) Pathology Information Management System (**PIMS**), anatomical pathology reports from Ontario public and private laboratories Ontario Registrar General's Office, Mortality files enhanced by death certificate notifications from Statistics Canada for Ontario residents deaths in other provinces/territories Out of Province, notifications from other provinces/territories of Ontario residents diagnosed or treated in the notifying P/T
Ontario Cancer Symptom Management Collaborative (OCSMC) Symptom Management Database	1. The Symptom Management Reporting Database was developed in order to assess the goal of OCSMC, which is to improve symptom management and collaborative palliative care planning through earlier identification, documentation and communication of patients' symptoms and performance status. 2. PHI is collected to evaluate the provision of symptom management and palliative care planning for cancer patients in Ontario.	This dataset contains: • Clinical data • Demographic data	Hospitals
Ontario Laboratories Information System (OLIS)	1. To support CCO's ORN and DAP-EPS Programs in accordance with CCO's Data Privacy Agreement with the MOHLTC as a PE, as amended. 2. PHI is required to enable CCO to link OLIS data with its patient records within other PE data holdings – such linkage is required to carry out health analytics.	This dataset contains: • Laboratory test result information from patients across Ontario	MOHLTC (via eHealth Ontario)
Ontario Mental Health Reporting Systems (OMHRS)	1. The OMHRS collects data on patients in adult designed inpatient mental health beds. This includes beds in General, Provincial Psychiatric, and Specialty Psychiatric facilities. RAI – Mental Health is used to collect the data. 2. CCO's ATC requires the information to better understand ALC in Ontario, and to support Ministry-led initiatives such as Ontario's Seniors Strategy.	Data elements include: • Administrative data • Clinical data • Demographic data	Institute for Clinical Evaluative Sciences (ICES) Originally collected from general, provincial psychiatric, and specialty psychiatric facilities.
Ontario Evidence-Based Positron Emission Tomography (EB-PET) Program	1. The purpose of this data holding is to carry out CCO's mandate to operate the evidence-based PET Scans Ontario Program. 2. PHI is collected by CCO to: • Provide direction to the PET Steering Committee and/or MOHLTC • Link to other data holdings for reporting and analysis for the evaluation and management of the PET Scans Ontario Program.	This dataset contains: • Administrative data • Clinical data • Patient demographic data • Physician demographic data	Referring physicians Diagnostic centres

Data Holding	(1) Statement of Purpose & (2) Need for PHI	Data	Source
Ontario Renal Network (ORN)	1. The purposes of the ORN data holding are: • Performance measurement and management; • Monitoring of system quality; • Funding; • Data quality; • System planning; and • CKD funding model development. 2. PHI is used to support management, funding, data QA, decision-making, planning, and disease surveillance and research activities.	The dataset contains: • Clinical data • Demographic data • Service volumes	Hospitals (ORRS) MOHLTC Sunnybrook Research Institute (**SRI**)
Out-of-Country (OOC)	1. The OOC data holding stores information about reimbursement for out of province/OOC cancer drugs or treatment. We use it as a PE to monitor trends in OOC services – for example to identify if a trend is occurring for one treatment, and to identify if and when it is more effective to deliver treatments in the province. It is also used for purposes of reimbursing patients on behalf of the MOHLTC. 2. PHI is needed to (1) conduct analysis and reporting to the MOHLTC on the OOC program for health system planning purposes (2) to reimburse eligible patients.	This dataset contains: • Administrative data • Clinical data	MOHLTC
Out of Province (OOP) Data	1. This data holding contains persons with OCSR reportable diseases. The purpose of these records is to serve as source records to create incident cases for the EDW-OCSR. Both alone, and as source records for incident cases, OOP data support management decision-making, planning, disease surveillance and research. 2. PHI is collected to ensure accuracy in linking records in EDW. PHI is used by internal and external researchers at the source record level.	This dataset will contain: • Administrative data • Clinical data • Demographic data	Out of Province Notifications from other provinces/territories of Ontario residents diagnosed or treated for cancer in the notifying P/T
Pathology Data Mart	1. This data holding is derived from the PIMS data holding and uploaded into the EDW for planning and management purposes. 2. PHI is used to support management decision-making, planning, disease surveillance and research, as well to contribute to resolving incidence case data in the OCSR.	This dataset contains: • Administrative data • Clinical data • Demographic data • Facility data	PIMS
Registered Persons Database (RPDB) Data Mart	The RPDB is a listing of all persons insured under OHIP. This data is used to ensure that individuals in other data sources are identified correctly and to support analysis by demographic groups and geography.	This dataset contains: • Administrative data • Demographic data • HIN	MOHLTC
Specialized Services Oversight Information System (SSOIS)	1. The purpose of the SSOIS data is to support planning, funding and forecasting for specialized cancer services within Ontario. 2. PHI is collected to calculate specific indicators and measures to gain a better understanding of volume and performance of specialized cancer services.	This dataset contains: • Administrative data • Clinical data • Patient Demographic data	Hospitals
Stem Cell Transplant (SCT)	1. The purpose of the SCT data set is to support planning, funding and forecasting of SCTs within Ontario. 2. PHI is collected to calculate specific indicators and measures that are required to support the Goals and Objectives framework for the SCT project.	This dataset contains: • Clinical/SCTs data • File descriptor data • Patient demographic data	Hospitals
Systemic Treatment Funding Model (STFM)	1. The purpose of the STFM PHI is to determine a funding model driven by systemic treatment activity data reported by cancer centres and hospitals. 2. PHI is needed to determine funding allocations for hospitals, on a patient-level basis.	This data holding includes: • Clinical • patient level data (Same as ALR)	From CCO's Activity-Level Reporting (ALR) data holding. Files originate from treating cancer centres and hospitals and are reported on a monthly basis.

Data Holding	(1) Statement of Purpose & (2) Need for PHI	Data	Source
Wait Times Information System (WTIS)	1. The purpose of the WTIS data holding is to enable the monitoring of wait times. The Ontario Wait Time Strategy implemented the web-based WTIS to facilitate wait time management and to provide the public with wait time information on surgical and diagnostic procedures. 2. PHI is collected from hospitals and the Enterprise Master Patient Index (**EMPI**) (which interfaces with the WTIS in order to organize patient information) and is used for the planning and management of the healthcare system.	This dataset contains: • Administrative data • Clinical data • Demographic data	Hospitals EMPI

Prescribed Person

Data Holding	(1) Statement of Purpose & (2) Need for PHI	Data	Source
Colon Cancer Check (CCC) Interim Solution	System no longer used, required for Data migration, Archive and Audit only 1. The purpose of the data holding is to securely store data (including PHI) to support CCC Screening Operations. 2. PHI is collected for CCC client management and operations including, clinical results, direct client interactions and correspondence.	This dataset contains: • Clinical data • Demographic and address data • Call Centre operational activities data	• MOHLTC • Laboratories • FH • Call Centre direct data entry.
Colon Cancer Check (CCC) List Management System (LMS)	1. The purpose is to support CCC Screening Operations. 2. PHI is collected for data exchange to and from Health Service Providers via secure web portal ("OMD") as well as for validation of patient lists and electronic distribution of Provider Reports.	This dataset contains: • Clinical data • Client Demographic data • Provider Demographic and Address data	• CCC - Siebel
Siebel	1. The purpose of this data holding is to support Integrated Screening Operations, Planning and Performance. 2. Integrated Screening Siebel CRM system. It is a front end system for InScreen client management and operations including, Clinical Results, direct client interaction and Correspondence.	This dataset contains: • Clinical data • Demographic and address data • Call Centre operational activities data	• MOHLTC (RPDB, HNS, CHDB, CPDB, CAPE) • Laboratory (LRT) • Hospital (CIRT) • FH • Statistics Canada (PC to LHIN) • Call Centre direct data entry
Screening Hub Integration	1. The purpose of this data holding is to support Integrated Screening Operations, Planning and Performance. 2. InScreen Integration Hub (Customer Data Integration) to support downstream InScreen information and data requirements. *E.g.,* Siebel InScreen and Data Mart reporting. Various sources from MOHLTC, Siebel InScreen, Statistics Canada and CCO are standardized, cleansed and integrated for downstream operations.	This dataset contains: • Clinical data • Demographic and address data • Call Centre operational activities data	• MOHLTC (RPDB, HNS, CHDB, CPDB, CAPE) • Laboratory (LRT) • Hospital (CIRT) • FH (Correspondence) • Statistics Canada (PC to LHIN) • Siebel Call Centre
Screening Hub Stage – Client Agency Program Enrollment (CAPE)	1. The CAPE data set will be used to identify physicians in Ontario who have rostered patients. 2. This information will be used to compile a list of eligible rostered patients who will be invited to participate in the CCC program.	This dataset contains: • Administrative Physician Data • HIN	• MOHLTC

Data Holding	(1) Statement of Purpose & (2) Need for PHI	Data	Source
Screening Hub Stage – Claims History Database (CHDB)	1. The claims data received will be used to determine volumes of non-program FOBT kits processed and validating performance of facilities and physicians who have conducted Colonoscopies. 2. It will also be used as criteria for identifying the candidate population for the invitation pilot.	This dataset contains: • Administrative Care • Clinical Data • PHI	• MOHLTC
Screening Hub Stage – Colonoscopy Interim Reporting Tool (CIRT)	1. The purpose of this data holding is to understand colonoscopy activity conducted within participating facilities. 2. The data collected through CIRT will be used to understand colonoscopy activity conducted within participating facilities from volume, wait time and quality perspectives. It is also used to determine funding and volume allocations across participating facilities.	This dataset contains: • Administrative Care • Clinical Data • PHI	• Hospitals
Screening Hub Stage – Lab Reporting Tool (LRT)	1. The purpose of this data holding is to gather information from laboratories on FOBT results. 2. The data collected through the LRT are FOBT results that is used for (a) generate participant communications; and (b) monitoring and reporting on FOBT volumes, geographic differences, test quality, variations between participating laboratories and highlighting the need for further awareness or education programs.	This dataset contains: • Administrative Care • Clinical Data • PHI	• Laboratories
Screening Hub Stage - Ontario Public Drug Programs (OPDP)	1. The purpose of this data holding is to gather information of FOBT dispensed by pharmacies. 2. This data will be used to evaluate the level of dispensing of FOBT kits at the pharmacies.	This dataset contains • Administrative Pharma Data • PHI	• MOHLTC
Screening Hub Stage – Ontario Cancer Registry OCR	1. The OCR is a computerized database of information on all Ontario residents who have been diagnosed with cancer ("incidence") and/or who have died of cancer ("mortality"). All new cases of cancer are registered, except non-melanoma skin cancer. 2. This information is used to support OCSR by identifying individuals who are ineligible for colorectal and cervical screening.	This dataset contains: • Administrative Care • Clinical Data • PHI	• CCO as PE
Screening Hub Stage – Registered Persons Database (RPDB)	1. This data holding contains information from Registered Person Database. This data is used in operationalization of colorectal and cervical screening. 2. This data will be used to identify Ontarians who are eligible and could be invited to participate in the CCC program. It will also be used for identity validation and data linking for client cancer journey assessment.	The dataset contains: • Administrative Care • Clinical Data • PHI	• MOHLTC
Screening Hub Stage - Siebel	1. The purpose of this data holding is to integrate information for InScreen. 2. Recent Client, Address and Screening related activity within Siebel InScreen, required in the Screening Hub for integration purposes.	The dataset contains: • Client demographics and address information • PHI	• Integration Hub • Call Centre direct entry
Primary Care Provider Reporting **This is the same as the Primary Care Screening Activity Report (PC SAR)**	1. This data holding contains information on primary care providers. 2, This is used to store primary care provider SARs. The reports summarizes client level information for providers.	This dataset contains: • Clinical data • PHI	• Integration Hub • Siebel

Data Holding	(1) Statement of Purpose & (2) Need for PHI	Data	Source
Cytobase	1. The purpose of this data holding is: -to carry out the mandate of the CSP -to facilitate the provision of health care related to cervical cancer screening to allow CCO to notify participants of their results -to maintain the OCSR -to conduct cancer planning and management as well as to perform quality and program management functions.	This dataset contains: • Demographic data about the patient, the requesting physician and the laboratory that assessed the test • Health information number • cervical test result	CytoBase
Oracle Business Intelligence Enterprise Edition (OBIEE)	1. The purpose of this data holding is to provide segmentation of data which enables Siebel CRM, via Campaign Management, to generate invitation, reminder, recall and test result notification correspondence for each of the three Cancer Screening modules (CCC, OCSP and OBSP).	This dataset contains: • Clinical data • Demographic and address data • Call Centre operational activities data	• This dataset is populated with data from Siebel CRM and the Integration Hub.
Mortality Data	1. The purpose of this data holding is for CCO to receive mortality data which contains the date of death and cause of death for Ontario residents who have died in Ontario for planning and management purposes. 2. PHI is collected to identify cases for the Ontario Cancer Screening Registry and for measuring cancer survival.	The dataset contains: • administrative data • demographic data	• Ministry of Government Services • Office of the Registrar General
Integrated Client Management System (ICMS)	OBSP screening data entered directly from screenings sites into the CCO ICMS Oracle database – this is the operational database used for recruiting, registering, booking, capturing results and reporting results to clients and physicians, film tracking, assessment results capture, recall letters, and operational & management level reporting 1. The purpose of this data holding is to store screening information for those clients participating in the OBSP program. 2. PHI is collected to implement, plan, manage, evaluate, allocate resources to and report on performance of the OBSP. PHI is also collected for OBSP client management and operations, including clinical results, direct client interactions and correspondence.	Clinical data (screening results, clinical history, assessments information, Screening appointment information, Demographic data, Physician information	
Data Submission Portal (DSP) – Registered Nurse Flexible Sigmoidoscopy (RNFS)	Registered Nurse Flexible Sigmoidoscopy information as reported by participating sites for use within the CCC Screening Program 1. This is the landing area for the raw data submissions from participating hospitals, use the Integration Hub or Siebel for standardized and integrated information.	Program participant, responsible physician, nurse and Flexible Sigmoidoscopy procedure details	
Hub: Fulfilment House (FH)	Correspondence feedback file information regarding Address corrections, Mailing Status and Return Mail from the FH for InScreen Campaign/Correspondence operations. 1. This is the landing area for the raw data extracts from the FH, use the Integration Hub or Siebel for standardized and integrated information.		

Appendix K: Log of Privacy Complaints

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-MF76B	OCSP	7-Jan-14	Yes, further investigation is required.	7-Jan-14	N/A	7-Jan-14	Contact Centre Agent	8-Apr-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	27-Dec-13	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is satisfied.
1-MG5TR	OCSP	9-Jan-14	Yes, further investigation is required.	9-Jan-14	N/A	9-Jan-14	Contact Centre Agent	9-Jan-14	Provide the client further explanation about the nature of the screening programs. Clarify client's misunderstanding/concerns about the letters.	Contact Centre Agent	9-Jan-14	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is satisfied.
1-MM4PB	OCSP	10-Jan-14	Yes, further investigation is required.	10-Jan-14	N/A	10-Jan-14	Contact Centre Agent	10-Jan-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	10-Jan-14	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is satisfied.
1-MM57E	OCSP	10-Jan-14	Yes, further investigation is required.	10-Jan-14	N/A	N/A	Contact Centre Agent	10-Jan-14	No further action required/possible.	Contact Centre Agent	10-Jan-14	No further action required/possible.
1-MM5BH	OCSP	10-Jan-14	Yes, further investigation is required.	10-Jan-14	N/A	10-Jan-14	Contact Centre Agent	10-Jan-14	Provide client instructions and requirements for withdrawal from screening correspondence program.	Contact Centre Agent	10-Jan-14	No further action required/possible.

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-NFHWP	OCSP	21-Jan-14	Yes, further investigation is required.	21-Jan-14	N/A	21-Jan-14	Contact Centre Agent	21-Jan-14	Provide the client further explanation about the nature of the screening programs and mailing logistics. Update client address/withdraw (facilitate as required).	Contact Centre Agent	21-Jan-14	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is satisfied.
1-NPUX9	OCSP	24-Jan-14	Yes, further investigation is required.	24-Jan-14	N/A	24-Jan-14	Contact Centre Agent	24-Jan-14	Provide the client further explanation about the nature of the screening programs. Clarify client's misunderstanding/concerns about the letters.	Contact Centre Agent	24-Jan-14	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is satisfied.
1-NPV31	OCSP	24-Jan-14	Yes, further investigation is required.	24-Jan-14	N/A	24-Jan-14	Contact Centre Agent	24-Jan-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	24-Jan-14	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is satisfied.
1-NWY23	OCSP	27-Jan-14	Yes, further investigation is required.	27-Jan-14	N/A	27-Jan-14	Contact Centre Agent	27-Jan-14	Provide the client further explanation about the nature of the screening programs and options to withdraw (facilitate as required).	Contact Centre Agent	27-Jan-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-ODUE8	OCSP	31-Jan-14	Yes, further investigation is required.	31-Jan-14	N/A	31-Jan-14	Contact Centre Agent	31-Jan-14	Provide the client further explanation about the nature of the screening programs. Clarify client's misunderstanding/concerns about the letters.	Contact Centre Agent	31-Jan-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client satisfied with response.
1-OTKK0	OCSP	6-Feb-14	Yes, further investigation is required.	2-Feb-14	N/A	2-Feb-14	Contact Centre Agent	2-Feb-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	2-Feb-14	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is not satisfied with the legislation; informed management, provided IPC contact information.
1-PAANX	OCSP	11-Feb-14	Yes, further investigation is required.	11-Feb-14	N/A	11-Feb-14	Contact Centre Agent	11-Feb-14	Provide the client further explanation about the nature of the screening programs. Clarify client's misunderstanding/concerns about the letters.	Contact Centre Agent	11-Feb-14	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is satisfied.
1-PAC3C	OCSP	11-Feb-14	Yes, further investigation is required.	11-Feb-14	N/A	11-Feb-14	Contact Centre Agent	11-Feb-14	Provide the client further explanation about the nature of the screening programs. Clarify client's misunderstanding/concerns about the letters.	Contact Centre Agent	11-Feb-14	Provided the client explanation about the screening programs & option to withdraw. Client does not want to withdraw from

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
												correspondence.
1-PAITO	OCSP	12-Feb-14	Yes, further investigation is required.	12-Feb-14	N/A	12-Feb-14	Contact Centre Agent	12-Feb-14	Provide the client further explanation about the nature of the screening programs and options to withdraw (facilitate as required).	Contact Centre Agent	12-Feb-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-PAIRD	OCSP	12-Feb-14	Yes, will be investigated.	12-Feb-14	N/A	N/A	Contact Centre Agent	12-Feb-14	No further action required/possible.	Contact Centre Agent	12-Feb-14	No further action required/possible.
1-Q62CY	OCSP	20-Feb-14	Yes, further investigation is required.	20-Feb-14	N/A	20-Feb-14	Contact Centre Agent	27-Feb-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	27-Feb-14	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is satisfied.
1-QMSL1	OCSP	25-Feb-14	Yes, further investigation is required.	25-Feb-14	N/A	25-Feb-14	Contact Centre Agent	25-Feb-14	Provide the client further explanation about the nature of the screening programs and options to withdraw (facilitate as required).	Contact Centre Agent	25-Feb-14	Provided the client explanation about the screening programs & option to withdraw. Client does not want to withdraw from correspondence.
1-QMW36	OCSP	26-Feb-14	Yes, further investigation is required.	26-Feb-14	N/A	26-Feb-14	Contact Centre Agent	26-Feb-14	Provide the client further explanation about the nature of the screening programs and options to withdraw (facilitate as required).	Contact Centre Agent	26-Feb-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-QMW3N	OCSP	26-Feb-14	Yes, will be investigated.	26-Feb-14	N/A	N/A	Contact Centre Agent	26-Feb-14	No further action required/possible.	Contact Centre Agent	26-Feb-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-QMX90	OCSP	26-Feb-14	Yes, further investigation is required.	26-Feb-14	N/A	26-Feb-14	Contact Centre Agent	26-Feb-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	26-Feb-14	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is satisfied.
1-R7LEX	OCSP	13-Mar-14	Yes, further investigation is required.	13-Mar-14	N/A	13-Mar-14	Contact Centre Agent	13-Mar-14	Provide the client further explanation about the nature of the screening programs and options to withdraw (facilitate as required).	Contact Centre Agent	13-Mar-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-RJ0YV	OCSP	25-Mar-14	Yes, will be investigated.	25-Mar-14	N/A	N/A	Contact Centre Agent	7-Jul-14	Anonymous Client, attempt to contact if possible and address complaint.	Contact Centre Agent	25-Mar-14	Anonymous client, could not be identified, no further action possible.
1-RJB5U	OCSP	25-Mar-14	Yes, further investigation is required.	25-Mar-14	N/A	25-Mar-14	Contact Centre Agent	16-May-14	Provide client instructions and requirements for withdrawal from screening correspondence program.	Contact Centre Agent	25-Mar-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-RJGY2	OCSP	26-Mar-14	Yes, further investigation is required.	26-Mar-14	N/A	26-Mar-14	Contact Centre Agent	26-Mar-14	Provide client instructions and requirements for withdrawal from screening correspondence program.	Contact Centre Agent	26-Mar-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-SG2I3	SAR	7-Apr-14	Yes, further investigation is required.	7-Apr-14	N/A	7-Apr-14	Contact Centre Agent	8-Apr-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	7-Apr-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client unhappy about the legislation.
1-SGVJR	CCC	7-Apr-14	Yes, will be investigated.	7-Apr-14	N/A	7-Apr-14	Contact Centre Agent	9-Apr-14	No further action required/possible.	Contact Centre Agent	7-Apr-14	No further action required/possible.
1-SG2LP	OCSP	7-Apr-14	Yes, further investigation is required.	7-Apr-14	N/A	7-Apr-14	Contact Centre Agent	7-Apr-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	7-Apr-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client satisfied with response.
1-SHBPP	OCSP	8-Apr-14	Yes, further investigation is required.	8-Apr-14	N/A	8-Apr-14	Contact Centre Agent	8-Apr-14	Provide the client further explanation about the nature of the screening programs and options to withdraw (facilitate as required).	Contact Centre Agent	8-Apr-14	Provided the client explanation about the screening programs & option to withdraw. Client does not want to withdraw from correspondence.
1-SHC5M	OCSP	8-Apr-14	Yes, further investigation is required.	8-Apr-14	N/A	8-Apr-14	Contact Centre Agent	8-Apr-14	Provide the client further explanation about the nature of the screening programs and options to withdraw (facilitate as required).	Contact Centre Agent	8-Apr-14	Provided the client explanation about the screening programs & option to withdraw. Client does not want to withdraw from correspondence.

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-SHC30	Screen for Life	8-Apr-14	Yes, further investigation is required.	8-Apr-14	N/A	8-Apr-14	Contact Centre Agent	8-Apr-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	8-Apr-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client unhappy about the legislation.
1-SHDHJ	Screen for Life	8-Apr-14	Yes, further investigation is required.	8-Apr-14	N/A	8-Apr-14	Contact Centre Agent	8-Apr-14	Provide the client further explanation about the nature of the screening programs and options to withdraw (facilitate as required).	Contact Centre Agent	8-Apr-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-SHGIH	Screen for Life	9-Apr-14	Yes, will be investigated.	9-Apr-14	N/A	9-Apr-14	Contact Centre Agent	9-Apr-14	Anonymous Client, attempt to contact if possible and address complaint.	Contact Centre Agent	9-Apr-14	Anonymous client, could not be identified, no further action possible.
1-SHIUZ	OCSP	9-Apr-14	Yes, will be investigated.	9-Apr-14	N/A	9-Apr-14	Contact Centre Agent	9-Apr-14	Anonymous Client, attempt to contact if possible and address complaint.	Contact Centre Agent	9-Apr-14	Anonymous client, could not be identified, no further action possible.
1-SHJLX	OCSP	9-Apr-14	Yes, will be investigated.	9-Apr-14	N/A	9-Apr-14	Contact Centre Agent	9-Apr-14	No further action required/possible.	Contact Centre Agent	N/A	Anonymous client, could not be identified, no further action possible.
1-SHJUL	OCSP	9-Apr-14	Yes, will be investigated.	9-Apr-14	N/A	9-Apr-14	Contact Centre Agent	9-Apr-14	Anonymous Client, attempt to contact if possible and address complaint.	Contact Centre Agent	9-Apr-14	Anonymous client, could not be identified, no further action possible.
1-SKGAU	OCSP	10-Apr-14	Yes, further investigation is required.	10-Apr-14	N/A	10-Apr-14	Contact Centre Agent	10-Apr-14	Provide the client further explanation about the nature of the screening programs and options to withdraw (facilitate as required).	Contact Centre Agent	10-Apr-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-SKGYG	Screen for Life	10-Apr-14	Yes, further investigation is required.	10-Apr-14	N/A	10-Apr-14	Contact Centre Agent	10-Apr-14	Provide the client further explanation about the nature of the screening programs and options to withdraw (facilitate as required).	Contact Centre Agent	10-Apr-14	Provided the client explanation about the screening programs & option to withdraw. Client does not want to withdraw from correspondence.
1-SKJ8D	OCSP	10-Apr-14	Yes, further investigation is required.	10-Apr-14	N/A	10-Apr-14	Contact Centre Agent	10-Apr-14	Provide the client further explanation about the nature of the screening programs and options to withdraw (facilitate as required).	Contact Centre Agent	10-Apr-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-SKPNH	OCSP	10-Apr-14	Yes, further investigation is required.	10-Apr-14	N/A	10-Apr-14	Contact Centre Agent	10-Apr-14	Provide the client further explanation about the nature of the screening programs and mailing logistics. Update client address/withdraw (facilitate as required).	Contact Centre Agent	10-Apr-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-SKPUR	CCC	10-Apr-14	Yes, further investigation is required.	10-Apr-14	N/A	10-Apr-14	Contact Centre Agent	10-Apr-14	Provide the client further explanation about the nature of the screening programs and options to withdraw (facilitate as required).	Contact Centre Agent	10-Apr-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-SKPQU	OCSP	10-Apr-14	Yes, further investigation is required.	10-Apr-14	N/A	10-Apr-14	Contact Centre Agent	10-Apr-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	10-Apr-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client unhappy about the legislation.

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-SOTU0	OCSP	16-Apr-14	Yes, further investigation is required.	16-Apr-14	N/A	16-Apr-14	Contact Centre Agent	16-Apr-14	Provide the client further explanation about the nature of the screening programs and options to withdraw (facilitate as required).	Contact Centre Agent	16-Apr-14	Provided the client explanation about the screening programs & option to withdraw. Client does not want to withdraw from correspondence.
1-SOV5C	OCSP	16-Apr-14	Yes, will be investigated.	16-Apr-14	N/A	16-Apr-14	Contact Centre Agent	21-Apr-14	No further action required/possible.	Contact Centre Agent	16-Apr-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-SYLVI	Screen for Life	22-Apr-14	Yes, further investigation is required.	22-Apr-14	N/A	22-Apr-14	Contact Centre Agent	7-Jul-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	22-Apr-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client unhappy about the legislation.
1-SYP42	OCSP	23-Apr-14	Yes, further investigation is required.	23-Apr-14	N/A	23-Apr-14	Contact Centre Agent	23-Apr-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	23-Apr-14	Provided the client explanation about the screening programs & option to withdraw. Client does not want to withdraw from correspondence.
1-T1XVH	Screen for Life	24-Apr-14	Yes, further investigation is required.	24-Apr-14	N/A	24-Apr-14	Contact Centre Agent	24-Apr-14	Provide the client further explanation about the nature of the screening programs and mailing logistics. Update client address/withdraw (facilitate as required).	Contact Centre Agent	24-Apr-14	Provided the client explanation about the screening programs & option to withdraw. Client does not want to withdraw from correspondence.

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-T22Q4	OCSP	24-Apr-14	Yes, further investigation is required.	24-Apr-14	N/A	24-Apr-14	Contact Centre Agent	24-Apr-14	Provide client information about CCO and its legislative authority and regulatory compliance requirements.	Contact Centre Agent	24-Apr-14	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is satisfied.
1-T3PH5	Screen for Life	28-Apr-14	Yes, further investigation is required.	28-Apr-14	N/A	28-Apr-14	Contact Centre Agent	28-Apr-14	Anonymous Client, attempt to contact if possible and address complaint.	Contact Centre Agent	28-Apr-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-T3PLL	OCSP	28-Apr-14	Yes, further investigation is required.	28-Apr-14	N/A	28-Apr-14	Contact Centre Agent	28-Apr-14	Provide the client further explanation about the nature of the screening programs and mailing logistics. Update client address/withdraw (facilitate as required).	Privacy and CC	28-Apr-14	CCO attempted to address complaint for the client, client did not cooperate (hung up/no response)
1-T3TU0	OCSP	28-Apr-14	Yes, further investigation is required.	28-Apr-14	N/A	28-Apr-14	Contact Centre Agent	28-Apr-14	Provide client instructions and requirements for withdrawal from screening correspondence program.	Contact Centre Agent	28-Apr-14	CCO attempted to address complaint for the client, client did not cooperate (hung up/no response)
1-T3UGS	OCSP	28-Apr-14	Yes, further investigation is required.	28-Apr-14	N/A	28-Apr-14	Contact Centre Agent	28-Apr-14	Provide client information about CCO and its legislative authority and regulatory compliance requirements.	Contact Centre Agent	28-Apr-14	Provided the client explanation about the screening programs & option to withdraw. Client does not want to withdraw from correspondence.

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-T3VII	Screen for Life	28-Apr-14	Yes, further investigation is required.	28-Apr-14	N/A	28-Apr-14	Contact Centre Agent	28-Apr-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	28-Apr-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-T3VPX	OCSP	28-Apr-14	Yes, further investigation is required.	28-Apr-14	N/A	28-Apr-14	Contact Centre Agent	29-Apr-14	Provide the client further explanation about the nature of the screening programs and mailing logistics. Update client address/withdraw (facilitate as required).	Contact Centre Agent	28-Apr-14	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is satisfied.
1-T7HKL	Screen for Life	30-Apr-14	Yes, further investigation is required.	30-Apr-14	N/A	30-Apr-14	Contact Centre Agent	9-May-14	Provide the client further explanation about the nature of the screening programs. Clarify client's misunderstanding/concerns about the letters.	Contact Centre Agent	30-Apr-14	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is satisfied.
1-TD4OS	Screen for Life	2-May-14	Yes, will be investigated.	2-May-14	N/A	2-May-14	Contact Centre Agent	2-May-14	No further action required/possible.	Contact Centre Agent	2-May-14	CCO attempted to address complaint for the client, client did not cooperate (hung up/no response)
1-TD5WZ	Screen for Life	2-May-14	Yes, further investigation is required.	2-May-14	N/A	2-May-14	Contact Centre Agent	9-May-14	Provide client information about CCO and its legislative authority and regulatory compliance requirements.	Legal	2-May-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
												with IPC. Client satisfied with response.
1-TD60D	SAR	2-May-14	Yes, further investigation is required.	2-May-14	N/A	2-May-14	Contact Centre Agent	2-May-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	2-May-14	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is satisfied.
1-TD8E3	Screen for Life	2-May-14	Yes, further investigation is required.	2-May-14	N/A	2-May-14	Contact Centre Agent	2-May-14	Provide the client further explanation about the nature of the screening programs and options to withdraw (facilitate as required).	Contact Centre Agent	2-May-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-TEHUH	Screen for Life	5-May-14	Yes, further investigation is required.	5-May-14	N/A	5-May-14	Contact Centre Agent	5-May-14	Provide the client further explanation about the nature of the screening programs and options to withdraw (facilitate as required).	Contact Centre Agent	5-May-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-TEHZI	Screen for Life	5-May-14	Yes, will be investigated.	5-May-14	N/A	5-May-14	Contact Centre Agent	6-May-14	Provide client instructions and requirements for withdrawal from screening correspondence program.	Contact Centre Agent	5-May-14	CCO attempted to address complaint for the client, client did not cooperate (hung up/no response)
1-TEIAN	Screen for Life	5-May-14	Yes, will be investigated.	5-May-14	N/A	5-May-14	Contact Centre Agent	13-May-14	No further action required/possible.	Contact Centre Agent	5-May-14	No further action required/possible.

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-TEJOT	OCSP	5-May-14	Yes, further investigation is required.	5-May-14	N/A	5-May-14	Contact Centre Agent	6-May-14	Provide the client further explanation about the nature of the screening programs and options to withdraw (facilitate as required).	Contact Centre Agent	6-May-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-TEK96	OCSP	5-May-14	Yes, further investigation is required.	5-May-14	N/A	5-May-14	Contact Centre Agent	5-May-14	Provide the client further explanation about the nature of the screening programs and mailing logistics. Update client address/withdraw (facilitate as required).	Contact Centre Agent	5-May-14	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is satisfied.
1-TEKUE	OBSP	5-May-14	Yes, will be investigated.	5-May-14	N/A	5-May-14	Contact Centre Agent	5-May-14	No further action required/possible.	Contact Centre Agent	5-May-14	CCO attempted to address complaint for the client, client did not cooperate (hung up/no response)
1-TFRYM	OCSP	6-May-14	Yes, further investigation is required.	6-May-14	N/A	6-May-14	Contact Centre Agent	6-May-14	Provide the client further explanation about the nature of the screening programs. Clarify client's misunderstanding/concerns about the letters.	Contact Centre Agent	6-May-14	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is satisfied.
1-TFTBX	OCSP	6-May-14	Yes, further investigation is required.	6-May-14	N/A	6-May-14	Contact Centre Agent	6-May-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	6-May-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-TJFGV	CCC	8-May-14	Yes, will be investigated.	8-May-14	N/A	8-May-14	Contact Centre Agent	8-May-14	No further action required/possible.	Contact Centre Agent	8-May-14	CCO attempted to address complaint for the client, client did not cooperate (hung up/no response)
1-TJTSB	CCC	9-May-14	Yes, further investigation is required.	9-May-14	N/A	9-May-14	Contact Centre Agent	16-May-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	16-May-14	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is satisfied.
1-TMR0G	OBSP	12-May-14	Yes, further investigation is required.	12-May-14	N/A	12-May-14	Contact Centre Agent	28-Jul-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	12-May-14	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is satisfied.
1-TMRN5	OCSP	13-May-14	Yes, will be investigated.	13-May-14	N/A	N/A	Contact Centre Agent	15-May-14	Anonymous Client, attempt to contact if possible and address complaint.	Contact Centre Agent	13-May-14	Anonymous client, could not be identified, no further action possible.
1-TN49A	Screen for Life	13-May-14	Yes, will be investigated.	13-May-14	N/A	N/A	Contact Centre Agent	13-May-14	Anonymous Client, attempt to contact if possible and address complaint.	Contact Centre Agent	13-May-14	Anonymous client, could not be identified, no further action possible.

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-TN4I1	Screen for Life	13-May-14	Yes, further investigation is required.	13-May-14	N/A	13-May-14	Contact Centre Agent	13-May-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	13-May-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-TN5F9	Screen for Life	13-May-14	Yes, further investigation is required.	13-May-14	N/A	13-May-14	Contact Centre Agent	13-May-14	No further action required/possible.	Contact Centre Agent	13-May-14	No further action required/possible.
1-TN76U	Screen for Life	14-May-14	Yes, further investigation is required.	14-May-14	N/A	14-May-14	Contact Centre Agent	14-May-14	No further action required/possible.	Contact Centre Agent	14-May-14	No further action required/possible.
1-TN8MJ	OCSP	14-May-14	Yes, will be investigated.	14-May-14	N/A	14-May-14	Contact Centre Agent	15-May-14	Anonymous Client, attempt to contact if possible and address complaint.	Contact Centre Agent	14-May-14	Anonymous client, could not be identified, no further action possible.
1-TP00R	Screen for Life	16-May-14	Yes, further investigation is required.	16-May-14	N/A	16-May-14	Contact Centre Agent	16-May-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	16-May-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-TS6I5	OCSP	20-May-14	Yes, further investigation is required.	20-May-14	N/A	20-May-14	Contact Centre Agent	20-May-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	20-May-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-TSBOC	Screen for Life	21-May-14	Yes, will be investigated.	21-May-14	N/A	21-May-14	Contact Centre Agent	21-May-14	No further action required/possible.	Contact Centre Agent	21-May-14	Anonymous client, could not be identified, no further action possible.

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-TTMXS	Screen for Life	22-May-14	Yes, further investigation is required.	22-May-14	N/A	22-May-14	Contact Centre Agent	22-May-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	22-May-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-TTPDX	Screen for Life	22-May-14	Yes, however the client was anonymous	22-May-14	N/A	22-May-14	Contact Centre Agent	22-May-14	Anonymous Client, attempt to contact if possible and address complaint.	Contact Centre Agent	22-May-14	Anonymous client was tracked, addressed complaint (withdrew client).
1-TYYUQ	OCSP	26-May-14	Yes, however the client was anonymous	26-May-14	N/A	26-May-14	Contact Centre Agent	26-May-14	Provide client instructions and requirements for withdrawal from screening correspondence program.	Contact Centre Agent	26-May-14	Anonymous client was tracked, addressed complaint (withdrew client).
1-TZDQC	OCSP	27-May-14	Yes, will be investigated.	27-May-14	N/A	27-May-14	Contact Centre Agent	27-May-14	No further action required/possible.	Contact Centre Agent	27-May-14	CCO attempted to address complaint for the client, client did not cooperate (hung up/no response)
1-TZFNB	OCSP	27-May-14	Yes, further investigation is required.	27-May-14	N/A	27-May-14	Contact Centre Agent	27-May-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	27-May-14	CCO attempted to address complaint for the client, client did not cooperate (hung up/no response)

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-TZGO3	OCSP	27-May-14	Yes, further investigation is required.	27-May-14	N/A	27-May-14	Contact Centre Agent	27-May-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	27-May-14	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is not satisfied with the legislation; informed management, provided IPC contact information.
1-TZLVE	Screen for Life	28-May-14	Yes, further investigation is required.	28-May-14	N/A	28-May-14	Contact Centre Agent	28-May-14	Provide the client further explanation about the nature of the screening programs and mailing logistics. Update client address/withdraw (facilitate as required).	Contact Centre Agent	28-May-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-U0PHC	Screen for Life	29-May-14	Yes, further investigation is required.	29-May-14	N/A	29-May-14	Contact Centre Agent	29-May-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	29-May-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-U0Q46	OCSP	29-May-14	Yes, further investigation is required.	29-May-14	N/A	29-May-14	Contact Centre Agent	29-May-14	Provide client information about CCO and its legislative authority and regulatory compliance requirements.	Contact Centre Agent	29-May-14	CCO attempted to address complaint for the client, client did not cooperate (hung up/no response)

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-U0Q1E	OCSP	29-May-14	Yes, further investigation is required.	29-May-14	N/A	29-May-14	Contact Centre Agent	29-May-14	Provide client information about CCO and its legislative authority and regulatory compliance requirements.	Contact Centre Agent	29-May-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client unhappy about the legislation.
1-U74OO	OCSP	4-Jun-14	Yes, further investigation is required.	4-Jun-14	N/A	4-Jun-14	Contact Centre Agent	4-Jun-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	4-Jun-14	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is satisfied.
1-UBVHB	OCSP	6-Jun-14	Yes, further investigation is required.	6-Jun-14	N/A	6-Jun-14	Contact Centre Agent	6-Jun-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	6-Jun-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-UBVVU	OCSP	6-Jun-14	Yes, further investigation is required.	6-Jun-14	N/A	6-Jun-14	Contact Centre Agent	6-Jun-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	6-Jun-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-UBW13	OCSP	6-Jun-14	Yes, further investigation is required.	6-Jun-14	N/A	6-Jun-14	Contact Centre Agent	12-Jun-14	Provide the client further explanation about the nature of the screening programs and mailing logistics. Update client address/withdraw (facilitate as required).	Contact Centre Agent	6-Jun-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-UFYLK	OCSP	9-Jun-14	Yes, further investigation is required.	9-Jun-14	N/A	9-Jun-14	Contact Centre Agent	10-Jun-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	9-Jun-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-UG29R	OCSP	9-Jun-14	Yes, further investigation is required.	9-Jun-14	N/A	9-Jun-14	Contact Centre Agent	9-Jun-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	9-Jun-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-UGHY2	OCSP	10-Jun-14	Yes, further investigation is required.	10-Jun-14	N/A	10-Jun-14	Contact Centre Agent	25-Jul-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	10-Jun-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-UGN8D	OCSP	11-Jun-14	Yes, further investigation is required.	11-Jun-14	N/A	11-Jun-14	Contact Centre Agent	13-Jun-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	11-Jun-14	CCO attempted to address complaint for the client, client did not cooperate (hung up/no response)

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-UHE9L	OCSP	12-Jun-14	Yes, further investigation is required.	12-Jun-14	N/A	12-Jun-14	Contact Centre Agent	12-Jun-14	Provide client information about CCO and its legislative authority and regulatory compliance requirements.	Contact Centre Agent	12-Jun-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-UIPP8	OCSP	13-Jun-14	Yes, further investigation is required.	13-Jun-14	N/A	13-Jun-14	Contact Centre Agent	13-Jun-14	No further action required/possible.	Contact Centre Agent	13-Jun-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-UIR43	OCSP	13-Jun-14	Yes, further investigation is required.	13-Jun-14	N/A	13-Jun-14	Contact Centre Agent	13-Jun-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	13-Jun-14	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is satisfied.
1-UISQ6	OCSP	13-Jun-14	Yes, further investigation is required.	13-Jun-14	N/A	13-Jun-14	Contact Centre Agent	16-Jun-14	Provide client information about CCO and its legislative authority and regulatory compliance requirements.	Contact Centre Agent	13-Jun-14	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is not satisfied with the legislation; informed management, provided IPC contact information.

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-UN125	Screen for Life	16-Jun-14	Yes, further investigation is required.	16-Jun-14	N/A	16-Jun-14	Contact Centre Agent	16-Jun-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	16-Jun-14	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is satisfied.
1-UN5LC	OCSP	17-Jun-14	Yes, further investigation is required.	17-Jun-14	N/A	17-Jun-14	Contact Centre Agent	17-Jun-14	Provide client instructions and requirements for withdrawal from screening correspondence program.	Contact Centre Agent	17-Jun-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-UNHGS	OCSP	17-Jun-14	Yes, further investigation is required.	17-Jun-14	N/A	17-Jun-14	Contact Centre Agent	17-Jun-14	Provide the client further explanation about the nature of the screening programs. Clarify client's misunderstanding/concerns about the letters.	Contact Centre Agent	17-Jun-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-UNHI9	OCSP	17-Jun-14	Yes, further investigation is required.	17-Jun-14	N/A	17-Jun-14	Contact Centre Agent	17-Jun-14	Provide client information about CCO and its legislative authority and regulatory compliance requirements.	Contact Centre Agent	17-Jun-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-UNKXP	OCSP	17-Jun-14	Yes, further investigation is required.	17-Jun-14	N/A	17-Jun-14	Contact Centre Agent	17-Jun-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	17-Jun-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-UNNUA	CCC	18-Jun-14	Yes, further investigation is required.	18-Jun-14	N/A	18-Jun-14	Contact Centre Agent	18-Jun-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	18-Jun-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-UNOAL	OCSP	18-Jun-14	Yes, will be investigated.	18-Jun-14	N/A	18-Jun-14	Contact Centre Agent	18-Jun-14	No further action required/possible.	Contact Centre Agent	18-Jun-14	CCO attempted to address complaint for the client, client did not cooperate (hung up/no response)
1-UNQ7V	OCSP	18-Jun-14	Yes, further investigation is required.	18-Jun-14	N/A	18-Jun-14	Contact Centre Agent	18-Jun-14	Provide the client further explanation about the nature of the screening programs and options to withdraw (facilitate as required).	Contact Centre Agent	18-Jun-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-UP429	OCSP	19-Jun-14	Yes, further investigation is required.	19-Jun-14	N/A	19-Jun-14	Contact Centre Agent	19-Jun-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	19-Jun-14	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is satisfied.
1-UP43X	OCSP	19-Jun-14	Yes, further investigation is required.	19-Jun-14	N/A	19-Jun-14	Contact Centre Agent	19-Jun-14	Provide the client further explanation about the nature of the screening programs and options to withdraw (facilitate as required).	Contact Centre Agent	19-Jun-14	CCO attempted to address complaint for the client, client did not cooperate (hung up/no response)
1-UP4TS	OCSP	19-Jun-14	Yes, will be investigated.	19-Jun-14	N/A	19-Jun-14	Contact Centre Agent	19-Jun-14	Anonymous Client, attempt to contact if possible and address complaint.	Contact Centre Agent	19-Jun-14	Anonymous client, could not be identified, no further action possible.

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-UP4UA	OBSP	19-Jun-14	Yes, further investigation is required.	19-Jun-14	N/A	19-Jun-14	Contact Centre Agent	19-Jun-14	Provide the client further explanation about the nature of the screening programs and options to withdraw (facilitate as required).	Contact Centre Agent	19-Jun-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-UP6Z1	OCSP	19-Jun-14	Yes, further investigation is required.	19-Jun-14	N/A	19-Jun-14	Contact Centre Agent	19-Jun-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	19-Jun-14	CCO attempted to address complaint for the client, client did not cooperate (hung up/no response)
1-UP71N	Screen for Life	19-Jun-14	Yes, further investigation is required.	19-Jun-14	N/A	19-Jun-14	Contact Centre Agent	24-Jun-14	Provide the client further explanation about the nature of the screening programs and options to withdraw (facilitate as required).	Contact Centre Agent	20-Jun-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-USH2Z	Screen for Life	23-Jun-14	Yes, further investigation is required.	23-Jun-14	N/A	23-Jun-14	Contact Centre Agent	23-Jun-14	Provide the client further explanation about the nature of the screening programs and options to withdraw (facilitate as required).	Contact Centre Agent	23-Jun-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-USH47	OCSP	23-Jun-14	Yes, will be investigated.	23-Jun-14	n/a	23-Jun-14	Privacy and CC	24-Jun-14	Provide the client further explanation about the nature of the screening programs. Clarify client's misunderstanding/concerns about the letters.	Privacy and CC	23-Jun-14	Provided the client explanation about the screening programs & option to withdraw. Client does not want to withdraw from correspondence.

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-UT2R7	OCSP	24-Jun-14	Yes, further investigation is required.	24-Jun-14	N/A	24-Jun-14	Contact Centre Agent	24-Jun-14	Provide the client further explanation about the nature of the screening programs and options to withdraw (facilitate as required).	Contact Centre Agent	24-Jun-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-UT5TC	CCC	24-Jun-14	Yes, further investigation is required.	24-Jun-14	N/A	24-Jun-14	Contact Centre Agent	24-Jun-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	24-Jun-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client unhappy about the legislation.
1-UT8OH	OCSP	24-Jun-14	Yes, further investigation is required.	24-Jun-14	N/A	24-Jun-14	Contact Centre Agent	24-Jun-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	24-Jun-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-UVU8Q	OCSP	26-Jun-14	Yes, further investigation is required.	26-Jun-14	N/A	26-Jun-14	Contact Centre Agent	26-Jun-14	Provide client instructions and requirements for withdrawal from screening correspondence program.	Contact Centre Agent	26-Jun-14	CCO attempted to address complaint for the client, client did not cooperate (hung up/no response)
1-UXO8D	OCSP	30-Jun-14	Yes, further investigation is required.	30-Jun-14	N/A	30-Jun-14	Contact Centre Agent	2-Jul-14	Provide client instructions and requirements for withdrawal from screening correspondence program.	Contact Centre Agent	30-Jun-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-UYHVQ	OCSP	3-Jul-14	Yes, however the client was anonymous	3-Jul-14	N/A	3-Jul-14	Contact Centre Agent	4-Jul-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	3-Jul-14	CCO attempted to address complaint for the client, client did not cooperate (hung up/no response)
1-V1CJD	OBSP	3-Jul-14	Yes, will be investigated.	3-Jul-14	N/A	3-Jul-14	Contact Centre Agent	3-Jul-14	No further action required/possible.	Contact Centre Agent	3-Jul-14	Anonymous client, could not be identified, no further action possible.
1-V1DYJ	OCSP	3-Jul-14	Yes, further investigation is required.	3-Jul-14	N/A	3-Jul-14	Contact Centre Agent	3-Jul-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	3-Jul-14	CCO attempted to address complaint for the client, client did not cooperate (hung up/no response)
1-V1EWR	Screen for Life	3-Jul-14	Yes, further investigation is required.	3-Jul-14	N/A	3-Jul-14	Contact Centre Agent	3-Jul-14	Provide client instructions and requirements for withdrawal from screening correspondence program.	Contact Centre Agent	3-Jul-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-V1G6J	OCSP	3-Jul-14	Yes, further investigation is required.	3-Jul-14	N/A	3-Jul-14	Contact Centre Agent	3-Jul-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	3-Jul-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-V3O2S	OCSP	4-Jul-14	Yes, further investigation is required.	4-Jul-14	N/A	4-Jul-14	Contact Centre Agent	4-Jul-14	Provide the client further explanation about the nature of the screening programs. Clarify client's misunderstanding/concerns about the letters.	Contact Centre Agent	4-Jul-14	Provided the client explanation about the screening programs & option to withdraw. Client does not want to withdraw from correspondence.
1-V43ET	OCSP	7-Jul-14	Yes, however the client was anonymous	7-Jul-14	N/A	7-Jul-14	Contact Centre Agent	7-Jul-14	No further action required/possible.	Contact Centre Agent	7-Jul-14	CCO attempted to address complaint for the client, client did not cooperate (hung up/no response)
1-V61B3	OCSP	7-Jul-14	Yes, further investigation is required.	7-Jul-14	N/A	7-Jul-14	Contact Centre Agent	7-Jul-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	7-Jul-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-V61PT	OCSP	7-Jul-14	Yes, however the client was anonymous	7-Jul-14	N/A	7-Jul-14	Contact Centre Agent	7-Jul-14	Provide client instructions and requirements for withdrawal from screening correspondence program.	Contact Centre Agent	7-Jul-14	CCO attempted to address complaint for the client, client did not cooperate (hung up/no response)
1-V6E6L	OCSP	8-Jul-14	Yes, further investigation is required.	8-Jul-14	N/A	8-Jul-14	Contact Centre Agent	8-Jul-14	Provide the client further explanation about the nature of the screening programs. Clarify client's misunderstanding/concerns about the letters.	Contact Centre Agent	8-Jul-14	Provided the client explanation about the screening programs & option to withdraw. Client does not want to withdraw from correspondence.
1-V6FK2	OCSP	8-Jul-14	Yes, further investigation is required.	8-Jul-14	N/A	8-Jul-14	Contact Centre Agent	8-Jul-14	Provide client instructions and requirements for withdrawal from screening correspondence program.	Contact Centre Agent	8-Jul-14	CCO attempted to address complaint for the client, client did not cooperate (hung up/no response)

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-V6GXZ	OCSP	8-Jul-14	Yes, further investigation is required.	8-Jul-14	N/A	8-Jul-14	Contact Centre Agent	8-Jul-14	Provide the client further explanation about the nature of the screening programs and mailing logistics. Update client address/withdraw (facilitate as required).	Contact Centre Agent	8-Jul-14	CCO attempted to address complaint for the client, client did not cooperate (hung up/no response)
1-V8J5P	OCSP	14-Jul-14	Yes, further investigation is required.	14-Jul-14	N/A	14-Jul-14	Contact Centre Agent	30-Jul-14	Provide client instructions and requirements for withdrawal from screening correspondence program.	Contact Centre Agent	14-Jul-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-V8YW6	OCSP	15-Jul-14	Yes, further investigation is required.	15-Jul-14	N/A	15-Jul-14	Contact Centre Agent	30-Jul-14	Provide client instructions and requirements for withdrawal from screening correspondence program.	Contact Centre Agent	15-Jul-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-V9CW3	OCSP	15-Jul-14	Yes, further investigation is required.	15-Jul-14	N/A	15-Jul-14	Contact Centre Agent	22-Jul-14	Provide client information about CCO and its legislative authority and regulatory compliance requirements.	Contact Centre Agent	15-Jul-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-V9DQI	OCSP	15-Jul-14	Yes, further investigation is required.	15-Jul-14	N/A	15-Jul-14	Contact Centre Agent	7-Aug-14	Provide client information about CCO and its legislative authority and regulatory compliance requirements.	Contact Centre Agent	15-Jul-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-V9DTC	OCSP	16-Jul-14	Yes, further investigation is required.	16-Jul-14	N/A	16-Jul-14	Contact Centre Agent	30-Jul-14	Provide client information about CCO and its legislative authority and regulatory compliance requirements.	Contact Centre Agent	16-Jul-14	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is not satisfied with the legislation; informed management, provided IPC contact information.
1-VA0UF	OBSP	16-Jul-14	Yes, further investigation is required.	16-Jul-14	N/A	16-Jul-14	Contact Centre Agent	16-Jul-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	16-Jul-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-VA0UV	OCSP	16-Jul-14	Yes, however the client was anonymous	16-Jul-14	N/A	16-Jul-14	Contact Centre Agent	16-Jul-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	16-Jul-14	Reviewed with client the efficacy of screening programs, the legislative requirements and regulatory compliance with IPC as requested by client.
1-VB2QT	OCSP	18-Jul-14	Yes, further investigation is required.	18-Jul-14	N/A	18-Jul-14	Contact Centre Agent	18-Jul-14	Provide the client further explanation about the nature of the screening programs. Clarify client's misunderstanding/concerns about the letters.	Contact Centre Agent	18-Jul-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-VCCUG	OCSP	21-Jul-14	Yes, further investigation is required.	21-Jul-14	N/A	21-Jul-14	Contact Centre Agent	21-Jul-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	21-Jul-14	CCO attempted to address complaint for the client, client did not cooperate (hung up/no response)
1-VCDFP	Screen for Life	22-Jul-14	Yes, however the client was anonymous	22-Jul-14	N/A	22-Jul-14	Contact Centre Agent	22-Jul-14	No further action required/possible.	Contact Centre Agent	22-Jul-14	No further action required/possible.
1-VCPE9	OCSP	22-Jul-14	Yes, further investigation is required.	22-Jul-14	N/A	22-Jul-14	Contact Centre Agent	24-Jul-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	22-Jul-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-VCR09	OCSP	22-Jul-14	Yes, further investigation is required.	22-Jul-14	N/A	22-Jul-14	Contact Centre Agent	22-Jul-14	Provide the client further explanation about the nature of the screening programs. Clarify client's misunderstanding/concerns about the letters.	Contact Centre Agent	22-Jul-14	Provided the client explanation about the screening programs & option to withdraw. Client does not want to withdraw from correspondence.
1-VDDNR	OCSP	24-Jul-14	Yes, further investigation is required.	24-Jul-14	N/A	24-Jul-14	Contact Centre Agent	24-Jul-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	22-Jul-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-VE6SI	Screen for Life	25-Jul-14	Yes, will be investigated.	25-Jul-14	N/A	N/A	Contact Centre Agent	25-Jul-14	No further action required/possible.	Contact Centre Agent	25-Jul-14	No further action required/possible.

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-VFB99	OCSP	28-Jul-14	Yes, further investigation is required.	28-Jul-14	N/A	28-Jul-14	Contact Centre Agent	28-Jul-14	Provide the client further explanation about the nature of the screening programs. Clarify client's misunderstanding/concerns about the letters.	Contact Centre Agent	28-Jul-14	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is satisfied.
1-VFM1E	OCSP	29-Jul-14	Yes, further investigation is required.	29-Jul-14	N/A	29-Jul-14	Contact Centre Agent	29-Jul-14	Provide the client further explanation about the nature of the screening programs. Clarify client's misunderstanding/concerns about the letters.	Contact Centre Agent	29-Jul-14	Provided the client explanation about the screening programs & option to withdraw. Client does not want to withdraw from correspondence.
1-VFYIR	OCSP	30-Jul-14	Yes, further investigation is required.	30-Jul-14	N/A	30-Jul-14	Contact Centre Agent	30-Jul-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	30-Jul-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-VGX88	OCSP	31-Jul-14	Yes, further investigation is required.	31-Jul-14	N/A	31-Jul-14	Contact Centre Agent	31-Jul-14	Provide client information about CCO and its legislative authority and regulatory compliance requirements.	Contact Centre Agent	31-Jul-14	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is not satisfied with the legislation; informed management, provided IPC contact information.

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-VGXOH	CCC	31-Jul-14	Yes, further investigation is required.	31-Jul-14	N/A	31-Jul-14	Contact Centre Agent	31-Jul-14	Provide the client further explanation about the nature of the screening programs and mailing logistics. Update client address/withdraw (facilitate as required).	Contact Centre Agent	31-Jul-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-VIT13	Screen for Life	6-Aug-14	Yes, however the client was anonymous	6-Aug-14	N/A	6-Aug-14	Contact Centre Agent	14-Aug-14	Anonymous Client, attempt to contact if possible and address complaint.	Contact Centre Agent	6-Aug-14	Anonymous client was tracked, addressed complaint (withdrew client).
1-VIT3Q	Screen for Life	6-Aug-14	Yes, however the client was anonymous	6-Aug-14	N/A	6-Aug-14	Contact Centre Agent	14-Aug-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	14-Aug-14	Anonymous client was tracked, addressed complaint (withdrew client).
1-VO0EY	OCSP	8-Aug-14	Yes, further investigation is required.	8-Aug-14	N/A	8-Aug-14	Contact Centre Agent	14-Aug-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	14-Aug-14	Provided the client explanation about the screening programs & option to withdraw. Client does not want to withdraw from correspondence.
1-VO84B	Screen for Life	11-Aug-14	Yes, further investigation is required.	11-Aug-14	N/A	11-Aug-14	Contact Centre Agent	11-Aug-14	Provide the client further explanation about the nature of the screening programs. Clarify client's misunderstanding/concerns about the letters.	Contact Centre Agent	11-Aug-14	Provided the client explanation about the screening programs & option to withdraw. Client does not want to withdraw from correspondence.
1-VO840	OCSP	11-Aug-14	Yes, further investigation is required.	11-Aug-14	N/A	11-Aug-14	Contact Centre Agent	11-Aug-14	Provide the client further explanation about the nature of the screening programs and mailing logistics. Update client address/withdraw (facilitate as required).	Contact Centre Agent	11-Aug-14	Provided the client explanation about the screening programs & option to withdraw. Client does not want to withdraw from correspondence.

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-VQ7LM	OCSP	13-Aug-14	Yes, further investigation is required.	13-Aug-14	N/A	13-Aug-14	Contact Centre Agent	13-Aug-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	13-Aug-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-XP95G	OCSP	18-Aug-14	Yes, further investigation is required.	18-Aug-14	N/A	18-Aug-14	Contact Centre Agent	20-Aug-14	Provide client instructions and requirements for withdrawal from screening correspondence program.	Contact Centre Agent	20-Aug-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-ZEJHS	OCSP	19-Aug-14	Yes, further investigation is required.	19-Aug-14	N/A	19-Aug-14	Contact Centre Agent	19-Aug-14	Provide client instructions and requirements for withdrawal from screening correspondence program.	Contact Centre Agent	19-Aug-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-ZEJQW	OCSP	19-Aug-14	Yes, further investigation is required.	19-Aug-14	N/A	19-Aug-14	Contact Centre Agent	19-Aug-14	Provide client instructions and requirements for withdrawal from screening correspondence program.	Contact Centre Agent	19-Aug-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-ZFJ1E	OCSP	19-Aug-14	Yes, further investigation is required.	19-Aug-14	N/A	19-Aug-14	Contact Centre Agent	19-Aug-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	19-Aug-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-ZFKD8	OCSP	20-Aug-14	Yes, further investigation is required.	20-Aug-14	N/A	20-Aug-14	Contact Centre Agent	20-Aug-14	Provide client instructions and requirements for withdrawal from screening correspondence program.	Contact Centre Agent	20-Aug-14	CCO attempted to address complaint for the client, client did not cooperate

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
												(hung up/no response)
1-ZFKMZ	OCSP	20-Aug-14	Yes, further investigation is required.	20-Aug-14	N/A	20-Aug-14	Contact Centre Agent	20-Aug-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	20-Aug-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-115BFV	OCSP	20-Aug-14	Yes, further investigation is required.	20-Aug-14	N/A	20-Aug-14	Contact Centre Agent	20-Aug-14	Provide the client further explanation about the nature of the screening programs. Clarify client's misunderstanding/concerns about the letters.	Contact Centre Agent	20-Aug-14	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is satisfied.
1-1251MX	Screen for Life	22-Aug-14	Yes, further investigation is required.	22-Aug-14	N/A	22-Aug-14	Contact Centre Agent	22-Aug-14	Provide the client further explanation about the nature of the screening programs. Clarify client's misunderstanding/concerns about the letters.	Contact Centre Agent	22-Aug-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-19WZYT	OCSP	25-Aug-14	Yes, further investigation is required.	25-Aug-14	N/A	25-Aug-14	Contact Centre Agent	30-Aug-14	Provide the client further explanation about the nature of the screening programs and mailing logistics. Update client address/withdraw (facilitate as required).	Contact Centre Agent	25-Aug-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-1C149Y	OCSP	27-Aug-14	Yes, further investigation is required.	27-Aug-14	N/A	27-Aug-14	Contact Centre Agent	27-Aug-14	Provide the client further explanation about the nature of the screening programs. Clarify client's misunderstanding/concerns about the letters.	Contact Centre Agent	27-Aug-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-1C14IN	OCSP	27-Aug-14	Yes, further investigation is required.	27-Aug-14	N/A	27-Aug-14	Contact Centre Agent	27-Aug-14	Provide the client further explanation about the nature of the screening programs and mailing logistics. Update client address/withdraw (facilitate as required).	Contact Centre Agent	27-Aug-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-1EIRNT	OBSP	28-Aug-14	Yes, further investigation is required.	28-Aug-14	N/A	28-Aug-14	Contact Centre Agent	28-Aug-14	Provide client information about CCO and its legislative authority and regulatory compliance requirements.	Contact Centre Agent	28-Aug-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-1EIS27	OCSP	29-Aug-14	Yes, further investigation is required.	29-Aug-14	N/A	29-Aug-14	Contact Centre Agent	29-Aug-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	29-Aug-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-1GPWNI	OCSP	29-Aug-14	Yes, further investigation is required.	29-Aug-14	N/A	29-Aug-14	Contact Centre Agent	29-Aug-14	Provide the client further explanation about the nature of the screening programs and mailing logistics. Update client address/withdraw (facilitate as required).	Contact Centre Agent	29-Aug-14	Reviewed with client the efficacy of screening programs, the legislative requirements and regulatory compliance with IPC as requested by client.

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-1OXQ0X	OCSP	2-Sep-14	Yes, further investigation is required.	2-Sep-14	N/A	2-Sep-14	Contact Centre Agent	8-Sep-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	2-Sep-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-1QUR56	OCSP	3-Sep-14	Yes, further investigation is required.	3-Sep-14	N/A	3-Sep-14	Contact Centre Agent	5-Sep-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	2-Sep-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-1QUR8R	OCSP	3-Sep-14	Yes, further investigation is required.	3-Sep-14	N/A	3-Sep-14	Contact Centre Agent	3-Sep-14	Provide the client further explanation about the nature of the screening programs and mailing logistics. Update client address/withdraw (facilitate as required).	Contact Centre Agent	3-Sep-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-1TQ40E	CCC	5-Sep-14	Yes, further investigation is required.	5-Sep-14	N/A	5-Sep-14	Contact Centre Agent	5-Sep-14	Provide client information about CCO and its legislative authority and regulatory compliance requirements.	Contact Centre Agent	5-Sep-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-1TQ427	OCSP	5-Sep-14	Yes, further investigation is required.	5-Sep-14	N/A	5-Sep-14	Contact Centre Agent	5-Sep-14	Provide client information about CCO and its legislative authority and regulatory compliance requirements.	Contact Centre Agent	5-Sep-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-20PTVH	OCSP	8-Sep-14	Yes, further investigation is required.	8-Sep-14	N/A	8-Sep-14	Contact Centre Agent	8-Sep-14	Provide the client further explanation about the nature of the screening programs. Clarify client's misunderstanding/concerns about the letters.	Contact Centre Agent	8-Sep-14	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is satisfied.
1-24YLKM	CCC	10-Sep-14	Yes, further investigation is required.	10-Sep-14	N/A	10-Sep-14	Contact Centre Agent	11-Sep-14	Provide client information about CCO and its legislative authority and regulatory compliance requirements.	Contact Centre Agent	10-Sep-14	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is not satisfied with the legislation; informed management, provided IPC contact information.
1-28Q0AO	OCSP	12-Sep-14	Yes, further investigation is required.	12-Sep-14	N/A	12-Sep-14	Contact Centre Agent	12-Sep-14	Provide the client further explanation about the nature of the screening programs and mailing logistics. Update client address/withdraw (facilitate as required).	Contact Centre Agent	12-Sep-14	Provided the client explanation about the screening programs & option to withdraw. Client does not want to withdraw from correspondence.
1-28Q0MS	OCSP	15-Sep-14	Yes, further investigation is required.	15-Sep-14	N/A	15-Sep-14	Contact Centre Agent	15-Sep-14	Provide client information about CCO and its legislative authority and regulatory compliance requirements.	Contact Centre Agent	15-Sep-14	CCO attempted to address complaint for the client, client did not cooperate (hung up/no response)
1-28Q0NP	Screen for Life	15-Sep-14	Yes, further investigation is required.	15-Sep-14	N/A	15-Sep-14	Contact Centre Agent	15-Sep-14	Anonymous Client, attempt to contact if possible and address complaint.	Contact Centre Agent	15-Sep-14	Anonymous client, could not be identified, no further

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
												action possible.
1-2EXQR0	OBSP	15-Sep-14	Yes, further investigation is required.	15-Sep-14	N/A	15-Sep-14	Contact Centre Agent	15-Sep-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	15-Sep-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-2EXRNA	OCSP	15-Sep-14	Yes, further investigation is required.	15-Sep-14	N/A	15-Sep-14	Contact Centre Agent	16-Sep-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	15-Sep-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-2GYAG8	OCSP	16-Sep-14	Yes, further investigation is required.	16-Sep-14	N/A	16-Sep-14	Contact Centre Agent	17-Sep-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	16-Sep-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-2GYBDP	OBSP	17-Sep-14	Yes, however the client was anonymous	17-Sep-14	N/A	17-Sep-14	Contact Centre Agent	17-Sep-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	17-Sep-14	CCO attempted to address complaint for the client, client did not cooperate (hung up/no response)

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-2IWCF4	Screen for Life	17-Sep-14	Yes, further investigation is required.	17-Sep-14	N/A	17-Sep-14	Contact Centre Agent	17-Sep-14	Provide client information about CCO and its legislative authority and regulatory compliance requirements.	Contact Centre Agent	17-Sep-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-2IWCFP	OCSP	17-Sep-14	Yes, further investigation is required.	17-Sep-14	N/A	17-Sep-14	Contact Centre Agent	17-Sep-14	Provide the client further explanation about the nature of the screening programs and mailing logistics. Update client address/withdraw (facilitate as required).	Contact Centre Agent	17-Sep-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-2IWCOC	OBSP	17-Sep-14	Yes, further investigation is required.	17-Sep-14	N/A	17-Sep-14	Contact Centre Agent	17-Sep-14	Provide the client further explanation about the nature of the screening programs. Clarify client's misunderstanding/concerns about the letters.	Contact Centre Agent	17-Sep-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-2TRENG	OCSP	23-Sep-14	Yes, further investigation is required.	23-Sep-14	N/A	23-Sep-14	Contact Centre Agent	25-Sep-14	Provide the client further explanation about the nature of the screening programs and mailing logistics. Update client address/withdraw (facilitate as required).	Contact Centre Agent	23-Sep-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-2VXTRS	CCC	25-Sep-14	Yes, further investigation is required.	25-Sep-14	N/A	25-Sep-14	Contact Centre Agent	25-Sep-14	No further action required/possible.	Contact Centre Agent	25-Sep-14	No further action required/possible.
1-33QZOP	Screen for Life	29-Sep-14	Yes, however the client was anonymous	29-Sep-14	N/A	29-Sep-14	Contact Centre Agent	30-Sep-14	Anonymous Client, attempt to contact if possible and address complaint.	Contact Centre Agent	29-Sep-14	Anonymous client, could not be identified, no further action possible.
1-35SWDT	Screen for Life	30-Sep-14	Yes, however the client was anonymous	30-Sep-14	N/A	30-Sep-14	Contact Centre Agent	30-Sep-14	Anonymous Client, attempt to contact if possible and address complaint.	Contact Centre Agent	30-Sep-14	Anonymous client, could not be identified, no further action possible.

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-35SWNM	OCSP	30-Sep-14	Yes, further investigation is required.	30-Sep-14	N/A	30-Sep-14	Contact Centre Agent	30-Sep-14	Provide the client further explanation about the nature of the screening programs. Clarify client's misunderstanding/concerns about the letters.	Contact Centre Agent	30-Sep-14	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is satisfied.
1-37RXWJ	OCSP	1-Oct-14	Yes, further investigation is required.	1-Oct-14	N/A	1-Oct-14	Contact Centre Agent	14-Oct-14	Provide the client further explanation about the nature of the screening programs and mailing logistics. Update client address/withdraw (facilitate as required).	Contact Centre Agent	1-Oct-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-37V0YQ	OCSP	1-Oct-14	Yes, further investigation is required.	1-Oct-14	N/A	1-Oct-14	Contact Centre Agent	1-Oct-14	Provide the client further explanation about the nature of the screening programs and mailing logistics. Update client address/withdraw (facilitate as required).	Contact Centre Agent	1-Oct-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-37V1OG	OCSP	2-Oct-14	Yes, however the client was anonymous	2-Oct-14	N/A	2-Oct-14	Contact Centre Agent	2-Oct-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	2-Oct-14	Reviewed with client the efficacy of screening programs, the legislative requirements and regulatory compliance with IPC as requested by client.
1-3LJF2X	OCSP	8-Oct-14	Yes, further investigation is required.	8-Oct-14	N/A	8-Oct-14	Contact Centre Agent	9-Oct-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	8-Oct-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-3LJXMS	OCSP	9-Oct-14	Yes, further investigation is required.	9-Oct-14	N/A	9-Oct-14	Contact Centre Agent	9-Oct-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	9-Oct-14	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is not satisfied with the legislation; informed management, provided IPC contact information.
1-3X3FZH	OCSP	14-Oct-14	Yes, further investigation is required.	14-Oct-14	N/A	14-Oct-14	Contact Centre Agent	14-Oct-14	Provide client information about CCO and its legislative authority and regulatory compliance requirements.	Contact Centre Agent	14-Oct-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-3X3HUK	OCSP	15-Oct-14	Yes, further investigation is required.	15-Oct-14	N/A	15-Oct-14	Contact Centre Agent	15-Oct-14	Provide the client further explanation about the nature of the screening programs. Clarify client's misunderstanding/concerns about the letters.	Contact Centre Agent	15-Oct-14	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is satisfied.

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-3YUC5S	OBSP	15-Oct-14	Yes, further investigation is required.	15-Oct-14	N/A	15-Oct-14	Contact Centre Agent	17-Oct-14	Provide client information about CCO and its legislative authority and regulatory compliance requirements.	Contact Centre Agent	15-Oct-14	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is not satisfied with the legislation; informed management, provided IPC contact information.
1-47AY28	OCSP	21-Oct-14	Yes, further investigation is required.	21-Oct-14	N/A	21-Oct-14	Contact Centre Agent	21-Oct-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	21-Oct-14	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is satisfied.
1-4K4UDS	OCSP	27-Oct-14	Yes, further investigation is required.	27-Oct-14	N/A	27-Oct-14	Contact Centre Agent	27-Oct-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	27-Oct-14	CCO attempted to address complaint for the client, client did not cooperate (hung up/no response)

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-4K4UDW	OCSP	27-Oct-14	Yes, further investigation is required.	27-Oct-14	N/A	27-Oct-14	Contact Centre Agent	18-Nov-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	27-Oct-14	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is not satisfied with the legislation; informed management, provided IPC contact information.
1-4OY2IE	OCSP	30-Oct-14	Yes, further investigation is required.	30-Oct-14	N/A	30-Oct-14	Contact Centre Agent	30-Oct-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	30-Oct-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-56XC7P	OCSP	3-Nov-14	Yes, further investigation is required.	3-Nov-14	N/A	3-Nov-14	Contact Centre Agent	3-Nov-14	Provide the client further explanation about the nature of the screening programs. Clarify client's misunderstanding/concerns about the letters.	Contact Centre Agent	3-Nov-14	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is not satisfied with the legislation; informed management, provided IPC contact information.

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-5AL2J2	OCSP	4-Nov-14	Yes, further investigation is required.	4-Nov-14	N/A	4-Nov-14	Contact Centre Agent	4-Nov-14	Provide client information about CCO and its legislative authority and regulatory compliance requirements.	Contact Centre Agent	4-Nov-14	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is not satisfied with the legislation; informed management, provided IPC contact information.
1-5AL4EZ	OCSP	4-Nov-14	Yes, further investigation is required.	4-Nov-14	N/A	4-Nov-14	Contact Centre Agent	4-Nov-14	Provide client information about CCO and its legislative authority and regulatory compliance requirements.	Contact Centre Agent	4-Nov-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-5E7SPD	Screen for Life	5-Nov-14	Yes, further investigation is required.	5-Nov-14	N/A	5-Nov-14	Contact Centre Agent	6-Nov-14	Provide client information about CCO and its legislative authority and regulatory compliance requirements.	Contact Centre Agent	5-Nov-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-5E7SQX	OCSP	5-Nov-14	Yes, further investigation is required.	5-Nov-14	N/A	5-Nov-14	Contact Centre Agent	5-Nov-14	Provide the client further explanation about the nature of the screening programs. Clarify client's misunderstanding/concerns about the letters.	Contact Centre Agent	5-Nov-14	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is satisfied.

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-5GRVMH	OCSP	6-Nov-14	Yes, further investigation is required.	6-Nov-14	N/A	6-Nov-14	Contact Centre Agent	6-Nov-14	Provide client information about CCO and its legislative authority and regulatory compliance requirements.	Contact Centre Agent	6-Nov-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-5LCDZH	OCSP	10-Nov-14	Yes, further investigation is required.	10-Nov-14	N/A	10-Nov-14	Contact Centre Agent	10-Nov-14	Provide client information about CCO and its legislative authority and regulatory compliance requirements.	Contact Centre Agent	10-Nov-14	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is not satisfied with the legislation; informed management, provided IPC contact information.
1-5LC9RR	OCSP	10-Nov-14	Yes, further investigation is required.	10-Nov-14	N/A	10-Nov-14	Contact Centre Agent	10-Nov-14	Provide the client further explanation about the nature of the screening programs. Clarify client's misunderstanding/concerns about the letters.	Contact Centre Agent	10-Nov-14	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is satisfied.
1-5ZIANA	CCC	11-Nov-14	Yes, further investigation is required.	11-Nov-14	N/A	11-Nov-14	Contact Centre Agent	11-Nov-14	Anonymous Client, attempt to contact if possible and address complaint.	Contact Centre Agent	11-Nov-14	No further action required/possible.

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-7248B3	OCSP	18-Nov-14	Yes, further investigation is required.	18-Nov-14	N/A	18-Nov-14	Contact Centre Agent	24-Nov-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	18-Nov-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-7DFOLM	OCSP	19-Nov-14	Yes, further investigation is required.	19-Nov-14	N/A	19-Nov-14	Contact Centre Agent	21-Nov-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	19-Nov-14	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is not satisfied with the legislation; informed management, provided IPC contact information.
1-7ILL0B	Screen for Life	20-Nov-14	Yes, further investigation is required.	20-Nov-14	N/A	20-Nov-14	Contact Centre Agent	20-Nov-14	Provide client instructions and requirements for withdrawal from screening correspondence program.	Contact Centre Agent	20-Nov-14	CCO attempted to address complaint for the client, client did not cooperate (hung up/no response)
1-7ILNOZ	Screen for Life	21-Nov-14	Yes, further investigation is required.	21-Nov-14	N/A	21-Nov-14	Contact Centre Agent	21-Nov-14	Provide client instructions and requirements for withdrawal from screening correspondence program.	Contact Centre Agent	21-Nov-14	CCO attempted to address complaint for the client, client did not cooperate (hung up/no response)

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-7QXX3A	OCSP	25-Nov-14	Yes, further investigation is required.	25-Nov-14	N/A	25-Nov-14	Contact Centre Agent	26-Nov-14	Provide the client further explanation about the nature of the screening programs. Clarify client's misunderstanding/concerns about the letters.	Contact Centre Agent	25-Nov-14	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is satisfied.
1-7YZB9B	OCSP	25-Nov-14	Yes, further investigation is required.	25-Nov-14	N/A	25-Nov-14	Contact Centre Agent	29-Dec-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	25-Nov-14	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is not satisfied with the legislation; informed management, provided IPC contact information.
1-7YZEBF	OCSP	26-Nov-14	Yes, further investigation is required.	26-Nov-14	N/A	26-Nov-14	Contact Centre Agent	18-Dec-14	Provide client instructions and requirements for withdrawal from screening correspondence program.	Contact Centre Agent	26-Nov-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-86Z6Z2	OCSP	26-Nov-14	Yes, further investigation is required.	26-Nov-14	N/A	26-Nov-14	Contact Centre Agent	26-Nov-14	Provide client instructions and requirements for withdrawal from screening correspondence program.	Contact Centre Agent	26-Nov-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-8JO2V7	Screen for Life	28-Nov-14	Yes, further investigation is required.	28-Nov-14	N/A	28-Nov-14	Contact Centre Agent	28-Nov-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	28-Nov-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-8JO323	OCSP	28-Nov-14	Yes, further investigation is required.	28-Nov-14	N/A	28-Nov-14	Contact Centre Agent	28-Nov-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	28-Nov-14	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is not satisfied with the legislation; informed management, provided IPC contact information.
1-98NY0P	Screen for Life	2-Dec-14	Yes, further investigation is required.	2-Dec-14	N/A	2-Dec-14	Contact Centre Agent	2-Dec-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	2-Dec-14	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is not satisfied with the legislation; informed management, provided IPC contact information.

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-98NY5R	OCSP	2-Dec-14	Yes, further investigation is required.	2-Dec-14	N/A	2-Dec-14	Contact Centre Agent	2-Dec-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	2-Dec-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-9NVCY6	Screen for Life	3-Dec-14	Yes, further investigation is required.	5-Dec-14	N/A	5-Dec-14	Privacy and CC	5-Dec-14	Anonymous Client, attempt to contact if possible and address complaint.	Privacy and CC	5-Dec-14	No further action required/possible.
1-9NYPX8	OCSP	4-Dec-14	Yes, further investigation is required.	4-Dec-14	N/A	4-Dec-14	Contact Centre Agent	4-Dec-14	Provide client information about CCO and its legislative authority and regulatory compliance requirements.	Contact Centre Agent	4-Dec-14	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is not satisfied with the legislation; informed management, provided IPC contact information.
1-9NYQD3	OCSP	4-Dec-14	Yes, further investigation is required.	4-Dec-14	N/A	4-Dec-14	Contact Centre Agent	4-Dec-14	Provide client information about CCO and its legislative authority and regulatory compliance requirements.	Contact Centre Agent	4-Dec-14	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is not satisfied with the legislation; informed management, provided IPC contact information.

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-9RR9PD	OCSP	4-Dec-14	Yes, further investigation is required.	4-Dec-14	N/A	4-Dec-14	Contact Centre Agent	4-Dec-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	4-Dec-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-AXPW4O	OCSP	9-Dec-14	Yes, further investigation is required.	9-Dec-14	N/A	9-Dec-14	Contact Centre Agent	4-Dec-14	Provide client information about CCO and its legislative authority and regulatory compliance requirements.	Contact Centre Agent	4-Dec-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-AXPXAF	OCSP	10-Dec-14	Yes, further investigation is required.	10-Dec-14	N/A	10-Dec-14	Contact Centre Agent	11-Dec-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	10-Dec-14	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-B5LCJC	OCSP	10-Dec-14	Yes, however the client was anonymous	10-Dec-14	N/A	10-Dec-14	Contact Centre Agent	12-Dec-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	10-Dec-14	Provided the client explanation about the screening programs & option to withdraw. Client does not want to withdraw from correspondence.
1-B5MC97	Screen for Life	11-Dec-14	Yes, further investigation is required.	11-Dec-14	N/A	11-Dec-14	Contact Centre Agent	12-Dec-14	Anonymous Client, attempt to contact if possible and address complaint.	Contact Centre Agent	12-Dec-14	No further action required/possible.
1-B7YJZA	OCSP	11-Dec-14	Yes, further investigation is required.	11-Dec-15	N/A	11-Dec-14	Contact Centre Agent	11-Dec-14	No further action required/possible.	Contact Centre Agent	11-Dec-14	No further action required/possible.
1-CNWPPT	Screen for Life	19-Dec-14	Yes, further investigation is required.	19-Dec-15	N/A	19-Dec-14	Contact Centre Agent	19-Dec-14	Anonymous Client, attempt to contact if possible and address complaint.	Contact Centre Agent	19-Dec-14	Anonymous client, could not be identified, no further

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
												action possible.
1-D33SOX	OCSP	23-Dec-14	Yes, further investigation is required.	23-Dec-15	N/A	23-Dec-14	Contact Centre Agent	23-Dec-14	Provide the client further explanation about the nature of the screening programs. Clarify client's misunderstanding/concerns about the letters.	Contact Centre Agent	23-Dec-14	Provided the client explanation about the screening programs & option to withdraw. Client does not want to withdraw from correspondence.
1-DV32U7	OCSP	31-Dec-14	Yes, further investigation is required.	31-Dec-15	N/A	31-Dec-14	Contact Centre Agent	31-Dec-14	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	31-Dec-14	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is satisfied.
1-EDPS3A	OCSP	5-Jan-15	Yes, however the client was anonymous	5-Jan-15	N/A	5-Jan-14	Contact Centre Agent	21-Jan-14	Anonymous Client, attempt to contact if possible and address complaint.	Contact Centre Agent	5-Jan-14	Anonymous client, could not be identified, no further action possible.
1-EDQORI	Screen for Life	6-Jan-15	Yes, however the client was anonymous	6-Jan-15	N/A	6-Jan-15	Contact Centre Agent	6-Jan-15	Anonymous Client, attempt to contact if possible and address complaint.	Contact Centre Agent	6-Jan-15	Anonymous client, could not be identified, no further action possible.
1-F6QRDU	OCSP	15-Jan-15	Yes, further investigation is required.	15-Jan-15	N/A	15-Jan-15	Contact Centre Agent	15-Jan-15	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	15-Jan-15	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-FN5NAW	OBSP	21-Jan-15	Yes, further investigation is required.	21-Jan-15	N/A	21-Jan-15	Contact Centre Agent	21-Jan-15	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	21-Jan-15	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is not satisfied with the legislation; informed management, provided IPC contact information.
1-FQ9OR5	OCSP	21-Jan-15	Yes, further investigation is required.	21-Jan-15	N/A	21-Jan-15	Contact Centre Agent	21-Jan-15	Provide client information about CCO and its legislative authority and regulatory compliance requirements.	Contact Centre Agent	21-Jan-15	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-FRUXPV	OCSP	22-Jan-15	Yes, further investigation is required.	22-Jan-15	N/A	22-Jan-15	Contact Centre Agent	22-Jan-15	No further action required/possible.	Contact Centre Agent	22-Jan-15	No further action required/possible.
1-G6UEC2	OCSP	26-Jan-15	Yes, further investigation is required.	26-Jan-15	N/A	26-Jan-15	Contact Centre Agent	26-Jan-15	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	26-Jan-15	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-GLZLNC	OCSP	30-Jan-15	Yes, further investigation is required.	30-Jan-15	N/A	30-Jan-15	Contact Centre Agent	30-Jan-15	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	30-Jan-15	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
												with IPC. Client is satisfied.
1-GLZM0F	OCSP	30-Jan-15	Yes, further investigation is required.	30-Jan-15	N/A	30-Jan-15	Contact Centre Agent	3-Feb-15	Provide client instructions and requirements for withdrawal from screening correspondence program.	Contact Centre Agent	30-Jan-15	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-H2U4KK	OCSP	4-Feb-15	Yes, further investigation is required.	4-Feb-15	N/A	4-Feb-15	Contact Centre Agent	4-Feb-15	Provide client information about CCO and its legislative authority and regulatory compliance requirements.	Contact Centre Agent	4-Feb-15	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is not satisfied with the legislation; informed management, provided IPC contact information.
1-HNI6OF	OCSP	9-Feb-15	Yes, further investigation is required.	9-Feb-15	N/A	9-Feb-15	Contact Centre Agent	9-Feb-15	Provide client information about CCO and its legislative authority and regulatory compliance requirements.	Contact Centre Agent	9-Feb-15	CCO attempted to address complaint for the client, client did not cooperate (hung up/no response)

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-HNI72J	OCSP	9-Feb-15	Yes, however the client was anonymous	9-Feb-15	N/A	9-Feb-15	Contact Centre Agent	9-Feb-15	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	9-Feb-15	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is satisfied.
1-HQKCSV	OCSP	10-Feb-15	Yes, further investigation is required.	10-Feb-15	N/A	10-Feb-15	Contact Centre Agent	10-Feb-15	Provide the client further explanation about the nature of the screening programs and mailing logistics. Update client address/withdraw (facilitate as required).	Contact Centre Agent	10-Feb-15	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-HVCF8N	CCC	13-Feb-15	Yes, further investigation is required.	13-Feb-15	N/A	13-Feb-15	Contact Centre Agent	17-Feb-15	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	13-Feb-15	Provided the client explanation about the screening programs & option to withdraw. Client does not want to withdraw from correspondence.
1-J4RCDF	Screen for Life	27-Feb-15	Yes, however the client was anonymous	27-Feb-15	N/A	27-Feb-15	Contact Centre Agent	2-Mar-15	Anonymous Client, attempt to contact if possible and address complaint.	Contact Centre Agent	27-Feb-15	Anonymous client, could not be identified, no further action possible.
1-JM23AM	OCSP	3-Mar-15	Yes, further investigation is required.	3-Mar-15	N/A	3-Mar-15	Contact Centre Agent	3-Mar-15	Provide client instructions and requirements for withdrawal from screening correspondence program.	Contact Centre Agent	3-Mar-15	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-JQHAGN	OCSP	5-Mar-15	Yes, further investigation is required.	5-Mar-15	N/A	5-Mar-15	Privacy and CC	6-Mar-15	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Privacy and CC	5-Mar-15	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-JXRYWN	OBSP	6-Mar-15	Yes, further investigation is required.	6-Mar-15	N/A	6-Mar-15	Contact Centre Agent	6-Mar-15	Provide the client further explanation about the nature of the screening programs. Clarify client's misunderstanding/concerns about the letters.	Contact Centre Agent	6-Mar-15	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is satisfied.
1-KRNYIN	Screen for Life	12-Mar-15	Yes, however the client was anonymous	12-Mar-15	N/A	12-Mar-15	Contact Centre Agent	12-Mar-15	Provide client instructions and requirements for withdrawal from screening correspondence program.	Contact Centre Agent	12-Mar-15	No further action required/possible.
1-KWI5U1	CCC	13-Mar-15	Yes, further investigation is required.	13-Mar-15	N/A	13-Mar-15	Contact Centre Agent	13-Mar-15	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	13-Mar-15	Provided the client explanation about the screening programs & option to withdraw. Client does not want to withdraw from correspondence.
1-LQGSJO	OCSP	18-Mar-15	Yes, further investigation is required.	18-Mar-15	N/A	18-Mar-15	Contact Centre Agent	18-Mar-15	Provide client instructions and requirements for withdrawal from screening correspondence program.	Contact Centre Agent	18-Mar-15	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-N04AAK	OBSP	27-Mar-15	Yes, further investigation is required.	27-Mar-15	N/A	27-Mar-15	Contact Centre Agent	27-Mar-15	Provide the client further explanation about the nature of the screening programs. Clarify client's misunderstanding/concerns about the letters.	Contact Centre Agent	27-Mar-15	Provided the client explanation about the screening programs & option to withdraw. Client does not want to withdraw from correspondence.
1-N04AHO	Screen for Life	27-Mar-15	Yes, further investigation is required.	27-Mar-15	N/A	27-Mar-15	Contact Centre Agent	27-Mar-15	Provide client instructions and requirements for withdrawal from screening correspondence program.	Contact Centre Agent	27-Mar-15	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-N77XFG	Screen for Life	27-Mar-15	Yes, further investigation is required.	27-Mar-15	N/A	27-Mar-15	Contact Centre Agent	27-Mar-15	Provide client information about CCO and its legislative authority and regulatory compliance requirements.	Contact Centre Agent	27-Mar-15	CCO attempted to address complaint for the client, client did not cooperate (hung up/no response)
1-NS2WUO	Screen for Life	30-Mar-15	Yes, further investigation is required.	30-Mar-15	N/A	30-Mar-15	Contact Centre Agent	1-Apr-15	Provide client instructions and requirements for withdrawal from screening correspondence program.	Contact Centre Agent	30-Mar-15	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-NZGJEB	OBSP	31-Mar-15	Yes, further investigation is required.	31-Mar-15	N/A	31-Mar-15	Contact Centre Agent	31-Mar-15	Provide client information about CCO and its legislative authority and regulatory compliance requirements.	Contact Centre Agent	31-Mar-15	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is not satisfied with the legislation; informed management, provided IPC contact

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
												information.
1-NZGMJT	OCSP	1-Apr-15	Yes, further investigation is required.	1-Apr-15	N/A	1-Apr-15	Contact Centre Agent	1-Apr-15	Provide the client further explanation about the nature of the screening programs and mailing logistics. Update client address/withdraw (facilitate as required).	Contact Centre Agent	1-Apr-15	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-O8TLLQ	OCSP	1-Apr-15	Yes, further investigation is required.	1-Apr-15	N/A	1-Apr-15	Contact Centre Agent	1-Apr-15	Provide the client further explanation about the nature of the screening programs. Clarify client's misunderstanding/concerns about the letters.	Contact Centre Agent	1-Apr-15	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is satisfied.
1-O8ULB9	OCSP	6-Apr-15	Yes, further investigation is required.	6-Apr-15	N/A	6-Apr-15	Contact Centre Agent	6-Apr-15	Provide client instructions and requirements for withdrawal from screening correspondence program.	Contact Centre Agent	6-Apr-15	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-PEDMQV	Screen for Life	9-Apr-15	Yes, further investigation is required.	9-Apr-15	N/A	9-Apr-15	Contact Centre Agent	9-Apr-15	Provide the client further explanation about the nature of the screening programs. Clarify client's misunderstanding/concerns about the letters.	Contact Centre Agent	9-Apr-15	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is satisfied.
1-PKH4G4	CCC	10-Apr-15	Yes, however the client was anonymous	10-Apr-15	N/A	10-Apr-15	Contact Centre Agent	20-Apr-15	Provide the client further explanation about the nature of the screening programs. Clarify client's misunderstanding/concerns about the letters.	Contact Centre Agent	10-Apr-15	Provided the client explanation about the screening programs & option to withdraw. Client does not want to withdraw from correspondence.
1-PKH4FN	OBSP	10-Apr-15	Yes, further investigation is required.	10-Apr-15	N/A	10-Apr-15	Contact Centre Agent	20-Apr-15	Provide the client further explanation about the nature of the screening programs. Clarify client's misunderstanding/concerns about the letters.	Contact Centre Agent	10-Apr-15	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is satisfied.
1-Q9BAC8	OBSP	14-Apr-15	Yes, further investigation is required.	14-Apr-15	N/A	14-Apr-15	Contact Centre Agent	27-Apr-15	Provide the client further explanation about the nature of the screening programs. Clarify client's misunderstanding/concerns about the letters.	Contact Centre Agent	14-Apr-15	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is satisfied.

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-Q9BFUL	OCSP	14-Apr-15	Yes, however the client was anonymous	14-Apr-15	N/A	14-Apr-15	Contact Centre Agent	17-Apr-15	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	14-Apr-15	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is not satisfied with the legislation; informed management, provided IPC contact information.
1-Q9BG55	OCSP	14-Apr-15	Yes, however the client was anonymous	14-Apr-15	N/A	14-Apr-15	Contact Centre Agent	14-Apr-15	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	14-Apr-15	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is not satisfied with the legislation; informed management, provided IPC contact information.
1-Q9BIQR	OBSP	14-Apr-15	Yes, further investigation is required.	14-Apr-15	N/A	14-Apr-15	Contact Centre Agent	14-Apr-15	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	14-Apr-15	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-QEQGUL	OBSP	15-Apr-15	Yes, further investigation is required.	15-Apr-15	N/A	15-Apr-15	Contact Centre Agent	15-Apr-15	Provide the client further explanation about the nature of the screening programs and mailing logistics. Update client address/withdraw (facilitate as required).	Contact Centre Agent	15-Apr-15	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is satisfied.
1-QEREUT	OBSP	15-Apr-15	Yes, further investigation is required.	15-Apr-15	N/A	15-Apr-15	Contact Centre Agent	15-Apr-15	Provide the client further explanation about the nature of the screening programs and mailing logistics. Update client address/withdraw (facilitate as required).	Contact Centre Agent	15-Apr-15	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is satisfied.
1-QLLTUQ	OCSP	17-Apr-15	Yes, further investigation is required.	17-Apr-15	N/A	17-Apr-15	Contact Centre Agent	17-Apr-15	Provide client information about CCO and its legislative authority and regulatory compliance requirements.	Contact Centre Agent	17-Apr-15	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-R2B897	CCC	20-Apr-15	Yes, however the client was anonymous	20-Apr-15	N/A	20-Apr-15	Contact Centre Agent	20-Apr-15	Provide client instructions and requirements for withdrawal from screening correspondence program.	Contact Centre Agent	20-Apr-15	CCO attempted to address complaint for the client, client did not cooperate (hung up/no response)
1-R79JXF	OCSP	21-Apr-15	Yes, further investigation is required.	21-Apr-15	N/A	21-Apr-15	Contact Centre Agent	21-Apr-15	Provide client instructions and requirements for withdrawal from screening correspondence program.	Contact Centre Agent	21-Apr-15	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-RCNQBW	OCSP	24-Apr-15	Yes, further investigation is required.	28-Apr-15	N/A	28-Apr-15	Contact Centre Agent	28-Apr-15	Provide client instructions and requirements for withdrawal from screening correspondence program.	Contact Centre Agent	28-Apr-15	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-S1QVDR	OCSP	30-Apr-15	Yes, however the client was anonymous	30-Apr-15	N/A	30-Apr-15	Contact Centre Agent	30-Apr-15	Anonymous Client, attempt to contact if possible and address complaint.	Contact Centre Agent	30-Apr-15	Anonymous client, could not be identified, no further action possible.
1-S1QVG7	OBSP	30-Apr-15	Yes, further investigation is required.	30-Apr-15	N/A	30-Apr-15	Contact Centre Agent	30-Apr-15	Provide client instructions and requirements for withdrawal from screening correspondence program.	Contact Centre Agent	30-Apr-15	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-SL80YU	OCSP	6-May-15	Yes, however the client was anonymous	6-May-15	N/A	6-May-15	Contact Centre Agent	6-May-15	Provide client information about CCO and its legislative authority and regulatory compliance requirements.	Contact Centre Agent	30-Apr-15	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is not satisfied with the legislation; informed management, provided IPC contact information.

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-SRY0NW	Screen for Life	8-May-15	Yes, however the client was anonymous	8-May-15	N/A	8-May-15	Contact Centre Agent	8-May-15	Provide the client further explanation about the nature of the screening programs and options to withdraw (facilitate as required).	Contact Centre Agent	8-May-15	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is not satisfied with the legislation; informed management, provided IPC contact information.
1-T6PCJJ	CCC	13-May-15	Yes, further investigation is required.	13-May-15	N/A	13-May-15	Contact Centre Agent	13-May-15	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	13-May-15	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is satisfied.
1-TZ4DM1	OCSP	25-May-15	Yes, further investigation is required.	25-May-15	N/A	25-May-15	Contact Centre Agent	25-May-15	Provide client information about CCO and its legislative authority and regulatory compliance requirements.	Contact Centre Agent	25-May-15	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-U1I9OR	OCSP	26-May-15	Yes, however the client was anonymous	26-May-15	N/A	26-May-15	Contact Centre Agent	26-May-15	Provide the client further explanation about the nature of the screening programs. Clarify client's misunderstanding/concerns about the letters.	Contact Centre Agent	26-May-15	Provided the client explanation about the screening programs & option to withdraw. Client does not want to withdraw from correspondence.

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-U3YHNQ	OCSP	28-May-15	Yes, further investigation is required.	28-May-15	N/A	28-May-15	Contact Centre Agent	28-May-15	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	28-May-15	Provided the client explanation about the screening programs & option to withdraw. Client does not want to withdraw from correspondence.
1-UF0YCU	OCSP	3-Jun-15	Yes, further investigation is required.	3-Jun-15	N/A	3-Jun-15	Contact Centre Agent	3-Jun-15	Provide the client further explanation about the nature of the screening programs. Clarify client's misunderstanding/concerns about the letters.	Contact Centre Agent	3-Jun-15	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-UFU5KL	Screen for Life	4-Jun-15	Yes, however the client was anonymous	4-Jun-15	N/A	4-Jun-15	Contact Centre Agent	4-Jun-15	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	4-Jun-15	CCO attempted to address complaint for the client, client did not cooperate (hung up/no response)
1-UFU5M4	Screen for Life	4-Jun-15	Yes, however the client was anonymous	4-Jun-15	N/A	4-Jun-15	Privacy and CC	17-Jun-15	Provide client information about CCO and its legislative authority and regulatory compliance requirements.	Privacy and CC	4-Jun-15	CCO attempted to address complaint for the client, client did not cooperate (hung up/no response)
1-UFU660	Screen for Life	4-Jun-15	Yes, however the client was anonymous	4-Jun-15	N/A	4-Jun-15	Contact Centre Agent	4-Jun-15	Provide client information about CCO and its legislative authority and regulatory compliance requirements.	Contact Centre Agent	4-Jun-15	CCO attempted to address complaint for the client, client did not cooperate (hung up/no response)

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-UQG9YQ	OCSP	8-Jun-15	Yes, further investigation is required.	8-Jun-15	N/A	8-Jun-15	Contact Centre Agent	8-Jun-15	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	8-Jun-15	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-UVEMSI	OCSP	11-Jun-15	Yes, further investigation is required.	11-Jun-15	N/A	11-Jun-15	Contact Centre Agent	11-Jun-15	Provide client instructions and requirements for withdrawal from screening correspondence program.	Contact Centre Agent	11-Jun-15	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-UYHNQI	OCSP	12-Jun-15	Yes, further investigation is required.	12-Jun-15	N/A	12-Jun-15	Contact Centre Agent	12-Jun-15	Provide the client further explanation about the nature of the screening programs and mailing logistics. Update client address/withdraw (facilitate as required).	Contact Centre Agent	12-Jun-15	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-UYHQWH	Screen for Life	15-Jun-15	Yes, further investigation is required.	15-Jun-15	N/A	15-Jun-15	Privacy and CC	15-Jun-15	No further action required/possible.	Privacy and CC	15-Jun-15	No further action required/possible.
1-V6653F	OCSP	15-Jun-15	Yes, however the client was anonymous	15-Jun-15	N/A	15-Jun-15	Contact Centre Agent	15-Jun-15	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	15-Jun-15	Provided the client explanation about the screening programs & option to withdraw. Client does not want to withdraw from correspondence.
1-VALX5J	OBSP	18-Jun-15	Yes, further investigation is required.	18-Jun-15	N/A	18-Jun-15	Contact Centre Agent	18-Jun-15	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	18-Jun-15	Provided the client explanation about the screening programs & option to withdraw. Client does not want to withdraw from correspondence.

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-VBE1ZI	OCSP	18-Jun-15	Yes, further investigation is required.	18-Jun-15	N/A	18-Jun-15	Contact Centre Agent	18-Jun-15	Provide the client further explanation about the nature of the screening programs. Clarify client's misunderstanding/concerns about the letters.	Contact Centre Agent	18-Jun-15	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-VBE6TV	OCSP	18-Jun-15	Yes, further investigation is required.	18-Jun-15	N/A	18-Jun-15	Contact Centre Agent	19-Jun-15	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	18-Jun-15	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-VLEE55	OBSP	22-Jun-15	Yes, further investigation is required.	22-Jun-15	N/A	22-Jun-15	Contact Centre Agent	22-Jun-15	Provide client instructions and requirements for withdrawal from screening correspondence program.	Contact Centre Agent	22-Jun-15	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-VLG2ZR	OCSP	23-Jun-15	Yes, further investigation is required.	23-Jun-15	N/A	23-Jun-15	Contact Centre Agent	23-Jun-15	Provide client instructions and requirements for withdrawal from screening correspondence program.	Contact Centre Agent	23-Jun-15	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-VPMEKJ	Screen for Life	24-Jun-15	Yes, however the client was anonymous	23-Jun-15	N/A	24-Jun-15	Privacy Specialist	29-Jun-15	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Privacy Specialist	24-Jun-15	Provided the client explanation about the screening programs & option to withdraw. Client does not want to withdraw from correspondence.

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-VQDNSI	OCSP	25-Jun-15	Yes, further investigation is required.	25-Jun-15	N/A	25-Jun-15	Contact Centre Agent	25-Jun-15	Provide client instructions and requirements for withdrawal from screening correspondence program.	Contact Centre Agent	25-Jun-15	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-VSFC4P	OCSP	26-Jun-15	Yes, further investigation is required.	26-Jun-15	N/A	26-Jun-15	Contact Centre Agent	26-Jun-15	Provide client instructions and requirements for withdrawal from screening correspondence program.	Contact Centre Agent	26-Jun-15	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-W26RJC	OCSP	30-Jun-15	Yes, further investigation is required.	30-Jun-15	N/A	30-Jun-15	Contact Centre Agent	30-Jun-15	Provide the client further explanation about the nature of the screening programs. Clarify client's misunderstanding/concerns about the letters.	Contact Centre Agent	30-Jun-15	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-W6S147	OCSP	2-Jul-15	Yes, further investigation is required.	2-Jul-15	N/A	2-Jul-15	Contact Centre Agent	3-Jul-15	Provide the client further explanation about the nature of the screening programs. Clarify client's misunderstanding/concerns about the letters.	Contact Centre Agent	2-Jul-15	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is satisfied.
1-W9AEFD	OCSP	3-Jul-15	Yes, further investigation is required.	3-Jul-15	N/A	3-Jul-15	Contact Centre Agent	3-Jul-15	No further action required/possible.	Contact Centre Agent	3-Jul-15	No further action required/possible.
1-WINQ6O	OBSP	8-Jul-15	Yes, further investigation is required.	8-Jul-15	N/A	8-Jul-15	Contact Centre Agent	10-Jul-15	Provide the client further explanation about the nature of the screening programs. Clarify client's misunderstanding/concerns about the letters.	Contact Centre Agent	8-Jul-15	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-WNPCNA	OBSP	10-Jul-15	Yes, further investigation is required.	10-Jul-15	N/A	10-Jul-15	Contact Centre Agent	13-Jul-15	Provide client instructions and requirements for withdrawal from screening correspondence program.	Contact Centre Agent	10-Jul-15	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-WV3QV0	OCSP	13-Jul-15	Yes, further investigation is required.	13-Jul-15	N/A	13-Jul-15	Contact Centre Agent	13-Jul-15	Provide the client further explanation about the nature of the screening programs. Clarify client's misunderstanding/concerns about the letters.	Contact Centre Agent	13-Jul-15	Provided the client explanation about the screening programs & option to withdraw. Client does not want to withdraw from correspondence.
1-X091QK	OBSP	16-Jul-15	Yes, further investigation is required.	16-Jul-15	N/A	16-Jul-15	Contact Centre Agent	16-Jul-15	Provide the client further explanation about the nature of the screening programs. Clarify client's misunderstanding/concerns about the letters.	Contact Centre Agent	16-Jul-15	Provided the client explanation about the screening programs & option to withdraw. Client does not want to withdraw from correspondence.
1-XGUDXP	OCSP	24-Jul-15	Yes, further investigation is required.	24-Jul-15	N/A	24-Jul-15	Contact Centre Agent	24-Jul-15	Provide client information about CCO and its legislative authority and regulatory compliance requirements.	Contact Centre Agent	24-Jul-15	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is not satisfied with the legislation; informed management, provided IPC contact information.

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-XNJMEC	Screen for Life	27-Jul-15	Yes, however the client was anonymous	27-Jul-15	N/A	27-Jul-15	Contact Centre Agent	27-Jul-15	Provide client information about CCO and its legislative authority and regulatory compliance requirements.	Contact Centre Agent	27-Jul-15	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is not satisfied with the legislation; informed management, provided IPC contact information.
1-XRJQJA	Screen for Life	29-Jul-15	Yes, however the client was anonymous	29-Jul-15	N/A	29-Jul-15	Contact Centre Agent	29-Jul-15	Provide client information about CCO and its legislative authority and regulatory compliance requirements.	Contact Centre Agent	29-Jul-15	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is not satisfied with the legislation; informed management, provided IPC contact information.
1-XSA01G	OCSP	30-Jul-15	Yes, further investigation is required.	30-Jul-15	N/A	30-Jul-15	Contact Centre Agent	30-Jul-15	Provide the client further explanation about the nature of the screening programs. Clarify client's misunderstanding/concerns about the letters.	Contact Centre Agent	30-Jul-15	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-Y48H0X	Screen for Life	4-Aug-15	Yes, further investigation is required.	4-Aug-15	N/A	4-Aug-15	Privacy Specialist	11-Sep-15	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Privacy Specialist	4-Aug-15	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is not satisfied with the legislation; informed management, provided IPC contact information.
1-Y48H55	OCSP	4-Aug-15	Yes, further investigation is required.	4-Aug-15	N/A	4-Aug-15	Contact Centre Agent	4-Aug-15	Provide the client further explanation about the nature of the screening programs. Clarify client's misunderstanding/concerns about the letters.	Contact Centre Agent	4-Aug-15	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is satisfied.
1-YL9RAB	OCSP	13-Aug-15	Yes, further investigation is required.	13-Aug-15	N/A	13-Aug-15	Contact Centre Agent	13-Aug-15	Provide the client further explanation about the nature of the screening programs and mailing logistics. Update client address/withdraw (facilitate as required).	Contact Centre Agent	13-Aug-15	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-YNCJ2U	OCSP	14-Aug-15	Yes, further investigation is required.	14-Aug-15	N/A	14-Aug-15	Contact Centre Agent	14-Aug-15	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	14-Aug-15	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client unhappy about the legislation.

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-Z95WYV	OCSP	24-Aug-15	Yes, further investigation is required.	24-Aug-15	N/A	24-Aug-15	Contact Centre Agent	24-Aug-15	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	24-Aug-15	Provided the client explanation about the screening programs & option to withdraw. Client does not want to withdraw from correspondence.
1-ZH16XT	OCSP	28-Aug-15	Yes, further investigation is required.	28-Aug-15	N/A	28-Aug-15	Privacy and CC	28-Aug-15	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Privacy Specialist	4-Sep-15	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is not satisfied with the legislation; informed management, provided IPC contact information.
1-ZTADFZ	OCSP	3-Sep-15	Yes, further investigation is required.	3-Sep-15	N/A	3-Sep-15	Contact Centre Agent	3-Sep-15	Provide client instructions and requirements for withdrawal from screening correspondence program.	Contact Centre Agent	3-Sep-15	Provided the client explanation about the screening programs & option to withdraw. Client does not want to withdraw from correspondence.
1-ZVS2IL	OBSP	4-Sep-15	Yes, further investigation is required.	4-Sep-15	N/A	4-Sep-15	Contact Centre Agent	4-Sep-15	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	4-Sep-15	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-ZVS2S6	OCSP	4-Sep-15	Yes, further investigation is required.	4-Sep-15	N/A	4-Sep-15	Contact Centre Agent	4-Sep-15	Provide client instructions and requirements for withdrawal from screening correspondence program.	Contact Centre Agent	4-Sep-15	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-107QNAT	OBSP	9-Sep-15	Yes, further investigation is required.	9-Sep-15	N/A	9-Sep-15	Contact Centre Agent	9-Sep-15	Provide the client further explanation about the nature of the screening programs and mailing logistics. Update client address/withdraw (facilitate as required).	Contact Centre Agent	9-Sep-15	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-10AOCLN	OCSP	11-Sep-15	Yes, further investigation is required.	11-Sep-15	N/A	11-Sep-15	Contact Centre Agent	17-Sep-15	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	11-Sep-15	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-10P9D8T	OCSP	18-Sep-15	Yes, further investigation is required.	18-Sep-15	N/A	18-Sep-15	Contact Centre Agent	18-Sep-15	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	18-Sep-15	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-10TTKT0	OCSP	21-Sep-15	Yes, however the client was anonymous	21-Sep-15	N/A	21-Sep-15	Contact Centre Agent	22-Sep-15	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	21-Sep-15	CCO attempted to address complaint for the client, client did not cooperate (hung up/no response)

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-10W26DG	OBSP	21-Sep-15	Yes, further investigation is required.	21-Sep-15	N/A	21-Sep-15	Contact Centre Agent	22-Sep-15	Provide the client further explanation about the nature of the screening programs and options to withdraw (facilitate as required).	Contact Centre Agent	21-Sep-15	Provided the client explanation about the screening programs & option to withdraw. Client does not want to withdraw from correspondence.
1-10Y3XIN	OCSP	22-Sep-15	Yes, further investigation is required.	22-Sep-15	N/A	22-Sep-15	Privacy and CC	22-Sep-15	Provide the client further explanation about the nature of the screening programs and options to withdraw (facilitate as required).	Privacy and CC	22-Sep-15	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-11044JR	Screen for Life	23-Sep-15	Yes, further investigation is required.	23-Sep-15	N/A	23-Sep-15	Privacy and CC	23-Sep-15	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Privacy and CC	23-Sep-15	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is not satisfied with the legislation; informed management, provided IPC contact information.
1-1104B73	CCC	23-Sep-15	Yes, further investigation is required.	23-Sep-15	N/A	23-Sep-15	Contact Center Management	23-Sep-15	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Center Management	23-Sep-15	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is not satisfied with the legislation; informed manageme

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
												nt, provided IPC contact information.
1-11044JR	Screen for Life	23-Sep-15	Yes, further investigation is required.	23-Sep-15	N/A	23-Sep-15	Privacy and CC	17-Dec-15	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Privacy and CC	17-Dec-15	Provided the client explanation about the screening programs & option to withdraw. Client does not want to withdraw from correspondence.
1-11RT70F	OCSP	7-Oct-15	Yes, further investigation is required.	7-Oct-15	N/A	7-Oct-15	Contact Centre Agent	7-Oct-15	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	7-Oct-15	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-11UH8LY	Screen for Life	9-Oct-15	Yes, however the client was anonymous	9-Oct-15	N/A	9-Oct-15	Contact Centre Agent	9-Oct-15	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	9-Oct-15	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is not satisfied with the legislation; informed management,

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
												provided IPC contact information.
1-1253REK	OCSP	14-Oct-15	Yes, further investigation is required.	14-Oct-15	N/A	14-Oct-15	Contact Centre Agent	14-Oct-15	Provide client instructions and requirements for withdrawal from screening correspondence program.	Contact Centre Agent	14-Oct-15	Provided the client explanation about the screening programs & option to withdraw. Client does not want to withdraw from correspondence.
1-133KJRX	OCSP	2-Nov-15	Yes, further investigation is required.	2-Nov-15	N/A	2-Nov-15	Contact Centre Agent	8-Dec-15	Provide the client further explanation about the nature of the screening programs and mailing logistics. Update client address/withdraw (facilitate as required).	Contact Center Management	8-Dec-15	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-13PLIZO	OCSP	13-Nov-15	Yes, further investigation is required.	13-Nov-15	N/A	13-Nov-15	Contact Centre Agent	13-Nov-15	Provide the client further explanation about the nature of the screening programs. Clarify client's misunderstanding/concerns about the letters.	Contact Centre Agent	13-Nov-15	Provided the client explanation about the screening programs & option to withdraw. Client does not want to withdraw from correspondence.

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-13PLJ38	OCSP	13-Nov-15	Yes, further investigation is required.	13-Nov-15	N/A	13-Nov-15	Privacy Specialist	16-Dec-15	Provide the client further explanation about the nature of the screening programs. Clarify client's misunderstanding/concerns about the letters.	Privacy Specialist	17-Nov-15	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is satisfied.
1-142KAYT	CCC	19-Nov-15	Yes, however the client was anonymous	19-Nov-15	N/A	19-Nov-15	Contact Centre Agent	19-Nov-15	Anonymous Client, attempt to contact if possible and address complaint.	Contact Centre Agent	19-Nov-15	Anonymous client, could not be identified, no further action possible.
1-14EAABB	CCC	24-Nov-15	Yes, however the client was anonymous	24-Nov-15	N/A	24-Nov-15	Contact Centre Agent	24-Nov-15	Anonymous Client, attempt to contact if possible and address complaint.	Contact Centre Agent	24-Nov-15	CCO attempted to address complaint for the client, client did not cooperate (hung up/no response)
1-14EAADN	OCSP	24-Nov-15	Yes, however the client was anonymous	24-Nov-15	N/A	24-Nov-15	Contact Centre Agent	24-Nov-15	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	24-Nov-15	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is satisfied.
1-14JM3OX	OCSP	27-Nov-15	Yes, further investigation is required.	27-Nov-15	N/A	27-Nov-15	Contact Centre Agent	27-Nov-15	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	27-Nov-15	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client unhappy about the legislation.

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-157I7TJ	OBSP	9-Dec-15	Yes, further investigation is required.	9-Dec-15	N/A	9-Dec-15	Contact Centre Agent	16-Dec-15	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	16-Dec-15	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is not satisfied with the legislation; informed management, provided IPC contact information.
1-16CGP6Z	OCSP	7-Jan-16	Yes, further investigation is required.	8-Jan-16	N/A	8-Jan-16	Privacy and CC	2-Feb-16	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Privacy and CC	8-Jan-16	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is not satisfied with the legislation; informed management, provided IPC contact information.
1-17JHQF1	OCSP	28-Jan-16	Yes, however the client was anonymous	28-Jan-16	N/A	28-Jan-16	Contact Centre Agent	28-Jan-16	Provide the client further explanation about the nature of the screening programs. Clarify client's misunderstanding/concerns about the letters.	Contact Centre Agent	1-Feb-16	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-17MIEAW	OBSP	26-Jan-16	Yes, further investigation is required.	26-Jan-16	N/A	26-Jan-16	Contact Centre Agent	29-Jan-16	Provide the client further explanation about the nature of the screening programs and mailing logistics. Update client address/withdraw (facilitate as required).	Contact Centre Agent	29-Jan-16	Provided client rationale for misdirected letter. Warm transferred the client to Canada Post to ensure error is not repeated.
1-181Y537	OCSP	8-Feb-16	Yes, will be investigated.	8-Feb-16	N/A	8-Feb-16	Contact Centre Agent	8-Feb-16	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	8-Feb-16	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client unhappy about the legislation.
1-18EOD0R	OCSP	12-Feb-16	Yes, will be investigated.	12-Feb-16	12-Feb-16	Re-curring complainant, advised multiple times. Only contacts via email, provided option to go to IPC.	Contact Center Management	12-Feb-16	No further action required/possible.	Contact Center Management	12-Feb-16	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is not satisfied with the legislation; informed management, provided IPC contact information.
1-18TOWH6	OCSP	22-Feb-16	Yes, will be investigated.	22-Feb-16	n/a	22-Feb-16	Contact Centre Agent	22-Feb-16	Anonymous Client, attempt to contact if possible and address complaint.	Contact Centre Agent	22-Feb-16	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client unhappy

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
												about the legislation.
1-18TOWPI	OCSP	22-Feb-16	Yes, further investigation is required.	22-Feb-16	n/a	22-Feb-16	Contact Center Management	3-Mar-16	Provide the client further explanation about the nature of the screening programs and mailing logistics. Update client address/withdraw (facilitate as required).	Contact Centre Agent	3-Mar-16	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-18TOWQQ	OBSP	22-Feb-16	Yes, will be investigated.	22-Feb-16	n/a	22-Feb-16	Contact Centre Agent	22-Feb-16	Provide the client further explanation about the nature of the screening programs and mailing logistics. Update client address/withdraw (facilitate as required).	Contact Centre Agent	22-Feb-16	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-18ZOWIE	Public Affairs	26-Feb-16	Yes, will be investigated.	26-Feb-16	n/a	26-Feb-16	Contact Centre Agent	26-Feb-16	Provide the client further explanation about the nature of the screening programs and mailing logistics. Update client address/withdraw (facilitate as required).	Contact Centre Agent	26-Feb-16	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is not satisfied with the legislation; informed management, provided IPC contact information.

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-19W2C3K	Screen for Life	17-Mar-16	Yes, will be investigated.	17-Mar-16	n/a	17-Mar-16	Privacy and CC	18-Mar-16	Provide the client further explanation about the nature of the screening programs and options to withdraw (facilitate as required).	Privacy and CC	18-Mar-16	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client unhappy about the legislation.
1-1A3I9Q9	Screen for Life	22-Mar-16	Yes, will be investigated.	22-Mar-16	n/a	22-Mar-16	Contact Centre Agent	22-Mar-16	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Contact Centre Agent	22-Mar-16	CCO attempted to address complaint for the client, client did not cooperate (hung up/no response)
1-1AI4U9H	Screen for Life	30-Mar-16	Yes, will be investigated.	30-Mar-16	30-Mar-16	30-Mar-16	Contact Centre Agent	30-Mar-16	Provide the client further explanation about the nature of the screening programs. Clarify client's misunderstanding/concerns about the letters.	Contact Centre Agent	30-Mar-16	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client unhappy about the legislation.
1-1BECX93	Screen for Life	14-Apr-16	Yes, will be investigated.	14-Apr-16	N/A	19-Apr-16	Privacy and CC	19-Apr-16	Provide the client further explanation about the nature of the screening programs and mailing logistics. Update client address/withdraw (facilitate as required).	Contact Centre Agent	19-Apr-16	Client complaint was received and addressed via email. No response in return.
1-1C6EQRJ	CCC	6-May-16	Yes, will be investigated.	6-May-16	N/A	6-May-16	Privacy and CC	10-May-16	Provide the client further explanation about the nature of the screening programs and options to withdraw (facilitate as required).	Contact Centre Agent	10-May-16	Anonymous client was tracked, addressed complaint (withdrew client).

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-1DB917F	OCSP	30-May-16	Yes, will be investigated.	30-May-16	N/A	30-May-16	Contact Centre Agent	22-Jun-16	Provide the client further explanation about the nature of the screening programs. Clarify client's misunderstanding/concerns about the letters.	Contact Centre Agent	22-Jun-16	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-1DFEYH7	Screen for Life	2-Jun-16	Yes, will be investigated.	8-Jun-16	22-Jun-16	22-Jun-16	Privacy and CC	22-Jun-16	Provide the client further explanation about the nature of the screening programs. Clarify client's misunderstanding/concerns about the letters.	Contact Center Management	22-Jun-16	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is not satisfied with the legislation; informed management, provided IPC contact information.
1-1DXUIQW	OCSP	13-Jun-16	Yes, will be investigated.	13-Jun-16	13-Jun-16	13-Jun-16	Contact Centre Agent	13-Jun-16	Provide the client further explanation about the nature of the screening programs and mailing logistics. Update client address/withdraw (facilitate as required).	Contact Centre Agent	13-Jun-16	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-1DXUITL	Screen for Life	13-Jun-16	Yes, will be investigated.	13-Jun-16	13-Jun-16	13-Jun-16	Contact Centre Agent	13-Jun-16	Anonymous Client, attempt to contact if possible and address complaint.	Contact Centre Agent	13-Jun-16	Anonymous client, could not be identified, no further action possible.
1-1DZGWLE	OCSP	14-Jun-16	Yes, will be investigated.	14-Jun-16	14-Jun-16	14-Jun-16	Contact Centre Agent	14-Jun-16	Provide the client further explanation about the nature of the screening programs and mailing logistics. Update client address/withdraw (facilitate as required).	Contact Centre Agent	14-Jun-16	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-1E9QLZV	OBSP	20-Jun-16	Yes, will be investigated.	20-Jun-16	n/a	20-Jun-16	Contact Centre Agent	20-Jun-16	Provide the client further explanation about the nature of the screening programs and mailing logistics. Update client address/withdraw (facilitate as required).	Contact Centre Agent	20-Jun-16	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-1EGK069	CCC	22-Jun-16	Yes, will be investigated.	24-Jun-16	N/A	18-Jul-16	Privacy and CC	5-Jul-16	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Privacy and CC	5-Jul-16	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is not satisfied with the legislation; informed management, provided IPC contact information.
1-1EWYE5G	OCSP	5-Jul-16	Yes, will be investigated.	5-Jul-16	5-Jul-16	n/a	Contact Centre Agent	5-Jul-16	Provide the client further explanation about the nature of the screening programs. Clarify client's misunderstanding/concerns about the letters.	Contact Centre Agent	5-Jul-16	CCO attempted to address complaint for the client, client did not cooperate (hung up/no response)
1-1FQ037T	OBSP	27-Jul-16	Yes, will be investigated.	27-Jul-16	n/a	27-Jul-16	Privacy Specialist	27-Jul-16	No further action required/possible.	Contact Centre Agent	27-Jul-16	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is satisfied.

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-1FUFXXJ	Screen for Life	29-Jul-16	Yes, will be investigated.	29-Jul-16	n/a	10-Aug-16	Privacy and CC	11-Aug-16	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Privacy Specialist	10-Aug-16	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client unhappy about the legislation.
1-1G1I7AC	OCSP	4-Aug-16	Yes, will be investigated.	4-Aug-16	n/a	4-Aug-16	Privacy and CC	11-Aug-16	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Privacy and CC	11-Aug-16	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client unhappy about the legislation.
1-1G8JVJ8	Screen for Life	8-Aug-16	Yes, will be investigated.	8-Aug-16	n/a	n/a	Contact Centre Agent	8-Aug-16	No further action required/possible.	Contact Centre Agent	8-Aug-16	CCO attempted to address complaint for the client, client did not cooperate (hung up/no response)
1-1GCKIG3	OCSP	11-Aug-16	Yes, will be investigated.	11-Aug-16	n/a	17-Aug-16	Privacy Specialist	24-Aug-16	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Privacy Specialist	17-Aug-16	Provided client information on CCO's Screening Programs, Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client is not satisfied with the legislation; informed management, provided IPC contact information.

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
1-1HD1LUS	OBSP	7-Sep-16	Yes, will be investigated.	7-Sep-16	n/a	7-Sep-16	Contact Centre Agent	7-Sep-16	Provide the client further explanation about the nature of the screening programs and mailing logistics. Update client address/withdraw (facilitate as required).	Contact Centre Agent	7-Sep-16	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-1HMXF73	CCC	13-Sep-16	Yes, will be investigated.	13-Sep-16	n/a	n/a	Privacy and CC	13-Sep-16	Provide the client further explanation about the nature of the screening programs and mailing logistics. Update client address/withdraw (facilitate as required).	Contact Centre Agent	13-Sep-16	CCO attempted to address complaint for the client, client did not cooperate (hung up/no response)
1-1HVJ0JU	Screen for Life	19-Sep-16	Yes, will be investigated.	19-Sep-16	n/a	n/a	Contact Centre Agent	19-Sep-16	Provide the client further explanation about the nature of the screening programs. Clarify client's misunderstanding/concerns about the letters.	Contact Centre Agent	19-Sep-16	Anonymous client, could not be identified, no further action possible.
1-1HY0XUZ	OCSP	21-Sep-16	Yes, will be investigated.	21-Sep-16	n/a	n/a	Contact Centre Agent	21-Sep-16	Anonymous Client, attempt to contact if possible and address complaint.	Contact Centre Agent	21-Sep-16	CCO attempted to address complaint for the client, client did not cooperate (hung up/no response)
1-1AU4LDR	Screen for Life	8-Apr-16	Yes, will be investigated.	8-Apr-16	n/a	n/a	Contact Centre Agent	8-Apr-16	Provide the client further explanation about the nature of the screening programs. Clarify client's misunderstanding/concerns about the letters.	Contact Centre Agent	8-Apr-16	Provided the client explanation about the screening programs & option to withdraw. Facilitated withdrawal from correspondence.
1-1HMXF73	CCC	13-Sep-16	Yes, will be investigated.	13-Sep-16	n/a	n/a	Contact Centre Agent	15-Sep-16	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Update client address/withdraw (facilitate as required).	Privacy and CC	15-Sep-16	Provide client information on CCO's Privacy Policies, Breach Management, legislative authority and regulatory compliance with IPC. Client

Activity #	Program	Date of the Complaint Received	Will the complaint be investigated	Date the decision to investigate (or not) is determined	Date the complainant advised: no investigation to be conducted/ provided response to their complaint	Date Complainant advised the complaint will be investigated	Agent to conduct investigation	Date Investigation Completed	Recommendations	Agent responsible for addressing each recommendation	Date recommendation was addressed	Manner in which recommendations were addressed
												unhappy about the legislation.

Appendix L: Checklist

Table 1 Privacy Checklist

IPC 2017 Triennial Review - Requested Privacy Documentation				
Req.	**Minimum Content of Required Documentation**	**Page Ref# in Manual**	**Req't Met**	**Identifying CCO Document**
1	**Privacy Policy (with respect to PE/PR)**			
	· An overarching privacy policy	15	✓	CCO's Privacy Policy
	· Describes the status of CCO and duties of CCO (prescribed entity (PE) and prescribed registry (PR))	15	✓	CCO's Privacy Policy
	Must indicate PR/PE has implemented policies/procedures/practices to protect privacy of individual's PHI and to maintain the confidentiality of that information and that these policies/procedures/practices are subject to IPC review every 3 years	15	✓	CCO's Privacy Policy
	· Articulates a commitment to comply with the provisions of the Act and its regulation applicable to PE/PR, as the case may be	15	✓	CCO's Privacy Policy
	· identify other positions or committees that support the privacy and security program, and their role in respect of these programs	15	✓	CCO's Privacy Policy
	· accountability framework for ensuring compliance with the *Act* aand CCO's security policies, procedures and practices must be articulated	15	✓	CCO's Privacy Policy
	· delegated day-to-day authority of the privacy and security program	15	✓	CCO's Privacy Policy
	Must identify the positions that have been delegated day-to-day authority to manage the privacy program and the security program and to whom these positions report	15	✓	CCO's Privacy Policy

	Must further identify the duties and responsibilities of the position(s) that have been delegated day-to-day authority to manage the privacy program and the security program and some of the key activities of these programs.	15	✓	Job descriptions: Director, Legal & Privacy; Group Manager, Privacy; Senior Privacy Specialist; Privacy Specialist
	· Indicates the Chief Executive Officer or the Executive Director, is accountable for ensuring compliance with the *Act,* its regulation and for ensuring compliance with privacy & security policies/procedures/practices	15	✓	CCO's Privacy Policy
	· CCO remains responsible for PHI used by its agents and identifies the policies/procedures/practices implemnted to ensure that its agents only collect, use, disclose, retain, and dispose of personal health information in compliance with the Act and in compliance with CCO policies	16	✓	CCO's Privacy Policy
	· Identifies the purposes for which PHI is collected, the types of PHI collected and the persons or organizations from which PHI is typically collected.	16	✓	CCO's Privacy Policy
	· not collecting PHI if other information will serve the purpose	16	✓	CCO's Privacy Policy
	· must ensure each collection identified in the Privacy Policy is consistent with the collections of PHI permitted by the Act and its regulation	16	✓	CCO's Privacy Policy
	· not collecting more PHI than is reasonably necessary to meet the purpose.	16	✓	CCO's Privacy Policy
	Policy must outline the policies, procedures and practices implemented by the PE/PR to ensure that both the amount and the type of PHI collected is limited to that which is reasonably necessary for its purpose	16	✓	CCO's Privacy Policy

	· a list of the data holdings of PHI maintained by CCO and where an individual may obtain further information in relation to the purposes of PHI data holdings	16	✓	CCO's Privacy Policy
	· Uses of PHI must be identified and each use of PHI must be consistent with the uses of PHI permitted by the Act and its regulation.	16	✓	CCO's Privacy Policy
	· Clearly distinguish between the use of PHI for purposes of section 39(1) or section 45 of PHIPA, and the use of PHI for research purposes	16	N/A	All research undertaken by CCO, per section 44 of PHIPA, is considered a disclosure of PHI to the researcher and is not considered a use of PHI for research purposes
	· Clearly distinguish between the use of PHI and the use of de-identified information and/or aggregate information.	16	✓	CCO's Privacy Policy; Data Use & Disclosure Standard; De-Identification Guidelines
	· not using PHI if other information will serve the purpose or not using more PHI than is reasonably necessary to meet the purpose and must identify some of the policies/procedures/practices of CCO in this regard, including limits to the use of PHI by agents	16	✓	CCO's Privacy Policy; Data Use & Disclosure Standard;
	· the purposes for which and the circumstances where PHI is disclosed and to whom disclosures are typically made	17	✓	CCO's Privacy Policy; Data Use & Disclosure Standard;
	· the statutory requirements that must be satisfied prior to disclosures- each disclosure of PHI identified in the Privacy Policy is consistent with	17	✓	CCO's Privacy Policy; Data Use and & Disclosure Standard and;

	the disclosures permitted by the Act and its regulation			Decision Criteria for Data Requests
	· distinguish between the purposes for which and the circumstances in which ~~when~~ PHI is disclosed and ~~when~~ the circumstances in which and the purposes for which de-identified and/or aggregate information is disclosed.	17	✓	CCO's Privacy Policy; Data Use & Disclosure Standard; De-Identification Guidelines
	· Review all de-identified and/or aggregate information prior to its disclosure in order to ensure that it is not reasonably foreseeable in the circumstances that the information could be used, either alone or with other information, to identify an individual	17	✓	CCO's Privacy Policy; Data Use & Disclosure Standard; De-Identification Guidelines
	· not disclosing PHI or not disclosing more PHI than is reasonably necessary to meet the purpose and identify some of the policies/procedures/practices implemented by CCO in this regard	17	✓	CCO's Privacy Policy; Data Use & Disclosure Standard; De-Identification Guidelines
	· address how long records of PHI are retained; whether the records are retained in identifiable form; the secure manner in which they are retained; and the manner in which records of PHI will be securely transferred and disposed of	17	✓	CCO's Privacy Policy; Digital Media Disposal Procedure; Digital Media Disposal Standard
	· outline some of the administrative, technical, and physical safeguards implemented to protect the privacy of individuals whose PHI is received and to maintain the confidentiality of that information, including steps taken to protect PHI against theft, loss, unauthorized use, or disclosure, and to protect records of PHI against	17	✓	CCO's Privacy Policy; Information Security Policy

	unauthorized copying, modification, or disposal. Must include requirement for secure retention of records of PHI			
	· contact information where individuals may direct inquiries or complaints related to privacy policies and practices of CCO. Contact information must include the name and/or title, mailing address, and the manner and format in which complaints or inquiries may be made. It should also state that individuals may direct complaints about CCO's compliance with PHIPA to the IPC and provide the mailing address and contact information for the IPC.	17-18	✓	CCO's Privacy Policy; Statement of Information Practices; Privacy Inquiries and Complaints Procedures
2	**Policy and Procedures for ongoing review of privacy policies procedures and practices**			
	· Policies and procedures need to be developed and implemented for the ongoing review of the privacy policies, procedures and practices. Review must occur on an annual basis.	18	✓	CCO's Privacy Policy; Privacy Audit and Compliance Policy
	o Must Identify: the frequency of the review, the agent(s) responsible for undertaking the review, the procedure to be followed in undertaking the review, the time frame in which the review will be undertaken	18	✓	Privacy Audit and Compliance Policy
	· identify the agent(s) responsible and the procedure to be followed in reviewing, amending and/or drafting new privacy policies, procedures and practices, including the approval of any amended or draft new policies.	18	✓	Privacy Audit and Compliance Policy

	· When reviewing if new privacy policies, procedures and practices are necessary, or amendments are required CCO must have regard to:	18	✓	Privacy Audit and Compliance Policy
	o orders, guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner of Ontario	18	✓	Privacy Audit and Compliance Policy
	o evolving industry privacy standards and best practices	18	✓	Privacy Audit and Compliance Policy
	o amendments to the Act and its regulation relevant to CCO	18	✓	Privacy Audit and Compliance Policy
	o recommendations arising from privacy and security audits, privacy impact assessments and investigations into privacy complaints, privacy breaches and information security breaches. And whether there is consistency with its actual practices and whether there is consistency between and among the privacy and security policies, procedures, and practices implemented.	18	✓	Privacy Audit and Compliance Policy
	· privacy policies, procedures and practices of CCO continue to be consistent with its actual practices	18	✓	Privacy Audit and Compliance Policy
	· stipulate that compliance will be audited in accordance with the *Policy and Procedures In Respect of Privacy Audit,* set out the frequency with which policies and procedures will be audited, and the agent responsible for conducting the audit and for ensuring compliance	19	✓	Privacy Audit and Compliance Policy; Logging, Monitoring and Auditing Standard
	· identify the agent(s) responsible and the procedure to be followed when communciating amended or new privacy policies, procedures and practices	19	✓	Privacy Audit and Compliance Policy

	· identify the agent(s) responsible and the procedure to be followed when reviewing and amending the communication materials available to the public when amendments or new policies are created. Method and nature of communication to be identified when when communicating amended or newly developed policies and procedures.	19	✓	Privacy Audit and Compliance Policy
	· require agents to comply with the policy and its procedures	19	✓	Privacy Audit and Compliance Policy
3	**Policy on the transparency of privacy policies, procedures and practices**			
	· identifies information made available to the public and other stakeholders relating to privacy at CCO. The Privacy Policy must identify where individuals may obtain further information in relation to its privacy policies, procedures, and practices.	19	✓	CCO's Privacy Policy; Statement of Information Practices; Privacy Inquiries and Complaints Procedure; Annual Privacy Report
	· Policy must make the following information available to the public and other stakeholders and must identify the means with which the information will be made available.	19	✓	CCO's Privacy Policy
	o Its Privacy Policy	19	✓	CCO's Privacy Policy; Privacy Inquiries and Complaints Procedure
	o Brochures or FAQs related to the privacy policies, procedures and practices implemented by CCO and the policy must set out the minimum content of the brochures or frequently asked questions. The brochures or FAQs must	19	✓	CCO's Privacy Policy; Privacy Inquiries and Complaints Procedure
	o Documentation related to the review by the IPC of the policies, procedures and practices implemented by CCO to protect the privacy and confidentiality of PHI received	19	✓	CCO's Privacy Policy; Privacy Inquiries and Complaints Procedure

	o A list of the data holdings of personal health information maintained by CCO	19	✓	CCO's Privacy Policy
	o contact information of an agent(s) where individuals may direct inquiries or complaints related to privacy	19	✓	CCO's Privacy Policy; Statement of Information Practices; Privacy Inquiries and Complaints Procedure
	· PIAs and summary of the PIAs conducted be made available	20	✓	CCO's Privacy Policy
	· brochures or frequently asked questions provide contact information where individuals may direct inquiries related to privacy	20	✓	CCO's Privacy Policy
	· the brochures or frequently asked questions must describe the status of CCO under the *Act,* the duties and responsibilities arising from this status, and the privacy policies, procedures, and practices implemented in respect of personal health information. The brochures or FAQs must set out some of the safeguards to to protect the privacy of individuals whose personal health information is received and to maintain the confidentiality of that information, including the steps taken to protect the personal health information against theft, loss, and unauthorized use or disclosure and to protect records of personal health information against unauthorized copying, modification, or disposal.	20	✓	CCO's Privacy Policy; Statement of Information Practices; Cancer Screening Privacy Frequently Asked Questions
	o The types of PHI collected and the persons or organizations from which this PHI is typically collected;	20	✓	CCO's Privacy Policy; Statement of Information Practices; Cancer Screening Privacy Frequently Asked Questions

	o The purposes for which PHI is collected;	20	✓	CCO's Privacy Policy; Statement of Information Practices; Cancer Screening Privacy Frequently Asked Questions
	o The purposes for which PHI is used, and if identifiable information is not routinely used, the nature of the information that is used;	20	✓	CCO's Privacy Policy; Statement of Information Practices; Cancer Screening Privacy Frequently Asked Questions
	o The circumstances in which and the purposes for which PHI is disclosed and the persons or organizations to which it is typically disclosed.	20	✓	CCO's Privacy Policy; Statement of Information Practices; Cancer Screening Privacy Frequently Asked Questions
	o The administrative, technical and physical safeguards implemented to protect the PHI it receives	20	✓	CCO's Privacy Policy; Statement of Information Practices; Cancer Screening Privacy Frequently Asked Questions
4	**Policy and Procedures for the collection of PHI**			
	· Must be developed and implemented to:	20		CCO's Privacy Policy
	o identify the purposes for which PHI will be collected by CCO	20	✓	CCO's Privacy Policy
	o the nature of the PHI that will be collected	20	✓	CCO's Privacy Policy
	o from whom the PHI will typically be collected	20	✓	CCO's Privacy Policy

	o the secure manner in which PHI will be collected.	20	✓	CCO's Privacy Policy
	· must articulate a commitment by CCO	20		CCO's Privacy Policy
	o not to collect PHI unless the collection is permitted by the *Act* and its regulation, if other information will serve the purpose.	20	✓	CCO's Privacy Policy
	o not to collect more PHI than is reasonably necessary to meet the purpose.	20	✓	CCO's Privacy Policy
	· require agents to comply with the policy and its procedures and stipulate compliance will be audited. Must indicate how and by whom compliance will be enforced and the frequency with which they will be audited and the agent responsible for conducting the audit and compliance. Policy must include the consequences of a breach of policy and that notification of a breach must be done at the first reasonable opportunity.	21	✓	Privacy Audit and Compliance Policy
	· notifying CCO if there may have been a breach of this policy or its procedures.	21	✓	Privacy Breach Management Policy; Privacy Breach Management Manual; Data Sharing Agreement Template

	· identify the agent(s) responsible for reviewing and determining whether to approve the collection of PHI, the process that must be followed and the requirements that must be satisfied	21	✓	Data Sharing Agreement Initiation Form; Data Sharing Agreement Initiation Procedure
	· set out the criteria that must be considered by the agent(s) responsible for determining whether to approve the collection of PHI	21	✓	Data Sharing Agreement Initiation Procedure
	· the criteria must require the agent(s) responsible for determining whether to approve the collection of PHI to ensure that: the collection is permitted by the Act and its regulation, other information, namely de-identified and/or aggregate information, will not serve the identified purpose, that only the minimum amount of PHI needed to fulfill the purpose is being collected, and that any and all conditions or restrictions set out in the Act and its regulation have been satisfied.	21	✓	Data Sharing Agreement Initiation Procedure
	· set out the manner in which the decision approving or denying the collection of PHI and the reasons for the decision are documented; the method by which and the format in which the decision will be communicated; and to whom the decision will be communicated.	21	✓	Information Management/Information Technology Stage - Gating Policy; Data Sharing Agreement Initiation Procedure
	· identify the conditions or restrictions that are required to be satisfied prior to the collection of PHI, including any documentation and/or agreements that must be completed, provided or executed, and the agent(s) or other persons or organizations, responsible for completing, providing or executing the documentation and/or agreements.	21	✓	Data Sharing Agreement Initiation Procedure

	· require that the records of PHI collected be retained in a secure manner	22	✓	Data Sharing Agreement Initiation Procedure
	· If the PHI is being collected by an agent of the prescribed person the policy and procedures shall require the records of personal health information to be transferred in a secure manner	22	✓	Data Sharing Agreement Initiation Procedure; CCO's Privacy Policy
	· identify the agent(s) responsible for ensuring that the records of PHI that have been collected are either securely returned or securely disposed of. If the records are to be disposed of, the policy and procedures must require them to be disposed of securely and in compliance with the Policies and Procedures for the Secure Disposal of Records of Personal Health Information.	22	✓	Data Sharing Agreement Initiation Procedure
	· If the records of PHI are to be returned to the person or organization from which they were collected, the policy and procedures must require the records to be transferred in a secure manner and in compliance with the Policy and Procedures for Secure Transfer of Records of Personal Health Information.	22	✓	Data Sharing Agreement Initiation Procedure
5	**List of data holding containing PHI**			
	· develop and retain an up-to-date list and brief description of the data holdings of PHI maintained by CCO	22	✓	CCO's Privacy Policy
6	**Policy and Procedures for statements of purpose for data holdings containing PHI**			
	· A policy and procedures must be developed and implemented with respect to the creation, review, amendment and approval of statements of purpose for data holdings containing PHI.	23	✓	CCO's Privacy Policy

	· Identify the persons and organizations that will be provided the statements of purpose	23	✓	CCO's Privacy Policy
	The policies and procedures must set out the process that must be followed in completing the statements of purpose for the data holdings containing PHI, including agent(s) or other persons that must be consulted in completing the statements of purpose and the agent(s) responsible for approving the statements of purpose	23	✓	CCO's Privacy Policy
	· The policy and procedures shall require the statements of purpose to set out:	23		
	o the purpose of the data holding,the PHI contained in the data holding, the source(s) of the PHI, the need for the PHI in relation to the identified purpose	23	✓	CCO's Privacy Policy
	· Identify the agent(s) responsible for completing the statements of purpose for the data holdings containing PHI	23	✓	CCO's Privacy Policy
	· Specify the role of the agent(s) that have been delegated day-to-day authority to manage the privacy program in respect of the statements of purpose	23	✓	CCO's Privacy Policy
	· The policy and procedures shall:	23		
	o require that the statements of purpose be reviewed on an ongoing basis and identify the frequency and requirments for reviewing the statements of purpose	23	✓	CCO's Privacy Policy
	· Document the agent(s) responsible and the process that must be followed in reviewing and amending the statements of purpose. This shall include:	23	✓	CCO's Privacy Policy

	o the agent(s) or other persons or organizations that must be consulted in reviewing, and if necessary, amending the statements of purpose	23	✓	CCO's Privacy Policy
	o the agent(s) responsible for approving the amended statements of purpose.	23	✓	CCO's Privacy Policy
	o identifying the persons and organizations that will be provided amended statements of purpose upon approval	23	✓	CCO's Privacy Policy
	· address how and by whom compliance will be enforced and the consequences of breach	23	✓	Privacy Audit and Compliance Policy
	· The policy and procedures must stipulate:	23		
	that CCO's agents must comply with the policy and procedures	23	✓	Privacy Audit and Compliance Policy; Privacy Breach Management Policy
	o that compliance will be audited in accordance with the *Policy and Procedures In Respect of Privacy Audits,* the frequency with which the policy and procedures will be audited and the agent(s) responsible for conducting the audit and for ensuring compliance with the policy and its procedures.	23	✓	Privacy Audit and Compliance Policy
	o the requirement of agents to notify CCO if a breach occurs	23	✓	Privacy Audit and Compliance Policy; CCO's Privacy Policy; Privacy Breach Management Policy
7	**Statements of purpose for data holding containing PHI**			
	· must draft a statement identifying:	24		

	o the purpose of the data holding, the personal health information contained in the data holding, the source(s) of the personal health information and the need for the personal health information in relation to the identified purpose	24	✓	CCO's Privacy Policy
8	**Policy and procedures for limiting agent access to and use of PHI**			
	· A policy and procedures must be developed and implemented to limit access and use of PHI by agents based on the "need to know" principle. The purpose of this policy and procedures is to ensure that agents of the prescribed person or prescribed entity access and use both the least identifiable information and the minimum amount of identifiable information necessary for carrying out their day-to-day employment, contractual or other responsibilities.	24	✓	CCO's Privacy Policy; Data Use & Disclosure Standard
	The policy and procedures must identify the limited and narrowly defined purposes for which and the circumstances in which agents are permitted to access and use personal health information and the levels of access to personal health information that may be granted. CCO must ensure that the duties of agents with access to personal health information are segregated in order to avoid a concentration of privileges that would enable a single agent to compromise personal health information.	24	✓	CCO's Privacy Policy; Data Use & Disclosure Standard

	For all other purposes and in all other circumstances, the policy and procedures must require agents to access and use de-identified and/or aggregate information, as defined in the *Policy and Procedures with Respect to De-identification and Aggregation.*		✓	CCO's Privacy Policy; Data Use & Disclosure Standard
	The policy and procedures must explicitly prohibit access to and use of personal health information if other information, such as de-identified and/or aggregate information, will serve the identified purpose and must prohibit access to or use of more personal health information than is reasonably necessary to meet the identified purpose.	24	✓	CCO's Privacy Policy; Data Use & Disclosure Standard
	The policy and procedures must also prohibit agents from using de-identified and/or aggregate information, either alone or with other information, to identify an individual. This includes attempting to decrypt information that is encrypted, attempting to identify an individual based on unencrypted information and attempting to identify an individual based on prior knowledge.	24	✓	Data Use & Disclosure Standard
	The agent(s) responsible and the process to be followed in receiving, reviewing and determining whether to approve or deny a request by an agent for access to and use of PHI shall be set out in the policy and procedures, along with the various level(s) of access that may be granted by CCO.	25	✓	Data Use & Disclosure Standard; Internal Data Access Policy; Internal Data Access Procedure

	· The Policy and procedures must set out the requirements to be satisfied in requesting, reviewing, and determining whether to approve or deny a request by an agent for access to and use of PHI. The documentation that must be completed, provided or executed, the agent responsible for completing, providing, or executing the documentation, the agent to whom it must be provided, and the required content.	25	✓	CCO's Privacy Policy; Data Use & Disclosure Standard; Internal Data Access Policy; Internal Data Access Procedure
	The policy and procedures must also set out the criteria that must be considered by the agent(s) responsible for determining whether to approve or deny a request by an agent for access to and use of PHI and, if the request is approved, the criteria that must be considered in determining the appropriate level of access. At a minimum, the agent(s) responsible for determining whether to approve or deny the request must be satisfied that:	25	✓	Data Use & Disclosure Standard; Internal Data Access Policy; Internal Data Access Procedure
	· The agent making the request routinely requires access to and use of PHI on an ongoing basis or for a specified period for his or her responsibilities;	25	✓	Data Use & Disclosure Standard; Internal Data Access Policy; Internal Data Access Procedure
	· The identified purpose for which access to and use of PHI is requested is permitted by the *Act* and its regulation;	25	✓	Data Use & Disclosure Standard; Internal Data Access Policy; Internal Data Access Procedure

	· The identified purpose for which access to and use of PHI is requested cannot be met with de-identified and/or aggregate data and can only reasonably be accomplished with PHI	25	✓	Data Use & Disclosure Standard; Internal Data Access Policy; Internal Data Access Procedure
	· In approving the request, no more PHI will be accessed and used than is reasonably necessary to meet the identified purpose.	25	✓	Data Use & Disclosure Standard; Internal Data Access Policy; Internal Data Access Procedure
	· The policy and procedures should also set out: the manner in which the decision approving or denying the request for access to and use of personal health information and the reasons for the decision are documented; the method by which and the format in which the decision will be communicated; to whom the decision will be communicated; any documentation that must be completed, provided and/or executed upon rendering the decision; the agent(s) responsible for completing, providing and/or executing the documentation; and the required content of the documentation.	25	✓	Data Use & Disclosure Standard; Internal Data Access Policy; Internal Data Access Procedure
	· The policy and procedures must identify the conditions or restrictions imposed on an agent granted approval to access and use personal health information, such as read, create, update or delete limitations, and the circumstances in which the conditions or restrictions will be imposed.	26	✓	Data Use & Disclosure Standard; Internal Data Access Policy; Internal Data Access Procedure

	· In the event that an agent only requires access to and use of personal health information for a specified period, the policy and procedures must set out the process to be followed in ensuring that access to and use of the personal health information is permitted only for that specified time period.	26	✓	Data Use & Disclosure Standard; Internal Data Access Policy; Internal Data Access Procedure
	· require an agent to notify CCO when the agent is no longer employed or retained by CCO	26	✓	Data Use & Disclosure Standard; Internal Data Access Policy; Internal Data Access Procedure; Employee Exit Process
	· an agent, as well as his or her supervisor, must notify CCO when the agent no longer requires access to or use of PHI	26	✓	Data Use & Disclosure Standard; Internal Data Access Policy; Internal Data Access Procedure; Employee Exit Process
	· procedure to be followed in providing the notification must also be identified and must include:	26		Data Use & Disclosure Standard; Internal Data Access Policy; Internal Data Access Procedure; Employee Exit Process

	· identifying the agent(s) to whom this notification must be provided, the time frame, the format of the notification, documentation that must be completed, provided and/or executed, the agent(s) responsible for completing, providing and/or executing the documentation, the agent(s) to whom the documentation must be provided, the required content of the documentation.	26	✓	Internal Data Access Procedure; Internal Data Access Policy; Employee Exit Process
	· within which this notification must be provided	26	✓	Data Use & Disclosure Standard; Internal Data Access Policy; Internal Data Access Procedure; Employee Exit Process
	· identify the agent(s) responsible for terminating access to and use of the PHI	26	✓	Data Use & Disclosure Standard; Internal Data Access Policy; Internal Data Access Procedure; Employee Exit Process
	· ensure that the procedures implemented in this regard are consistent with the Policy and Procedures for Termination or Cessation of the Employment or Contractual Relationship.	26	✓	Internal Data Access Procedure; Internal Data Access Policy; Employee Exit Process
	· require an agent granted approval to access and use PHI to securely retain the records of PHI	26	✓	CCO's Privacy Policy; Data Use & Disclosure Standard;
	· an agent granted approval to access and use PHI to securely dispose of the records of PHI	27	✓	CCO's Privacy Policy; Digital Media Disposal Standard; Digital

				Media Disposal Procedure
	· address where documentation related to the receipt, review, approval, denial or termination of access to and use of PHI is to be retained	27	✓	Internal Data Access Procedure
	· require that a log be maintained of agents granted approval to access and use PHI	27	✓	Internal Data Access Procedure; Log of Access Requests on the eCCO Data Access Request Tool
	· require agents to comply with the policy and its procedures and address how compliance will be enforced and the consequences of breach.	27	✓	Internal Data Access Procedure; Log of Access Requests on the eCCO Data Access Request Tool
	· regular audits of agents granted approval to access and use PHI must be conducted in accordance with the Policy and Procedures In Respect of Privacy Audits.	27	✓	Internal Data Access Procedure; Log of Access Requests on the eCCO Data Access Request Tool
	· identify the agent(s) responsible for conducting the audits and for ensuring compliance with the policy	27	✓	Internal Data Access Procedure; Log of Access Requests on the eCCO Data Access Request Tool
	· require agents to notify CCO if there may have been a breach of this policy or its procedures.	27	✓	Internal Data Access Procedure; Log of Access Requests on the eCCO Data Access Request Tool

9	**Log of agents granted approval to access and use of PHI**			
	· Must maintain a log of agents granted approval to access and use PHI. The log must: name the agent granted approval to access and use PHI,the data holdings of PHI the agent has been granted approval to access and use, the level or type of access and use granted, the date that access and use was granted, the termination date or the date of the next audit of access and use of PHI.	28	✓	CCO's Internal Direct Access Request on-line tool
10	**Policy and procedures for the use of PHI for research**			
	· A policy and procedures must be developed and implemented to identify whether and in what circumstances, if any, CCO permits PHI to be used for research purposes.		**N/A**	
	· entity must require agents to comply with the policy and its procedures		**N/A**	
	· Policy and procedures must stipulate:		**N/A**	
	o that compliance will be audited in accordance with the *Policy and Procedures In Respect of Privacy Audits*		**N/A**	
	o the frequency with which the policy and procedures will be audited		**N/A**	
	o the agent(s) responsible for conducting the audit and for ensuring compliance with the policy and its procedures.		**N/A**	
	o that agents are required to notify CCO if there may have been a breach		**N/A**	
	· sets out the circumstances in which PHI is permitted to be used for research purposes.		**N/A**	
	· set out the manner in which the decision approving or denying the request to use PHI for research purposes		**N/A**	

	· clearly distinguish between the use of PHI for research purposes and the use of PHI for purposes of subsection 39(1)(c) or section 45 of the *Act*, as the case may be.		**N/A**	
	· The policy and procedures must also identify the agent(s) responsible for:		**N/A**	
	o Receiving		**N/A**	
	o reviewing		**N/A**	
	o determining whether to approve or deny a request for the use of PHI for research purposes		**N/A**	
	o the process that must be followed. this shall include		**N/A**	
	§ a discussion of the documentation that must be completed, provided and/or executed;		**N/A**	
	§ the agent(s) responsible for completing, providing and/or executing the documentation;		**N/A**	
	§ the agent(s) to whom this documentation must be provided;		**N/A**	
	§ the required content of the documentation.		**N/A**	
	· address the requirements that must be satisfied and the criteria that must be considered when determining whether to approve the request to use PHI for research purposes.		**N/A**	
	o In identifying the requirements and criteria that must be satisfied the policy and procedures shall have regard to the *Act* and its regulation.		**N/A**	
	· require the agent(s) responsible for determining whether to approve or deny the request to review the written research plan to ensure:		**N/A**	
	o it complies with the requirements in the *Act* and its regulation		**N/A**	

	o that the written research plan has been approved by a research ethics board		**N/A**	
	o that CCO is in receipt of a copy of the decision of the research ethics board approving the written research plan.		**N/A**	
	· the agent(s) responsible for determining whether to approve or deny the request must be required to ensure:		**N/A**	
	o PHI being requested is consistent with the PHI identified in the written research plan approved by the research ethics board.		**N/A**	
	o that de-identified and/or aggregate information, will not serve the research purpose		**N/A**	
	· must identify the conditions or restrictions that will be imposed on the approval to use PHI for research purposes		**N/A**	
	o In determining the conditions or restrictions the policy and procedures shall have regard to the *Act* and its regulation.		**N/A**	
	· identify the agent(s) responsible for ensuring that any conditions or restrictions imposed on the use of PHI for research purposes are in fact being satisfied.		**N/A**	
	· require the agent granted approval to use PHI for research purposes to retain the records in compliance with the written research plan		**N/A**	
	· address whether an agent granted approval to use PHI for research purposes is required to securely return or dispose of the records of PHI		**N/A**	
	o If the records of PHI are required to be securely returned the policy and procedures must stipulate:		**N/A**	

	§ the time frame following the retention period		**N/A**	
	§ the secure manner in which the records must be returned		**N/A**	
	§ the agent to whom the records must be securely returned.		**N/A**	
	o If the records of PHI are required to be disposed of in a secure manner		**N/A**	
	o The policy and procedures must further stipulate:		**N/A**	
	§ the time frame following the retention period		**N/A**	
	§ must require a certificate of destruction to be provided		**N/A**	
	§ a certificate of destruction be provided to CCO		**N/A**	
	§ the time frame following secure disposal. The certificate of destruction confirming the secure disposal must be required to:		**N/A**	
	· identify the records of PHI securely disposed of		**N/A**	
	· the date, time and method of secure disposal employed		**N/A**	
	· signed confirmation of secure disposal.		**N/A**	
	· address where written research plans and other documentation related to requests for the use of PHI for research purposes will be retained		**N/A**	
	· If the prescribed person or prescribed entity does not permit personal health information to be used for research purposes, the policy and procedures must expressly prohibit the use of personal health information for research purposes and must indicate whether or not de-identified and/or aggregate information may be used for research purposes.	31	✓	Data Use & Disclosure Standard
	· The policy and procedures should also set out:		**N/A**	

	o the requirement that decisions approving or denying a request to use de-identified and/or aggregate information be documented		**N/A**	
	o method and the format of how the decision will be communicated		**N/A**	
	o to whom the decision will be communicated.		**N/A**	
	· If the records of PHI are required to be de-identified and retained by the agent the policy and procedures shall be compliant with the *Policy and Procedures With Respect to De-Identification and Aggregation*.		**N/A**	
	· identify the agent(s) responsible for ensuring that records of PHI used for research purposes are:		**N/A**	
	o securely returned, disposed of or de-identified		**N/A**	
	o the process to be followed when PHI records are not securely returned		**N/A**	
	· require that a log be maintained of the approved uses of PHI for research purposes		**N/A**	
	· identify if we do not permit PHI to be used for research purposes		**N/A**	
	· identify if we permit de-identified and/or aggregate information		**N/A**	
	o when deciding the use of de-identified and/or aggregate information for research purpose, the process that must be followed shall include:		**N/A**	
	· a discussion of the documentation that must be completed, provided and/or executed		**N/A**	
	· the agent(s) responsible for completing, providing and/or executing the documentation		**N/A**	

	· the agent(s) to whom this documentation must be provided		**N/A**	
	· the required content of the documentation.		**N/A**	
	· address the requirements and criteria that must be considered by the agent(s) when deciding on a request to use de-identified and/or aggregate information		**N/A**	
	· At a minimum, the policy and procedures must require:		**N/A**	
	o the de-identified and/or aggregate information to be reviewed to ensure that the information does not identify an individual		**N/A**	
	o the agent(s) responsible for undertaking this review be identified.		**N/A**	
	· identify the conditions or restrictions that will be imposed on using de-identified and/or aggregate information		**N/A**	
	· prohibit an agent using de-identified and/or aggregate information to identify an individual.		**N/A**	
11	**Log of approved uses of PHI for research**			

	· when permitting the use of PHI for research purposes we must maintain a log of the approved uses and at a minimum, include: the name of the research study, name of the agent(s) to whom the approval was granted, date of the decision of the research ethics board approving the written research plan, date that the approval to use PHI for research purposes was granted by CCO, date that the PHI was provided to the agent(s), nature of the PHI provided to the agent(s),retention period for the records of PHI identified in the written research plan approved by the research ethics board, whether the records of PHI will be securely returned, securely disposed of or de-identified and retained following the retention period, the date the records of PHI were securely returned or disposed of		**N/A**	
12	**Policy and procedures for disclosure of PHI for purposes other than research**			
	· identify whether and in what circumstances, if any, PHI is permitted to be disclosed for purposes other than research.	33	✓	Data Use & Disclosure Standard; Business Process for Data Requests; De-Identification Guidelines
	· articulate a commitment by CCO not to disclose PHI if other information will serve the purpose and require agents to comply with the policy and its procedures	33	✓	Data Use & Disclosure Standard
	· articulate a commitment by CCO not to disclose more PHI than is reasonably necessary to meeet the purpose.	33	✓	Data Use & Disclosure Standard
	· identify the agent(s) responsible for conducting the audit and for ensuring compliance with the policy and its procedures.	33	✓	Privacy Audit and Compliance Policy

	· must stipulate that compliance will be audited in accordance with the Policy and Procedures In Respect of Privacy Audits,	33	✓	Privacy Audit and Compliance Policy
	· must state the frequency with which the policy and procedures will be audited	33	✓	Data Sharing Agreement Template; Data Sharing Agreement Initiation Procedure; Internal Data Sharing Procedure
	· require agents to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach.	33	✓	Data Use & Disclosure Standard; Privacy Breach Management Policy; Internal Data Sharing Procedure; CCO's Privacy Policy
	· require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the Policy and Procedures for Privacy Breach Management, if an agent breaches or believes there may have been a breach of this policy or its procedures	33	✓	Data Use & Disclosure Standard; Privacy Breach Management Policy; Internal Data Sharing Procedure
	· require that all disclosures of personal health information comply with the Act and its regulation.	34	✓	Data Use & Disclosure Standard; Internal Data Sharing Procedure
	· set out the purposes when disclosure of PHI is permitted for purposes other than research.	34	✓	Business Process for Data Requests; Data Use & Disclosure Standard

	· set out the manner in which the decision made for requests are documented	34	✓	Business Process for Data Requests
	· address the requirements that must be satisfied and the criteria that must be considered by the agent(s) responsible for determining whether to approve the request for the disclosure of personal health information for purposes other than research. In identifying the requirements that must be satisfied and the criteria that must be considered, the policy and procedures shall have regard to the Act and its regulation	34	✓	Data Use & Disclosure Standard; Data Access Committee: Terms of Reference & Decision Criteria for CCO Data Requests; Internal Data Sharing Procedure
	· identify the agent(s) responsible for receiving, reviewing and determining whether to approve or deny a request for the disclosure of personal health information for purposes other than research and the process that must be followed in this regard. This shall include a discussion of the documentation that must be completed, provided and/or executed; the agent(s) or other persons or organizations responsible for completing, providing and/or executing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation.	34	✓	Business Process for Data Requests; Internal Data Sharing Procedure

	· the agent(s) responsible for determining whether to approve or deny the request for the disclosure of personal health information for purposes other than research must be required to ensure that the disclosure is permitted by the Act and its regulation and that any and all conditions or restrictions set out in the Act and its regulation have been satisfied. …The criteria must also require the agent(s) responsible for determining whether to approve or deny the request to ensure that other information, namely de-identified and/or aggregate information, will not serve the identified purpose of the disclosure and that no more personal health information is being requested than is reasonably necessary to meet the identified purpose.	34	✓	CCO's Privacy Policy; Data Use & Disclosure Standard; Internal Data Sharing Procedure
	· set out the manner in which the decision approving or denying the request for the disclosure of personal health information for purposes other than research and the reasons for the decision are documented; the method by which and the format in which the decision will be communicated; and to whom the decision will be communicated.	34	✓	Business Process for Data Requests; Internal Data Sharing Procedure
	· ensure that de-identified and/or aggregate information, will not serve the identified purpose of the disclosure	34	✓	De-Identification Guidelines
	· address where documentation related to the requests for the disclosure of PHI for purposes other than research will be retained	35	✓	Business Process for Data Requests
	· identify the conditions or restrictions required to be satisfied prior to the disclosure of PHI for purposes other than research	35	✓	Data Sharing Agreement Initiation Procedure; Business Process for Data Requests;

				Internal Data Sharing Procedure
	· require a Data Sharing Agreement to be executed in accordance with the Policy and Procedures for the Execution of Data Sharing Agreements and the Template Data Sharing Agreement prior to any disclosure of personal health information for purposes other than research.	35	✓	Data Sharing Agreement Standard; Data Sharing Agreement Initiation Procedure
	· identify the agent(s) responsible for ensuring that any conditions or restrictions that must be satisfied prior to the disclosure of PHI have been satisfied	35	✓	Data Sharing Agreement Initiation Procedure; Internal Data Sharing Procedure;
	· require records of PHI to be transferred in a secure manner	35	✓	Data Sharing Agreement Initiation Procedure; Internal Data Sharing Procedure;

	· identify the agent(s) responsible for ensuring that records of personal health information disclosed to a person or organization for purposes other than research are either securely returned or securely disposed of, as the case may be, following the retention period in the Data Sharing Agreement or the date of termination of the Data Sharing Agreement.	35	✓	Data Sharing Agreement Standard
	· address the process to be followed where records of personal health information are not securely returned or a certificate of destruction is not received within a reasonable period of time following the retention period in the Data Sharing Agreement or the date of termination of the Data Sharing Agreement. This shall include the agent(s) responsible for implementing this process and the stipulated time frame following the retention period or the date of termination within which this process must be implemented. (p. 35)	35	✓	Data Sharing Agreement Standard; Data Sharing Agreement Initiation Form
	· document the decision making process for the disclosure of de-identified and/or aggregate information	35	✓	Business Process for Data Requests; De-Identification Guidelines
	· If CCO does not permit PHI to be disclosed in these circumstances, the policy and procedures must expressly prohibit the disclosure of PHI for non-research purposes, except where required by law, and must indicate whether or not de-identified and/or aggregate information may be disclosed.	36	✓	N/A

	· the policy and procedures must identify the agent(s) responsible for deciding on a request for the disclosure of de-identified and/or aggregate information. This shall include: a discussion of the documentation that must be completed, provided and/or executed, the agent(s) or other persons or organizations responsible for completing, providing and/or executing the documentation, the agent(s) to whom this documentation must be provided, the required content of the documentation	36	✓	Business Process for Data Requests
	· address the requirements that must be satisfied and the criteria that must be considered by the agent(s) responsible for determining whether to approve or deny the request for the disclosure of de-identified and/or aggregate information for purposes other than research. At a minimum, the policy and procedures must require the de-identified and/or aggregate information to be reviewed prior to the disclosure of the de-identified and/or aggregate information in order to ensure that the information does not identify an individual and that it is not reasonably foreseeable in the circumstances that the information could be utilized, either alone or with other information, to identify an individual. The agent(s) responsible for undertaking this review shall also be identified. The policy and procedures should also set out the manner in which the decision approving or denying the request for the disclosure of de-identified and/or aggregate information for purposes other than research and the reasons for the decision are documented; the method	36	✓	Data Use & Disclosure Standard, Business Process for Data Requests, Data Access Committee: Terms of Reference & Decision Criteria for CCO Data Requests

	by which and the format in which the decision will be communicated; and to whom the decision will be communicated.			
	· identify the conditions or restrictions that are required to be satisfied prior to the disclosure of de-identified and/or aggregate information for non-research purposes, including any documentation and/or agreements that must be completed, provided or executed and the agent(s) responsible for completing, providing or executing the documentation and/or agreements	36	✓	Business Process for Data Requests; De-Identification Guidelines
	· require the person to acknowledge and agree, in writing not to use the de-identified information, either alone or with other information, to identify an individual. This includes attempting to decrypt information that is encrypted, attempting to identify an individual based on unencrypted information and attempting to identify an individual based on prior knowledge.	37	✓	Data Sharing Agreement Template
	· identify the agent(s) responsible for ensuring that any conditions or restrictions that must be satisfied prior to the disclosure of the de-identified and/or aggregate information have in fact been satisfied, including the execution of the written acknowledgement. Further, the policy and procedures shall require the responsible agent(s) to track receipt of the executed written acknowledgments and shall set out the procedure that must be followed and the documentation that must be maintained in this regard.	37	✓	Business Process for Data Requests
13	**Policy and procedures for disclosure of PHI for research purposes and the execution of research agreements**			

	· identify whether and in what circumstances, if any, CCO permits PHI to be disclosed for research purposes.	37	✓	Data Use & Disclosure Standard; Business Process for Data Requests
	· not disclosing PHI if other information will serve the research purpose and not disclosing more PHI than is reasonably necessary to meet the research purpose.	37	✓	Data Use & Disclosure Standard; Application for Disclosure of Information from CCO for Research Purposes
	· require agents to comply with the poicy and its procedures	37	✓	Data Use & Disclosure Standard
	· address how and by whom compliance will be enforced and the consequences of breach.	37	✓	Privacy Audit and Compliance Policy; Privacy Breach Management Manual; Privacy Breach Management Policy; Privacy Breach Report Form
	· stipulate that compliance will be audited in accordance with the *Policy and Procedures In Respect of Privacy Audits,* set out the frequency with which the policy will be audited and identify the agents responsible for conducting the audit and for ensuring compliance	37	✓	Privacy Audit and Compliance Policy

	· require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the Policy and Procedures for Privacy Breach Management, if an agent breaches or believes there may have been a breach of this policy or its procedures.	37	✓	Research Data Disclosure Agreement; Privacy Breach Management Policy; Privacy Breach Management Manual; Data Use & Disclosure Standard
	· set out the circumstances in which PHI is permitted to be disclosed for research purposes.	37	✓	Data Use & Disclosure Standard; Business Process for Data Requests
	· set out the manner in which the decision making process for the disclosure of PHI for research purposes are documented	38	✓	Decision Criteria for Data Requests
	· identify the agent(s) responsible for making a decision on a request for the disclosure of PHI for research purposes	38	✓	Business Process for Data Requests; Data Disclosure Subcommittee Terms of Reference
	o a discussion of the documentation that must be completed by agent(s) of CCO or by the researcher	38	✓	Business Process for Data Requests
	o the agent(s) to whom this documentation must be provided	38	✓	Business Process for Data Requests
	o the required content of the documentation.	38	✓	Business Process for Data Requests; Decision Criteria for Data Requests

	· address the requirements and criteria that must be considered by the agent(s) responsible for deciding on a the request for the disclosure of PHI	38	✓	Decision Criteria for Data Requests
	· prior to any approval of the disclosure of personal health information for research purposes, the policy and procedures must require the agent(s) responsible for determining whether to approve or deny the request to ensure that the prescribed person or prescribed entity is in receipt of a written application, a written research plan and a copy of the decision of the research ethics board approving the written research plan and that the written research plan complies with the requirements in the Act and its regulation.	38	✓	Data Use & Disclosure Standard; Business Process for Data Requests
	· ensure that the PHI being requested is consistent with the PHI identified in the written research plan	38	✓	Application for Disclosure of Information from CCO for Research Purposes; Research Data Disclosure Agreement
	· ensure that de-identified and/or aggregate information, will not serve the research purpose and no more PHI is being requested than is reasonably necessary to meet the research purpose.	38	✓	Data Use & Disclosure Standard; Application for Disclosure of Information from CCO for Research Purposes; Research Data Disclosure Agreement
	· address where documentation relating to making a decision on the requests for the disclosure of PHI for research purposes will be retained	38	✓	Business Process for Data Requests

	· set out the method by which and the format in which the decision will be communicated; and to whom the decision will be communicated.	38	✓	Business Process for Data Requests
	· identify the conditions or restrictions that are required to be satisfied prior to the disclosure of personal health information for research purposes, including any documentation and/or agreements that must be completed, provided or executed and the agent(s) or researcher responsible for completing, providing or executing the documentation and/or agreements. At a minimum, the policy and procedures must require that a Research Agreement be executed in accordance with the Template Research Agreement prior to the disclosure of personal health information for research purposes.	38	✓	Data Use & Disclosure Standard; Research Data Disclosure Agreement; Business Process for Data Requests
	· identify the agent(s) responsible for ensuring that any conditions or restrictions that must be satisfied prior to the disclosure of personal health information for research purposes have in fact been satisfied, including the execution of a Research Agreement.	39	✓	Business Process for Data Requests
	· PHI is transferred in a secure manner in compliance with the *Policy and Procedures for Secure Transfer of Records of Personal Health Information*.	39	✓	Application for Disclosure of Information from CCO for Research Purposes; Research Data Disclosure Agreement
	· PHI disclosed to a researcher are either securely returned, disposed of or de-identified following the retention period	39	✓	Application for Disclosure of Information from CCO for Research Purposes; Research Data

				Disclosure Agreement
	· address the process to be followed by the responsible agent(s) where records of PHI are not securely returned, a certificate of destruction is not received or written confirmation of de-identification is not received	39	✓	Business Process for Data Requests
	· If CCO does not permit PHI to be disclosed for research purposes, the policy and procedures must expressly prohibit the disclosure of PHI for research purposes	39	N/A	
	· If CCO permits de-identified and/or aggregate information to be disclosed the policy and procedures must identify the agent(s) responsible for receiving, reviewing and determining whether to approve or deny a request for the disclosure, as well as the process that must be followed in this regard. This shall include:	39	✓	Business Process for Data Requests; Data Disclosure Subcommittee Terms of Reference
	o a discussion of the documentation that must be completed, provided and/or executed by agent(s) of CCO or by the researcher	39	✓	Business Process for Data Requests
	o the agent(s) to whom this documentation must be provided	39	✓	Business Process for Data Requests
	o the required content of the documentation.	39	✓	Business Process for Data Requests
	· address whether CCO requires the preparation of a written research plan in accordance with the Act and its regulation and/or requires research	40	✓	Business Process for Data Requests; Decision Criteria for Data Requests

	ethics board approval of the written research plan prior to the disclosure of de-identified and/or aggregate information for research purposes			
	· address the requirements and the criteria that must be considered by the agent(s) responsible for deciding on a request for the disclosure of de-identified and/or aggregate information	40	✓	Business Process for Data Requests; Decision Criteria for Data Requests
	· require the de-identified and/or aggregate information to be reviewed and identify the conditions or restrictions that are required to be satisfied prior to disclosure in order to ensure it does not identify an individual and that it is not reasonably foreseeable in the circumstances that the information could be utilized, either alone or with other information, to identify an individual. The agent(s) responsible for undertaking this review shall also be identified.	40	✓	Business Process for Data Requests; De-Identification Guidelines
	Set out the manner in which the decision approving or denying the request for disclosure of de-identified and/or aggregate information for research purposes and the reasons for the decision are documented; the method by which and the format in which the decision will be communicated; and to whom the decision will be communicated.	40	✓	Business Process for Data Requests
	The policy and procedures must also identify the conditions or restrictions that are required to be satisfied prior to the disclosure of de-identified and/or aggregate information for research purposes, including any documentation and/or agreements that must be completed, provided or executed and the agent(s) or researcher responsible for completing, providing or executing the documentation and/or agreements.	40	✓	Business Process for Data Requests

	At a minimum, the prescribed person or prescribed entity must require the researcher to whom the de-identified and/or aggregate information will be disclosed to acknowledge and agree, in writing, that the researcher will not use the de-identified and/or aggregate information, either alone or with other information, to identify an individual. This includes attempting to decrypt information that is encrypted, attempting to identify an individual based on unencrypted information and attempting to identify an individual based on prior knowledge.	40	✓	Research Data Disclosure Agreement
	The policy and procedures must also identify the agent(s) responsible for ensuring that any conditions or restrictions that must be satisfied prior to the disclosure of the de-identified and/or aggregate information have in fact been satisfied, including the execution of the written acknowledgement. Further, the policy and procedures shall require the responsible agent(s) to track receipt of the executed written acknowledgements and shall set out the procedure that must be followed and the documentation that must be maintained in this regard.	40	✓	Business Process for Data Requests
14	**Template research agreements**			
	· A Research Agreement must be executed with the researchers to whom personal health information will be disclosed prior to the disclosure of the personal health information for research purposes.	41	✓	Research Data Disclosure Agreement Business Process for Data Requests
	· the research agreement must:			

	· describe the status of CCO under the *Act*	41	✓	Application for Disclosure of Information from CCO for Research Purposes; Research Data Disclosure Agreement
	· specify the nature of the PHI that will be disclosed	41	✓	Application for Disclosure of Information from CCO for Research Purposes;
	· provide a definition of personal health information that is consistent with the Act and its regulation.	41	✓	Research Data Disclosure Agreement
	· identify the research purpose for which the PHI is being disclosed	41	✓	Application for Disclosure of Information from CCO for Research Purposes; Research Data Disclosure Agreement
	· identify the statutory authority for each collection, use and disclosure identified.	41	✓	Application for Disclosure of Information from CCO for Research Purposes; Research Data Disclosure Agreement

	· only permit the researcher to use the personal health information for the purposes set out in the written research plan approved by the research ethics board and must prohibit the use of the personal health information for any other purpose.	41	✓	Research Data Disclosure Agreement
	· prohibit the researcher from permitting persons to access and use the PHI except those persons described in the written research plan	41	✓	Application for Disclosure of Information from CCO for Research Purposes; Research Data Disclosure Agreement
	· explicitly state whether or not the personal health information may be linked to other information and must prohibit the personal health information from being linked except in accordance with the written research plan approved by the research ethics board.	41	✓	Application for Disclosure of Information from CCO for Research Purposes; Research Data Disclosure Agreement
	· require the researcher to acknowledge that the personal health information that is being disclosed pursuant to the Research Agreement is necessary for the identified research purpose and that other information, namely de-identified and/or aggregate information, will not serve the research purpose.	41	✓	Research Data Disclosure Agreement
	· researcher must acknowledge that no more PHI is being collected and will be used than is reasonably necessary to meet the research purpose.	41	✓	Application for Disclosure of Information from CCO for Research Purposes

	· impose restrictions on the disclosure of PHI requiring the researcher to: agree not to disclose PHI except as required by law, not to publish the PHI in a form that could reasonably enable a person to ascertain the identity of the individual, not to make contact or attempt to make contact with the individual to whom the PHI relates, unless the consent of the individual to being contacted is first obtained in accordance with subsection 44(6) of the Act.	41	✓	Research Data Disclosure Agreement
	· require the researcher and the prescribed person or prescribed entity to acknowledge and agree that the researcher has submitted an application in writing, a written research plan that meets the requirements of the Act and its regulation, and a copy of the decision of the research ethics board approving the written research plan.	42	✓	Research Data Disclosure Agreement
	· the researcher will comply with the Research Agreement and with the written research plan	42	✓	Application for Disclosure of Information from CCO for Research Purposes; Research Data Disclosure Agreement

	· require the secure transfer of records of personal health information that will be disclosed pursuant to the Research Agreement. The Research Agreement shall set out the secure manner in which records of personal health information will be transferred, including under what conditions and to whom the records will be transferred, and the procedure that will be followed in ensuring that the records of personal health information are transferred in a secure manner. In identifying the secure manner in which the records of personal health information will be transferred, the Research Agreement shall have regard to the Policy and Procedures for Secure Transfer of Records of Personal Health Information implemented by the prescribed person or prescribed entity.	42	✓	Business Process for Data Requests; Research Data Disclosure Agreement; Secure Transfer of Personal Health Information Policy; Secure Transfer of Personal Health Information Standard
	· The retention period for the records of personal health information subject to the Research Agreement must also be identified, including the length of time that the records of personal health information will be retained in identifiable form. The retention period identified must be consistent with that set out in the written research plan approved by the research ethics board.	42	✓	Application for Disclosure of Information from CCO for Research Purposes; Research Data Disclosure Agreement

	· require the researcher to ensure that the records of personal health information are retained in a secure manner and shall identify the precise manner in which the records of personal health information in paper and electronic format will be securely retained.	42	✓	Application for Disclosure of Information from CCO for Research Purposes
	· In identifying the secure manner in which the records of PHI will be retained, the Research Agreement shall have regard to the written research plan	42	✓	Application for Disclosure of Information from CCO for Research Purposes; Research Data Disclosure Agreement
	· require the researcher to take steps that are reasonable in the circumstances to ensure that the personal health information subject to the Research Agreement is protected against theft, loss and unauthorized use or disclosure and to ensure that the records of personal health information subject to the Research Agreement are protected against unauthorized copying, modification or disposal. The reasonable steps that are required to be taken by the researcher must be detailed in the Research Agreement and, at a minimum, shall include those set out in the written research plan approved by the research ethics board	42	✓	Research Data Disclosure Agreement

	· address whether the records of personal health information subject to the Research Agreement will be returned in a secure manner, will be disposed of in a secure manner or will be de-identified and retained by the researcher following the retention period set out in the Research Agreement. In this regard, the provisions in the Research Agreement shall be consistent with the written research plan approved by the research ethics board.	43	✓	Research Data Disclosure Agreement; Application for Disclosure of Information from CCO for Research Purposes
	· In identifying the secure manner in which the records of PHI will be disposed of regard may be had to the Policy and Procedures for Secure Disposal of Records of Personal Health Information	43	✓	Application for Disclosure of Information from CCO for Research Purposes; Research Data Disclosure Agreement
	· If the records of personal health information are required to be returned in a secure manner, the Research Agreement must stipulate the time frame following the retention period within which the records must be securely returned, the secure manner in which the records must be returned and the agent of the prescribed person or prescribed entity to whom the records must be securely returned. …In identifying the secure manner in which the records of personal health information will be returned, regard may be had to the Policy and Procedures for Secure Transfer of Records of Personal Health Information implemented by the prescribed person or prescribed entity.	43	✓	Application for Disclosure of Information from CCO for Research Purposes; Secure Transfer of Personal Health Information Policy; Secure Transfer of Personal Health Information Standard.

	· If the records of personal health information are required to be disposed of in a secure manner, the Research Agreement must provide a definition of secure disposal that is consistent with the Act and its regulation and must identify the precise manner in which the records of personal health information subject to the Research Agreement must be securely disposed of. The Research Agreement must also stipulate the time frame following the retention period set out in the Research Agreement within which the records of personal health information must be securely disposed of and within which a certificate of destruction must be provided.	43	✓	Application for Disclosure of Information from CCO for Research Purposes; Research Data Disclosure Agreement
	· In identifying the secure manner in which the records of personal health information will be disposed of, it must be ensured that the method of secure disposal identified is consistent with the Act and its regulation; with orders issued by the Information and Privacy Commissioner of Ontario under the Act and its regulation, including Order HO-001 and Order HO-006; and with guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner of Ontario pursuant to the Act and its regulation, including Fact Sheet 10: Secure Destruction of Personal Information. In addition, regard may be had to the Policy and Procedures for Secure Disposal of Records of Personal Health Information implemented by the prescribed person or prescribed entity.	43	✓	Application for Disclosure of Information from CCO for Research Purposes; Research Data Disclosure Agreement

	· identify the agent of the prescribed person or prescribed entity to whom the certificate of destruction must be provided, the time frame following secure disposal within which the certificate of destruction must be provided and the required content of the certificate of destruction.	43	✓	Research Data Disclosure Agreement; Data and Record Destruction Certificate
	· the certificate of destruction must be required to identify the records of personal health information securely disposed of; to stipulate the date, time, location and method of secure disposal employed; and to bear the name and signature of the person who performed the secure disposal.	44	✓	Data and Record Destruction Certificate
	· If the records of personal health information are required to be de-identified and retained by the researcher rather than being securely returned or disposed of, the manner and process for de-identification must be set out in the Research Agreement. In identifying the manner and process for de-identification, regard may be had to the Policy and Procedures with Respect to De-Identification and Aggregation implemented by the prescribed person or prescribed entity. The Research Agreement must also require the researcher to submit written confirmation that the records were de-identified and shall stipulate the time frame following the retention period set out in the Research	44	N/A	Application for Disclosure of Information from CCO for Research Purposes; De-Identification Guidelines

	Agreement within which the written confirmation must be provided and the agent of the prescribed person or prescribed entity to whom the written confirmation must be provided.			
	· identify the agent of CCO to whom notification must be provided in the event of a breach	44	✓	Research Data Disclosure Agreement
	· require the researcher to notify the prescribed person or prescribed entity immediately, in writing, if the researcher becomes aware of a breach or suspected breach of the Research Agreement, a breach or suspected of subsection 44(6) of the Act or if personal health information subject to the Research Agreement is stolen, lost or accessed by unauthorized persons or is believed to have been stolen, lost or accessed by unauthorized persons. The Research Agreement should also identify the agent of the prescribed person or prescribed entity to whom notification must be provided and must require the researcher to take steps that are reasonable in the circumstances to contain the breach and to contain the theft, loss or access by unauthorized persons.	44	✓	Research Data Disclosure Agreement
	· outline the consequences of breach of the agreement and must indicate whether compliance with the Research Agreement will be audited by the prescribed person or prescribed entity and, if so, the manner in which compliance will be audited and the notice, if any, that will be provided of the audit.	44	✓	Research Data Disclosure Agreement; Privacy Audit and Compliance Policy

	· require the researcher to ensure that all persons who will have access to the personal health information, as identified in the written research plan approved by the research ethics board, are aware of and agree to comply with the terms and conditions of the Research Agreement prior to being given access to the personal health information. The Research Agreement must set out the method by which this will be ensured by the researcher, such as requiring the persons identified in the written research plan to sign an acknowledgement prior to being granted access, indicating that they are aware of and agree to comply with the terms and conditions of the Research Agreement.	44	✓	Research Data Disclosure Agreement
15	**Log of research agreements**			
	· maintain a log of executed Research Agreements. Log must include: the name of the research study, name of the principal researcher to whom the PHI was disclosed pursuant to the Research Agreement, date(s) of receipt of the written application, the written research plan and the written decision of the research ethics board approving the research plan, date that the approval to disclose the PHI for research purposes was granted by the prescribed person or prescribed entity, date that the Research Agreement was executed, date that the PHI was disclosed, nature of the PHI disclosed, retention period for the records of PHI, whether the records of PHI will be securely returned, disposed of or de-identified and retained by the researcher following the retention period, date that the records of PHI were securely	45	✓	Log of Research Agreements

	returned or a certificate of destruction was received			
	· the log must include the date that the records of personal health information were securely returned, a certificate of destruction was received or written confirmation of de-identification was received or the date by which they must be returned, disposed of or de-identified.	45	✓	Business Process for Data Requests
16	**Policy and procedure for the execution of data sharing agreements**			
	A policy and procedures must be developed and implemented to identify the circumstances requiring the execution of a Data Sharing Agreement and the process that must be followed and the requirements that must be satisfied prior to the execution of a Data Sharing Agreement.	45	✓	Data Sharing Agreement Initiation Procedure; Data Sharing Agreement Standard
	· set out the circumstances requiring the execution of a Data Sharing Agreement prior to the collection of personal health information for purposes other than research and must require the execution of a Data Sharing Agreement prior to any disclosure of personal health information for purposes other than research.	45	✓	Data Sharing Agreement Initiation Procedure; Data Sharing Agreement Standard

	· identify the agent(s) responsible for ensuring that a Data Sharing Agreement is executed, as well as the process that must be followed and the requirements that must be satisfied in this regard. This shall include a discussion of the documentation that must be completed, provided and/or executed; the agent(s) or other persons or organizations responsible for completing, providing and/or executing the documentation; the agent(s) to whom the documentation must be provided; and the required content of the documentation.	45	✓	Data Sharing Agreement Initiation Procedure; Data Sharing Agreement Initiation Form
	· the agents responsible for ensuring that a DSA is executed must be satisfied that the collection was approvd in accordance with the Policy and Procedures for the Collection of PHI	46	✓	Data Sharing Agreement Initiation Procedure
	· approving the disclosure of PHI for purposes other than research, must be in accordance with the Policy and Procedures for Disclosure of Personal Health Information For Purposes Other Than Research.	46	✓	Data Sharing Agreement Initiation Procedure
	· require that a log of Data Sharing Agreements be maintained and must identify the agent(s) responsible for maintaining such a log.	46	✓	Data Sharing Agreement Initiation Procedure
	· require agents to comply with the policy and its procedures and address how compliance will be enforced	46	✓	Data Sharing Agreement Initiation Procedure

	· stipulate that compliance will be audited in accordance with the Policy and Procedures In Respect of Privacy Audits, must set out the frequency with which the policy and procedures will be audited and must identify the agent(s) responsible for conducting the audit and for ensuring compliance with the policy and its procedures.	46	✓	Data Sharing Agreement Initiation Procedure; Data Sharing Agreement Standard
	· require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the Policy and Procedures for Privacy Breach Management, if an agent breaches or believes there may have been a breach of this policy or its procedures.	46	✓	Data Sharing Agreement Initiation Procedure; Data Sharing Agreement Standard; Privacy Breach Management Policy; Privacy Breach Management Manual
17	**Template data sharing agreements**			
	· ensure that a Data Sharing Agreement is executed in the circumstances set out in the Policy and Procedures for the Execution of Data Sharing Agreements	46	✓	Data Sharing Agreement Initiation Procedure
	· describe the status of CCO under the Act	46	✓	Data Sharing Agreement Template
	· specify the precise nature of the PHI subject to the Data Sharing Agreement	46	✓	Data Sharing Agreement Template
	· provide a definition of PHI that is consistent with the Act and its regulation	46	✓	Data Sharing Agreement Template
	· identify the person or organization that is collecting, or disclosing PHI pursuant to the Data Sharing Agreement	47	✓	Data Sharing Agreement Template

	· identify the purposes for which the PHI is being collected and how it will be used.	47	✓	Data Sharing Agreement Template
	· state whether or not the PHI collected will be linked to other information	47	✓	Data Sharing Agreement Template
	· If PHI will be linked to other information the DSA must identify the nature of the information to which the PHI will be linked, the source of information to which the PHI will be linked, how the linkage will be conducted and why the linkage is required for the identified purpose	47	✓	Data Sharing Agreement Initiation Procedure; Data Sharing Agreement Template
	· contain an acknowledgement that the personal health information collected pursuant to the Data Sharing Agreement is necessary for the purpose for which it was collected and that other information, namely de-identified and/or aggregate information, will not serve the purpose and that no more personal health information is being collected and will be used than is reasonably necessary to meet the purpose.	47	✓	Data Sharing Agreement Initiation Procedure; CCO's Privacy Policy; Data Sharing Agreement Template
	· identify the purposes for which the PHI subject to the Data Sharing Agreement may be disclosed	47	✓	Data Sharing Agreement Template
	· require the collection, use and disclosure of PHI to comply with the Act and its regulation and set out the specific statutory authority for each collection, use and disclosure contemplated in the Data Sharing Agreement.	47	✓	Data Sharing Agreement Template

	· require the secure transfer of the records of personal health information subject to the Data Sharing Agreement. The Data Sharing Agreement shall set out the secure manner in which the records of personal health information will be transferred, including under what conditions and to whom the records will be transferred, and the procedure that must be followed in ensuring that the records are transferred in a secure manner. In identifying the secure manner in which the records of personal health information will be transferred, regard may be had to the Policy and Procedures for Secure Transfer of Records of Personal Health Information implemented by the prescribed person or prescribed entity.	47	✓	Data Sharing Agreement Initiation Procedure; CCO's Privacy Policy; Data Sharing Agreement Template; Secure Transfer of Personal Health Information Policy; Secure Transfer of Personal Health Information Standard;
	· require the records of personal health information to be retained in a secure manner and shall identify the precise manner in which the records of personal health information in paper and electronic format will be securely retained, including whether the records will be retained in identifiable form. In identifying the secure manner in which the records of personal health information will be retained, the Data Sharing Agreement may have regard to the Policy and Procedures for Secure Retention of Records of Personal Health Information implemented by the prescribed person or prescribed entity.	48	✓	Data Sharing Agreement Initiation Procedure; Retention of Records Containing Personal Health Information Policy; CCO's Privacy Policy; Data Sharing Agreement Initiation Form; Data Sharing Agreement Template
	· in identifying the relevent retention period, it must be ensured that the records of PHI are retained only for as long as necessary to fulfill the purposes for which the records of PHI were collected	48	✓	Data Sharing Agreement Template

	· require reasonable steps to be taken to ensure that the personal health information subject to the Data Sharing Agreement is protected against theft, loss and unauthorized use or disclosure and to ensure that the records of personal health information are protected against unauthorized copying, modification or disposal. The reasonable steps that are required to be taken shall also be detailed in the Data Sharing Agreement.	48	✓	Data Sharing Agreement Initiation Procedure; CCO's Privacy Policy; Data Sharing Agreement Template
	· address whether the records of PHI will be returned or disposed of in a secure manner	48	✓	Data Sharing Agreement Template
	· If the records of personal health information are required to be returned in a secure manner, the Data Sharing Agreement must stipulate the time frame following the retention period or following the date of termination of the Data Sharing Agreement within which the records of personal health information must be securely returned, the secure manner in which the records must be returned and the person to whom the records must be securely returned. In identifying the secure manner in which the records of personal health information will be returned, regard may be had to the Policy and Procedures for Secure Transfer of Records of Personal Health Information implemented by the prescribed person or prescribed entity.	48	✓	Data Sharing Agreement Initiation Procedure; Secure Transfer of Personal Health Information Policy; Secure Transfer of Personal Health Information Standard; CCO's Privacy Policy; Data Sharing Agreement Template

	· If the records of personal health information are required to be disposed of in a secure manner, the Data Sharing Agreement must provide a definition of secure disposal that is consistent with the Act and its regulation and must identify the precise manner in which the records of personal health information subject to the Data Sharing Agreement must be securely disposed of. The Data Sharing Agreement must also stipulate the time frame following the retention period or following the date of termination of the Data Sharing Agreement within which the records of personal health information must be securely disposed of and within which a certificate of destruction must be provided.	48	✓	Data Sharing Agreement Initiation Procedure; CCO's Privacy Policy; Data Sharing Agreement Template
	· in identifying the secure manner in which the records of PHI will be disposed of, it must be ensured that the method of secure disposal is conistent with orders issued by the IPC under the Act and its regulation (ie. Order HO-001 and HO-006), with guidelines, fact sheets and best practices issued by the IPC (ie Fact Sheet 10: Secure Destruction of Personal Information).	49	✓	Data Sharing Agreement Initiation Procedure; Data Sharing Agreement Template

	· require that notification be provided at the first reasonable opportunity if the Data Sharing Agreement has been breached or is suspected to have been breached or if the personal health information subject to the Data Sharing Agreement is stolen, lost or accessed by unauthorized persons or is believed to have been stolen, lost or accessed by unauthorized persons. It should also identify whether the notification must be verbal and/or in writing and to whom the notification must be provided. The Data Sharing Agreement must also require that reasonable steps be taken to contain the breach of the Data Sharing Agreement and to contain the theft, loss or access by unauthorized persons.	49	✓	Data Sharing Agreement Initiation Procedure; CCO's Privacy Policy; Data Sharing Agreement Template
	· the secure manner of disposal must be consistent with the Act	49	✓	Data Sharing Agreement Template
	· the Data Sharing Agreement, in relation to secure disposal, must: identify the person to whom the certificate of destruction must be provided, the time frame following secure disposal within which the certificate of destruction must be provided, the required content of the certificate of destruction	49	✓	Data Sharing Agreement Template
	· outline the consequences of breach of the agreement	49	✓	Data Sharing Agreement Initiation Procedure; Privacy Breach Management Policy; Data Sharing Agreement Template

	· indicate whether compliance with the Data Sharing Agreement will be audited and, if so, the manner in which compliance will be audited and the notice, if any, that will be provided of the audit.	49	✓	Data Sharing Agreement Initiation Procedure; Data Sharing Agreement Standard; Privacy Audit and Compliance Policy
	· require that all persons who will have access to the personal health information are aware of and agree to comply with the terms and conditions of the Data Sharing Agreement prior to being given access to the personal health information. The Data Sharing Agreement must set out the method by which this will be ensured. This may include requiring the persons that will have access to the personal health information to sign an acknowledgement, prior to being granted access, indicating that they are aware of and agree to comply with the terms and conditions of the Data Sharing Agreement.	49	✓	Data Sharing Agreement Standard; Data Sharing Agreement Template
18	**Log of data sharing agreements**			
	· maintain a log of executed Data Sharing Agreements. The log must include: the name of the person or organization from whom the PHI was collected or to whom the PHI was disclosed, date that the collection or disclosure of PHI was approved, date that the Data Sharing Agreement was executed, date the PHI was collected or disclosed, nature of the PHI subject to the DSA, retention period for the records of PHI, whether the records of PHI will be securely returned or disposed of, date the records of PHI were securely returned or a certificate of destruction	50	✓	CCO's Privacy Policy; Log of Data Sharing Agreements

19	**Policy and procedures for executing agreements with third party service providers in respect of PHI**			
	· written agreements must be entered into with third party service providers, containing language from the Template Agreement for Third Party Service Providers, prior to permitting third party service providers to access and use the PHI of CCO	50	✓	CCO's Privacy Policy; Data Use & Disclosure Standard ; Digital PHI Handling Standard; Digital PHI Handling Procedure
	· identify the agents responsible for ensuring that and agreement is executed, as well as the process that must be followed and the requirements that must be satisfied prior to the execution of such an agreement.	50	✓	Data Use & Disclosure Standard; CCO Procurement Policy
	· state that CCO shall not provide PHI to a third party service provider if de-identified and/or aggregate information will serve the purpose, and will not provide more PHI than is reasonably necessary to meet the purpose	50	✓	Data Use & Disclosure Standard
	· identify the agent responsible for making the determination of whether de-identified/aggregate information will serve the purpose, and that no more information is provided than is reasonably necessary to meet the purpose	51	✓	Privacy Inquiries and Complaints Procedure
	· identify the agent(s) responsible for ensuring that records of PHI provided to a third party are securely returned or disposed of following termination of the agreement	51	✓	Template Schedule for Third Party Agreements
	· address the process to be followed where records of PHI are not securely returned or a certificate of destruction is not received following the termination of the agreement, including the agent responsible for implementation and time frame	51	✓	Template Schedule for Third Party Agreements

	following termination within which process must be implemented.			
	· a log be maintained of all agreements executed with third parties, and identify the agent responsible for maintaining such a log	51	✓	Procurement Documentation and Records Management Procedure
	· require agents to comply with the policy and its procedures	51	✓	Data Use & Disclosure Standard
	· address how and by whom compliance will be enforced and the consequences of breach.		✓	Data Use & Disclosure Standard; Privacy Audit and Compliance Policy; Privacy Breach Management Manual; Privacy Breach Management Policy
	· stipulate that compliance will be audited, set out the frequency with which the policy and procedures will be audited and identify the agents responsible for conducing the audit and ensuring compliance	51	✓	Data Use & Disclosure Standard; Privacy Audit and Compliance Policy
	· require agents to notify CCO if an agent believes there may have been a breach of this policy or its procedures.	51	✓	Privacy Breach Management Manual; Privacy Breach Management Policy;
20	**Template agreement for all third party service providers**			
	· A written agreement must be entered into with third party service providers that will be permitted to access and use PHI of CCO.	52	✓	Template Schedule for Third Party Agreements; Consulting Agreement - Template

	· provide a definition of PHI consistent with the *Act* and its regulation.	52	✓	Template Schedule for Third Party Agreements; Consulting Agreement - Template
	· Where appropriate, specify the precise nature of the PHI that the third party will be permitted to access and use	52	✓	Template Schedule for Third Party Agreements; Consulting Agreement - Template
	· describe the status of CCO under the Act	52	✓	Template Schedule for Third Party Agreements; Consulting Agreement - Template
	· All third party service providers that are permitted to access and use PHI shall be considered agents of CCO with the possible exception of electronic service providers.	52	✓	Template Schedule for Third Party Agreements; Consulting Agreement - Template
	· Agreements with electronic service providers shall explicitly state whether or not the third party service provider is an agent of CCO (prescribed person or prescribed entity) in providing services pursuant to the agreement.	52	✓	Template Schedule for Third Party Agreements; Consulting Agreement - Template
	· if third party is an agent the agreement must require the third party service provider to comply with the provisions of the Act and its regulation, and to comply with CCO's privacy and security policies	52	✓	Template Schedule for Third Party Agreements; Consulting Agreement - Template
	· services provided by the third party must be performed in a professional manner	52	✓	Template Schedule for Third Party Agreements; Consulting Agreement - Template

	· identify the purposes for which the third party is permitted to access and use PHI, and any limitation, conditions or restrictions theron	52	✓	Template Schedule for Third Party Agreements; Consulting Agreement - Template
	· ensure that each use identified in the agreement is consistent with the uses of PHI permitted by the Act and its regulation.	52	✓	Template Schedule for Third Party Agreements; Consulting Agreement - Template
	· prohibit third party from collecting, using or disclosing PHI except as permitted in the Agreement	52	✓	Template Schedule for Third Party Agreements; Consulting Agreement - Template
	· in the case of an electronic service provider that is not an agent of CCO the agreement must explicitly prohibit the electronic service provider from using PHI except as necessary in the course of providing services pursuant to the agreement.	52	N/A	
	· prohibit the third party from using PHI if other information will serve the purpose, and from using more PHI than is necessary to serve the purpose	53	✓	Template Schedule for Third Party Agreements; Consulting Agreement - Template
	· identify the purposes for which the third party is permitted to disclose the PHI of CCO, and any limitation, conditions or restrictions imposed thereon	53	✓	Template Schedule for Third Party Agreements; Consulting Agreement - Template
	· ensure that each disclosure identified in the agreement is consistent with the disclosures of PHI permitted by the Act and its regulation.	53	✓	Template Schedule for Third Party Agreements; Consulting Agreement - Template

	· the agreement must prohibit the third party from disclosing PHI if other information will serve the purpose, and from disclosing more PHI than is reasonably necessary to serve the purpose	53	✓	Template Schedule for Third Party Agreements; Consulting Agreement - Template
	· In the case of an electronic service provider that is not an agent of CCO the agreement must prohibit the electronic service provider from disclosing PHI to which it has access	53	N/A	
	· require the third party to securely transfer the records of PHI, and set out the responsibilities of the third party in this regard	53	✓	Template Schedule for Third Party Agreements
	· the agreement must have regard to the Policy and Procedures for Secure Transfer of Records of Personal Health Information	53	✓	Template Schedule for Third Party Agreements
	· where the retention or disposal of records of PHI outside the premises of CCO is the primary service provided to CCO, the agreement shall require the third party to provide documentation setting out the date, time and mode of transfer of the records of PHI	53	✓	Template Schedule for Third Party Agreements
	· require the third party to retain the records of PHI in a secure manner, in accordance with secure retention policies	54	✓	Template Schedule for Third Party Agreements
	· outline the responsibilities of the third party in securely retaining the records of PHI	54	✓	Template Schedule for Third Party Agreements

	· where the retention of records of PHI is the primary service provided to CCO by the third party the agreement must obligate the third party to maintain a detailed inventory of the records of PHI being retained on behalf of CCO	54	✓	Template Schedule for Third Party Agreements
	· address whether records of PHI will be securely returned or disposed of in a secure manner	54	✓	Template Schedule for Third Party Agreements
	· If the records of PHI are required to be returned in a secure manner, the agreement must stipulate the time frame and the secure manner in which the records must be returned	54	✓	Template Schedule for Third Party Agreements
	If the records of PHI are required to be returned, the Agreement must stipulate the agent of CCO to whom the records must be securely returned.		N/A, provisions will be added to body of agreement as required	
	· If the records of PHI are required to be disposed of the agreement must provide a definition of secure disposal consistent with the Act and its regulation	54	✓	Template Schedule for Third Party Agreements
	· the agreement must identify the precise manner in which the records of PHI are to be securely disposed of.	54	✓	Template Schedule for Third Party Agreements

	· enable CCO to witness the secure disposal of the records of PHI	55	✓	Template Schedule for Third Party Agreements
	· ensure the method of secure disposal is consistent with the Act and regulation	55	✓	Template Schedule for Third Party Agreements
	· in identifying the secure manner in which the records of PHI will be disposed of, it must be ensured that the method of secure disposal is consistent with orders issued by the IPC (ie. Order HO-001 and HO-006); and with guidelines, fact sheets and best practices issued by the IPC (ie. Fact Sheet 10: Secure Destruction of Personal Information and the Policy and Procedures for Secure Disposal of Records of PHI).	55	✓	Template Schedule for Third Party Agreements
	· stipulate the time frame the records of PHI must be securely disposed of and when a certificate of destruction must be provided to CCO	55	✓	Template Schedule for Third Party Agreements
	· the agreement, in terms of secure disposal, must set out:	55		
	· the agent of CCO to whom the certificate of destruction must be provided	55	N/A, provisions will be added to body of agreement as required	

	· the required content of the certificate of destruction	55	✓	Template Schedule for Third Party Agreements; Consulting Agreement - Template
	· certificate of destruction must:	55		
	· identify the records of PHI securely disposed of	55	✓	Template Schedule for Third Party Agreements; Consulting Agreement - Template
	· to stipulate the date, time and method of secure disposal employed	55	✓	Template Schedule for Third Party Agreements; Consulting Agreement - Template
	· bear the name and signature of the person who performed the secure disposal.	55	✓	Template Schedule for Third Party Agreements; Consulting Agreement - Template
	· Where the disposal of records of PHI is the primary service provided to CCO by the third party the agreement must set out the responsibilities of the third party including:	55		
	· The time frame within which the records are required to be securely disposed of	55	N/A, provisions will be added to body of agreement as required	

	· The precise method by which records must be securely disposed of	55	N/A, provisions will be added to body of agreement as required	
	· The conditions pursuant to which the records will be securely disposed of	55	N/A, provisions will be added to body of agreement as required	
	· The person(s) responsible for ensuring the secure disposal of the records.	55	N/A, provisions will be added to body of agreement as required	

	· require the third party service provider to take steps that are reasonable in the circumstances to ensure that PHI accessed and used is protected against theft, loss, unauthorized use or disclosure, and to ensure that the records are proected against unauthorized copying, modification or disposal, and detail the reasonable steps the third party must take in this regard.	55	✓	Template Schedule for Third Party Agreements; Consulting Agreement - Template
	· identify whether the notification of a breach, by the third party must be verbal or written and to whom the notification must be provided.	56	✓	Template Schedule for Third Party Agreements; Consulting Agreement - Template
	· require the third party to provide training to its agents on the importance of protecting PHI and the consequnces of breach	56	✓	Template Schedule for Third Party Agreements
	· require the third party to ensure that its agents who will have access to the records of PHI agree to comply with the terms and conditions of the agreement prior to being given access PHI, and set out the method by which this will be ensured	56	✓	Template Schedule for Third Party Agreements
	· In the event that the agreement permits the third party to subcontract the services, the third party must provide CCO with advance notice of its intention to do so, and require third party to enter into agreement with subcontractor consistent wtih obligations to CCO, and provide CCO with copy of such agreement	56	✓	Template Schedule for Third Party Agreements; Consulting Agreement - Template

	· require the third party to notify CCO if there has been a breach of the PHI or agreement, and identify whether notification verbal, written or both	56	✓	Template Schedule for Third Party Agreements; Consulting Agreement - Template
	· identify to whom the notification must be provided	56	✓	Template Schedule for Third Party Agreements; Consulting Agreement - Template
	· The third party must also be required to take steps that are reasonable in the circumstances to contain the breach	56	✓	Template Schedule for Third Party Agreements; Consulting Agreement - Template
	· outline the consequences of breach of the agreement	56-57	✓	Template Schedule for Third Party Agreements; Consulting Agreement - Template
	· Indicate whether CCO will be auditing compliance with the agreement, and If so, specify the precise manner in which compliance will be audited and the notice, if any, thatwill be provided to the third party of the audit	57	✓	Template Schedule for Third Party Agreements
21	**Log of agreements with third party service providers**			
	· maintain a log of executed agreements with third party service providers. The log must include:	57		
	· The name of the third party service provider	57	✓	Contract Management System; Log of Third Party Service Providers with Access to PHI

	· The nature of the services provided that require access and use of PHI	57	✓	Contract Management System; Log of Third Party Service Providers with Access to PHI
	· The date that the agreement was executed	57	✓	Contract Management System; Log of Third Party Service Providers with Access to PHI
	· The date that the records of PHI or access was provided	57	✓	Contract Management System; Log of Third Party Service Providers with Access to PHI
	· The nature of the PHI provided or to which access provided	57	✓	Contract Management System; Log of Third Party Service Providers with Access to PHI
	· The date of termination of the agreement	57	✓	Contract Management System; Log of Third Party Service Providers with Access to PHI
	· Whether the records of PHI will be securely returned or disposed of following termination of agreement	57	✓	Contract Management System; Log of Third Party Service Providers with Access to PHI

	· The date the records of PHI were securely returned or a certificate of destruction was provided, or the date that access to the PHI was terminated or the date by which the above must occur	57	✓	Contract Management System; Log of Third Party Service Providers with Access to PHI
22	**Policy and procedures for the linkage of records of PHI**			
	· A policy and procedures must be developed and implemented with respect to linkages of records of personal health information.	57	✓	Data Linkage Policy; Data Linkage Procedure
	· identify whether or not CCO permits the linkage of records of PHI and if it is not permitted, the policy and procedures must expressly prohibit the linkage of records of PHI	57	✓	Data Linkage Policy; Data Linkage Procedure
	· if linkages are permitted the circumstances in which such linkages are permitted must be identified	57	✓	Data Linkage Policy; Data Linkage Procedure
	· The policy and procedures should also set out:	58		
	· the manner in which the decision approving or denying the request to link records of PHI and reasons for the decision are documented	58	✓	Data Linkage Policy; Data Linkage Procedure
	· the method and format and to whom the decision will be communicated	58	✓	Data Linkage Policy; Data Linkage Procedure
	· In identifying the purposes and the circumstances in which the linkage of records of PHI is permitted, regard must be had to the sources of the records of PHI that are requested to be linked and the identity of the person or organization that will ultimately make use of the linked records of PHI, including:	58	✓	Data Linkage Policy; Data Linkage Procedure

	· The linkage of records of PHI in the custody of CCO for the exclusive use by CCO	58	✓	Data Linkage Policy; Data Linkage Procedure
	· The linkage of records of PHI in the custody of CCO with records of PHI collected from another person or organization for the exclusive use by CCO	58	✓	Data Linkage Policy; Data Linkage Procedure
	· The linkage of records of PHI in the custody of CCO for purposes of disclosure to another person or organzization	58	✓	Data Linkage Policy; Data Linkage Procedure
	· The linkage of records of PHI the custody of CCO with records of PHI collected from another person or organization for the purposes of disclosure to another person or organization	58	✓	Data Linkage Policy; Data Linkage Procedure
	· identify the agent(s) determining the approval or denial of the request to link records of PHI	58	✓	Data Linkage Policy; Data Linkage Procedure
	· address the requirements that must be satisfied and the criteria that must be considered by the agent(s) responsible for determining whether to approve or deny the request	58	✓	Data Linkage Policy; Data Linkage Procedure
	· Where the linked records of PHI will be disclosed by the CCO to another person or organization, the policy and procedures must require that the disclosure be approved pursuant (as may be applicible) to:	59	✓	Data Linkage Policy; Data Linkage Procedure
	· Policy and Procedures for Disclosure of Personal Health Information for Research Purposes.	59	✓	Data Linkage Policy
	· Execution of Research Agreements	59	✓	Data Linkage Policy
	· Policy and Procedures for Disclosure of Personal Health Information For Purposes Other Than Research	59	✓	Data Linkage Policy

	· Where the linked records of PHI will be used by CCO, the policy and procedures must require that the use be approved pursuant (as may be applicable) to:	59	✓	Data Linkage Policy
	· Policy and Procedures for the Use of Personal Health Information for Research	59	N/A	
	· Policy and Procedures for Limiting Agent Access to and Use of Personal Health Information,	59	✓	Data Linkage Policy
	· require that the linked records of PHI be de-identified and/or aggregated	59	✓	Data Linkage Policy; Data Linkage Procedure
	· outline the process to be followed in linking records of PHI	59	✓	Data Linkage Policy; Data Linkage Procedure
	· require that linked records of PHI be retained	59	✓	Data Linkage Policy; Data Linkage Procedure
	· address the secure disposal of records of PHI linked by CCO	59	✓	Data Linkage Policy; Data Linkage Procedure
	· require agents to comply with the policy and its procedures and address how and by whom compliance will be enforced and the consequences of breach	59	✓	Privacy Breach Management Policy; Privacy Breach Management Manual
	· stipulate that compliance will be audited	59	✓	Privacy Audit and Compliance Policy
	· require agents to notify CCO if an agent believes there may have been a breach of this policy or its procedures.	60	✓	Privacy Breach Management Manual; Privacy Breach Management Policy

	· require that a log be maintained of the linkages of records of PHI approved by CCO and identify the agent(s) responsible for maintaining such a log.	60	✓	Data Linkage Policy; Data Linkage Procedure; List of Data Linkages
23	**Log of approved linkages of records of PHI**			
	· maintain a log of linkages of records of PHI approved by the CCO. The log must include: name of the agent, person or organization who requested the linkage, date that the linkage of records of PHI was approved, nature of the records of PHI linked	60	✓	List of Data Linkages
24	**Policy and procedures with respect to de-identification and aggregation**			
	· A policy and procedures must be developed and implemented with respect to de-identification and aggregation	60	✓	CCO's Privacy Policy; Data Use & Disclosure Standard; De-Identification Guidelines
	· Policy requires that PHI will not be used if other information, namely de-identified and / or aggregate information, will serve the identified purpose	60	✓	CCO's Privacy Policy; Data Use & Disclosure Standard
	· cell-sizes of less than five and the exceptions thereto must be articulated. In articulating the policy with respect to cell-sizes of less than five, regard must be had to the restrictions related to cell-sizes of less than five	60	✓	Data Use & Disclosure Standard; De-Identification Guidelines
	· provide a definition of de-identified information and aggregate information	60	✓	Data Use & Disclosure Standard; De-Identification Guidelines
	· the definition of de-identified information and aggregate information and the policy with respect to cell-sizes of less than five must have regard to, and must be consistent with, the meaning of	60	✓	Data Use & Disclosure Standard; De-Identification Guidelines

	"identifying information" in subsection 4(2) of the Act			
	· identify the information that must be removed, encrypted and/or truncated in order to constitute de-identified information	61	✓	De-Identification Guidelines
	· address the agent(s) responsible for de-identifying and/or aggregating information and the procedure to be followed in this regard.	61	✓	Business Process for Data Requests
	· require de-identified and/or aggregate information of cell sizes less than five to be reviewed prior to use or disclosure in order to ensure that it is not reasonably forseeable in the circumstances that the information could be used, either alone or with other information, to identify an an individual	61	✓	Business Process for Data Requests; Decision Criteria for Data Requests; Data Use & Disclosure Standard
	· set out the process to be followed in reviewing the de-identified and/or aggregate information and the criteria to be used in assessing the risk of re-identification	61	✓	De-Identification Guidelines
	· In establishing the criteria CCO shall have regard to the type of identifying information available, including information that can be used to identify an individual directly (e.g., name, address, health card number) or indirectly (e.g., date-of-birth, postal code, gender).	61	✓	De-Identification Guidelines
	· prohibit agents from using de-identified and/or aggregate information, including information in cell-sizes of less than five, to identify an individual	61	✓	Privacy & Security Acknowledgement Form; Business process for Data Requests

	· identify the mechanisms implemented to ensure that de-identified and/or aggregate information will not identify an individual	61	✓	Business Process for Data Requests; De-Identification Guidelines
	· require agents to comply with the policy and its procedures and address how and by whom compliance will be enforced and the consequences of breach.	61	✓	Privacy Audit and Compliance Policy
	· stipulate that compliance will be audited	61	✓	Privacy Audit and Compliance Policy
	· require agents to notify CCO if an agent believes there may have been a breach of this policy or its procedures.	61	✓	Privacy Breach Management Policy; Privacy Breach Management Manual
25	**PIA policy and procedures**			
	· A policy and procedures must be developed and implemented to identify the circumstances in which privacy impact assessments are required to be conducted.	62	✓	CCO's Privacy Policy; Privacy Impact Assessment Standard
	· ensure that CCO conducts PIAs on existing and proposed data holdings involving PHI	62	✓	Privacy Impact Assessment Standard
	· PIAs must be conducted whenever a new or a change to an existing information system, technology, or program involving PHI is contemplated	62	✓	Privacy Impact Assessment Standard
	· If there are limited and specific circumstances in which PIAs are not required to be conducted on existing and proposed data holdings involving PHI and whenever a new or a change to an existing information system, technology or program involving PHI is contemplated, these shall be outlined in the policy and procedures along with a rationale for why PIAs are not required.	62	✓	Privacy Impact Assessment Standard

	· identify the agent(s) responsible for making this determination and must require the determination and the reasons for the determination to be documented	62	✓	Privacy Impact Assessment Standard
	· address the timing of PIAs	62	✓	Privacy Impact Assessment Standard
	· With respect to proposed data holdings involving PHI and new or changes to existing information systems, technologies or programs involving PHI, the policy and procedures must require that PIAs be conducted at the conceptual design stage and that they be reviewed and amended, if necessary, during the detailed design and implementation stage.	62	✓	Privacy Impact Assessment Standard
	· With respect to existing data holdings involving PHI, the policy and procedures must require that a timetable be developed to ensure PIAs are conducted and the policy and procedures must identify the agent(s) responsible for developing the timetable.	62	✓	Privacy Impact Assessment Standard
	· Once PIAs have been completed the policy and procedures shall require that they be reviewed on an ongoing basis in order to ensure that they continue to be accurate and continue to be consistent with the information practices of the prescribed person or prescribed entity.	62	✓	Privacy Impact Assessment Standard
	The policy and procedures must also identify the circumstances in which and the frequency with which PIAs are required to be reviewed.	62	✓	Privacy Impact Assessment Standard

	· The policy and procedures must also identify the agent(s) responsible and the process that must be followed: - in identifying when PIAs are required; - in identifying when PIAs are required to be reviewed in accordance with the policy and procedures; and - in ensuring that PIAs are conducted and completed; and in ensuring that PIAs are reviewed and amended, if necessary.	62	✓	Privacy Impact Assessment Standard
	· Identify the role of agent(s) that have been delegated day-to-day authority to manage the privacy program and security program in respect to PIAs	63	✓	Privacy Impact Assessment Standard
	· stipulate the required content of a PIA. The PIA at a minimum must be required to describe:	63		Privacy Impact Assessment Standard
	· The data holding, information system, technology or program at issue;	63	✓	Privacy Impact Assessment Standard
	· The nature and type of PHI collected, used or disclosed or that is proposed to be collected used or disclosed	63	✓	Privacy Impact Assessment Standard
	· The sources of the PHI;	63	✓	Privacy Impact Assessment Standard
	· The purposes for which the PHI is collected, used or disclosed or is proposed to be collected, used of disclosed.	63	✓	Privacy Impact Assessment Standard
	· The reason that the PHI is required for the purposes identified;	63	✓	Privacy Impact Assessment Standard
	· The flows of the PHI	63	✓	Privacy Impact Assessment Standard

	· The statutory authority for each collection, use and disclosure of PHI identified;	63	✓	Privacy Impact Assessment Standard
	· The limitations imposed on the collection, use and disclosure of the PHI	63	✓	Privacy Impact Assessment Standard
	· Whether or not the PHI is or will be linked to other information;	63	✓	Privacy Impact Assessment Standard
	· The retention period for the records of PHI	63	✓	Privacy Impact Assessment Standard
	· The secure manner in which the records of PHI are or will be retained, transferred and disposed of;	63	✓	Privacy Impact Assessment Standard
	· The functionality for logging access, use, modification and disclosure of the PHI	63	✓	Privacy Impact Assessment Standard
	· the functionality to audit logs for unauthorized use or disclosure;		✓	Privacy Impact Assessment Standard
	· The risks to the privacy of individuals whose PHI is or will be part of the data holding, information system, technology or program and an assessment of those risks;	63	✓	Privacy Impact Assessment Standard
	· Recommendations to address and eliminate or reduce the privacy risks	63	✓	Privacy Impact Assessment Standard
	· The administrative, technical and physical safeguards implemented or proposed to be implemented to protect the PHI	63	✓	Privacy Impact Assessment Standard
	· outline the process for addressing the recommendations arising from PIAs, including the agent(s) responsible for assigning other agent(s) to address the recommendations for establishing timelines to address the recommendations, for addressing the recommendations and for monitoring and ensuring the implementation of	64	✓	Privacy Impact Assessment Standard; Privacy and Information Security Risk Management Procedure

	the recommendations, is also required to be outlined.			
	· require that a log be maintained of privacy impact assessments~~:~~ that have been completed, that have been undertaken but that have not been completed, that have not been undertaken, identify the agent(s) responsible for maintaining such a log.	64	✓	Privacy Impact Assessment Standard; Log of Privacy Impact Assessments
	· must require agents to comply with the policy and its procedures and address how and by whom compliance will be enforced and the consequences of a breach.	64	✓	Privacy Impact Assessment Standard; Privacy Audit and Compliance Policy
	· The policy and procedures must also stipulate that compliance will be audited in accordance with the Policy and Procedures In Respect of Privacy Audits, must set out the frequency with which the policy and procedures will be audited and must identify the agent (s) responsible for conducting the audit and ensuring compliance.	64	✓	Privacy Audit and Compliance Policy
	· must also require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the Policy and Procedures for Privacy Breach Management, if an agent breaches or believes there may have been a breach of this policy or its procedures.	64	✓	Privacy Impact Assessment Standard; Breach Management Manual; Privacy Breach Management Policy
	· In developing the policy and procedures, it is recommended regard be had to the *Privacy Impact Assessment Guidelines for the Ontario Personal Health Information Protection Act*, published by the Information and Privacy Commissioner of Ontario.	64	✓	Privacy Impact Assessment Standard
26	**Log of PIAs**			

	· maintain a log of PIAs that have been completed and of PIAs that have been undertaken but that have not been completed. The log shall describe:	64	✓	Log of Privacy Impact Assessments
	· the data holding, information system, technology or program involving PHI	64	✓	Log of Privacy Impact Assessments
	· the date that the PIA was completed or is expected to be completed	64	✓	Log of Privacy Impact Assessments
	· the agent(s) responsible for completing or ensuring the completion of the PIA	64	✓	Log of Privacy Impact Assessments
	· the recommendations arising from the PIA	64	✓	Log of Privacy Impact Assessments
	· the agent(s) responsible for addressing each recommendation, the date that each recommendation was or is expected to be addressed	64	✓	Log of Privacy Impact Assessments
	· the manner in which each recommendation was or is expected to be addressed.	64	✓	Log of Privacy Impact Assessments
	· maintain a log of data holdings involving PHI and of new or changes to existing information systems, technologies or programs involving PHI for which PIAs have not been undertaken	64	✓	Log of Privacy Impact Assessments
	· For each data holding, information system, technology or program, the log shall either set out the reason that a PIA will not be undertaken and the agents responsible for making this determination or set out the date that the PIA is expected to be completed and the agents responsible for completing the PIA	64-65	✓	Log of Privacy Impact Assessments
27	**Policy and procedures in respect of privacy audits**			

	· A policy and procedures must be developed and implemented that sets out the types of privacy audits that are required to be conducted	65	✓	CCO's Privacy Policy; Privacy Audit and Compliance Policy
	· At a minimum, the audits required to be conducted shall include audits to assess compliance with the privacy policies, procedures and practices implemented by CCO	65	✓	Privacy Audit and Compliance Policy
	· At a minimum, the audits required to be conducted shall include audits to assess compliance with the privacy policies, procedure must include audits of the agent(s) permitted to access and use PHI pursuant to the *Policy and Procedures for Limiting Agent Access and Use of PHI*	65	✓	Privacy Audit and Compliance Policy
	· With respect to each privacy audit that is required to be conducted, the policy and procedures must: - set out the purposes of the privacy audit, - the nature and scope of the privacy audit (i.e. document reviews, interviews, site visits, inspections), - the agent(s) responsible for conducting the privacy audit and; - the frequency with which and the circumstances in which each privacy audit is required to be conducted.	65	✓	Privacy Audit and Compliance Policy
	· Require a privacy audit schedule to be developed and shall identify the agent(s) responsible for developing the privacy audit schedule	65	✓	Privacy Audit and Compliance Policy

	· For each type of privacy audit that is required to be conducted, the policy and procedures shall also set out the process and that must be completed to conduct the audit. This is to include the criteria that must be considered in selecting the subject matter of the audit and whether or not notification will be provided of the audit, and if so, the nature and content of the notification and to whom the notification must be provided.	65	✓	Privacy Audit and Compliance Policy
	· The policy and procedures must further discuss the documentation that must be completed, provided and/or executed in undertaking each privacy audit; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation.	65	✓	Privacy Audit and Compliance Policy
	· The role of the agent(s) that have been delegated day-to-day authority to manage the privacy and security program	65	✓	Privacy Audit and Compliance Policy
	· process that must be followed in addressing the recommendations arising from privacy audits, including the agent(s) responsible for assigning other agent(s) to address the recommendations, for establishing timelines to address the recommendations, for addressing the recommendations and for monitoring and ensuring the implementation of the recommendations.	65	✓	Privacy Audit and Compliance Policy

	· documentation must be completed, provided and/or executed at the conclusion of the privacy audit, including the agent(s) responsible for completing, providing and/or executing the documentation, the agent(s) to whom the documentation must be provided and the required content of the documentation.	65	✓	Privacy Audit and Compliance Policy
	· address the manner and format in which the findings of privacy audits, including the recommendations arising from the privacy audits and the status of addressing the recommendations are communicated. This shall include a discussion of the agent(s) responsible for communicating the findings of the privacy audit; the mechanism and format for communicating the findings of the privacy audit; the time frame within which the findings of the privacy audit must be communicated; and to whom the findings of the privacy audit will be communicated, including the Chief Executive Officer or the Executive Director.	66	✓	Privacy Audit and Compliance Policy
	· require that a log be maintained of privacy audits and identify the agent(s) responsible for maintaining the log and for tracking that the recommendations arising from the privacy audits are addressed within the identified time frame. They should further address where documentation related to privacy audits will be retained and the agent(s) responsible for retaining this documentation.	66	✓	Privacy Audit and Compliance Policy; Privacy Risk Register

	· require the agent(s) responsible for conducting the privacy audit to notify CCO of a privacy breach at the first reasonable opportunity, of a privacy breach or suspected privacy breach in accordance with the Policy and Procedures for Privacy Breach Management and of an information security breach or suspected information security breach in accordance with the Policy and Procedures for Information Security Breach Management.	66	✓	Privacy Audit and Compliance Policy
28	**Log of privacy audits**			
	· maintain a log of privacy audits that have been completed.	66	✓	Privacy Audit and Compliance Policy; Privacy Risk Register
	· The log will set out: the nature and type of the privacy audit conducted, the date that the privacy audit was completed, the agent(s) responsible for completing the privacy audit, recommendations arising from the privacy audit, the agent(s) responsible for addressing each recommendation, the date that each recommendation was or is expected to be addressed, the manner in which each recommendation was or is expected to be addressed.	66	✓	Privacy Audit and Compliance Policy; Privacy Risk Register
29	**Policy and procedures for privacy breach management**			
	· A policy and procedures must be developed and implemented to address the identification, reporting, containment, notification, investigation and remediation of privacy breaches	66	✓	CCO's Privacy Policy; Privacy Breach Management Manual; Privacy Breach Management Policy;
	· The policy and procedures must provide a definition of the term “privacy breach.” At a minimum, a privacy breach shall be defined to include:	66	✓	CCO's Privacy Policy; Privacy Breach Management Manual; Privacy

				Breach Management Policy
	· The collection, use and disclosure of PHI that is not in compliance with the Act or its regulation;	66	✓	Privacy Breach Management Manual; Privacy Breach Management Policy
	· A contravention of the privacy policies, procedures or practices implemented by CCO;	66	✓	Privacy Breach Management Manual; Privacy Breach Management Policy
	· A contravention of Data Sharing Agreements, Research Agreements, Confidentiality Agreements and Agreements with Third Party Service Providers retained by CCO;	67	✓	Privacy Breach Management Manual; Privacy Breach Management Policy
	· Circumstances where PHI is stolen, lost or subject to unauthorized use or disclosure or where records of personal health information are subject to unauthorized copying, modification or disposal.	67	✓	Privacy Breach Management Manual; Privacy Breach Management Policy
	· impose a mandatory requirement on agents to notify CCO of a privacy breach or suspected privacy breach	67	✓	Privacy Breach Management Manual; Privacy Breach Management Policy
	· identify the agent(s) who must be notified of the privacy breach or suspected privacy breach and shall provide contact information for the agent(s) who must be notified.	67	✓	Privacy Breach Management Manual; Privacy Breach Management Policy

	· stipulate the time frame within which notification must be provided, whether the notification must be provided verbally and/or in writing and the nature of the information that must be provided upon notification.	67	✓	Privacy Breach Management Manual; Privacy Breach Management Policy
	The policy and procedures shall also address the documentation that must be completed, provided and/or executed with respect to notification; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation.	67	✓	Privacy Breach Management Manual; Privacy Breach Management Policy
	· require a determination to be made of whether a privacy breach has in fact occurred and if so, what, if any, PHI has been breached. The agent(s) responsible for making this determination must also be identified.	67	✓	Privacy Breach Management Manual; Privacy Breach Management Policy; Privacy Breach Report Form
	· address when senior management, including the Chief Executive Officer or the Executive Director, will be notified. This shall include a discussion of the agent(s) responsible for notifying senior management; the time frame within which notification must be provided; the manner in which this notification must be provided; and the nature of the information that must be provided to senior management upon notification.	67	✓	Privacy Breach Management Manual; Privacy Breach Management Policy

	· The policy and procedures shall also require that containment be initiated immediately and shall identify the agent(s) responsible for containment and the procedure that must be followed in this regard, including any documentation that must be completed, provided and/or executed by the agent(s) responsible for containing the breach and the required content of the documentation.	67	✓	Privacy Breach Management Manual; Privacy Breach Management Policy
	· ensure that reasonable steps are taken in the circumstances to protect PHI from further theft, loss or unauthorized use or disclosure and to protect records of personal health information from further unauthorized copying, modification or disposal. At a minimum, these steps shall include ensuring that no copies of the records of personal health information have been made and ensuring that the records of personal health information are either retrieved or disposed of in a secure manner. Where the records of personal health information are securely disposed of, written confirmation should be obtained related to the date, time and method of secure disposal. These steps shall also include ensuring that additional privacy breaches cannot occur through the same means and determining whether the privacy breach would allow unauthorized access to any other information and, if necessary, taking further action to prevent additional privacy breaches.	67	✓	Privacy Breach Management Manual; Privacy Breach Management Policy

	· The agent(s) responsible and the process to be followed in reviewing the containment measures implemented and determining whether the privacy breach has been effectively contained or whether further containment measures are necessary, must be identified in the policy and procedures. The policy and procedures shall also address the documentation that must be completed, provided and/or executed by the agent(s) responsible for reviewing the containment measures; the agent(s) to whom this documentation must be provided; and the required content of the documentation.	68	✓	Privacy Breach Management Manual; Privacy Breach Management Policy
	· require the HIC or other organization that disclosed the PHI to CCO to be notified at the first reasonable opportunity whenever PHI is or is believed to be stolen, lost or accessed by unauthorized persons and whenever required pursuant to the agreement with the HIC or other organization.	68	✓	Privacy Breach Management Manual; Privacy Breach Management Policy
	The policy and procedure shall set:			
	· set out the agent(s) responsible for notifying the HIC or other organization	68	✓	Privacy Breach Management Manual; Privacy Breach Management Policy
	· the format of the notification	68	✓	Privacy Breach Management Manual; Privacy Breach Management Policy
	· the nature of the information that must be provided upon notification	68	✓	Privacy Breach Management Manual; Privacy Breach

				Management Policy
	At a minimum, the policy and procedures must require the HIC or other organization to be advised of the extent of the privacy breach, the nature of the PHI at issue, the measures implemented to contain the privacy breach and further actions that will be undertaken with respect to the privacy breach, including investigation and remediation.	68	✓	Privacy Breach Management Manual; Privacy Breach Management Policy
	As a secondary collector of PHI, a prescribed person or prescribed entity should not directly notify the individual to whom the PHI relates of a privacy breach. The required notification shall be provided by the HIC.	68	✓	Privacy Breach Management Manual; Privacy Breach Management Policy
	· set out whether any other persons or organizations must be notified of the privacy breach and shall set out the agent(s) responsible for notifying these other persons or organizations, the format of the notification, the nature of the information that must be provided upon notification and the time frame for notification.	68	✓	Privacy Breach Management Manual; Privacy Breach Management Policy
	· identify the agent(s) responsible for investigating the privacy breach, the nature and scope of the investigation (i.e. document reviews, interviews, site visits, inspections) and the process that must be followed in investigating the privacy breach.	68	✓	Privacy Breach Management Manual; Privacy Breach Management Policy
	· the policy and procedures must: · include a discussion of the documentation that must be completed, provided and/or executed in undertaking the investigation	68 68	✓	Privacy Breach Management Manual; Privacy Breach Management Policy

	· the agent(s) responsible for completing, providing and/or executing the documentation	68	✓	Privacy Breach Management Manual; Privacy Breach Management Policy
	· the agent(s) to whom this documentation must be provided	68	✓	Privacy Breach Management Manual; Privacy Breach Management Policy
	· the required content of the documentation	68	✓	Privacy Breach Management Manual; Privacy Breach Management Policy; Privacy Breach Report Form; Privacy Breach Log
	· The role of the agent(s) that have a delegated day-to-day authority to manage the privacy and security program	68	✓	Privacy Breach Management Manual; Privacy Breach Management Policy
	· identify the agent(s) responsible for:	68	✓	Privacy Breach Management Manual; Privacy Breach Management Policy
	· for assigning other agent(s) to address the recommendations	68	✓	Privacy Breach Management Manual; Privacy Breach Management Policy
	· for establishing timelines to address the recommendations	68	✓	Privacy Breach Management Manual; Privacy Breach Management Policy

	· for addressing the recommendations;	68	✓	Privacy Breach Management Manual; Privacy Breach Management Policy
	· monitoring and ensuring that the recommendations are implemented within the stated timelines	68	✓	Privacy Breach Management Manual; Privacy Breach Management Policy; Privacy Breach Management Form
	· the nature of the documentation that must be completed, provided and/or executed at the conclusion of the investigation of the privacy breach	68	✓	Privacy Breach Management Manual; Privacy Breach Management Policy; Privacy Breach Management Form
	· the agent(s) responsible for completing, providing and/or executing the documentation	69	✓	Privacy Breach Management Manual; Privacy Breach Management Policy
	· the agent(s) to whom the documentation must be provided	69	✓	Privacy Breach Management Manual; Privacy Breach Management Policy
	· the required content of the documentation	69	✓	Privacy Breach Management Manual; Privacy Breach Management Policy; Privacy Breach Form and Privacy Breach Log

	The policy and procedures must also address the manner and format in which the findings of the investigation of the privacy breach, including the recommendations arising from the investigation and the status of implementation of the recommendations, are communicated. This shall include a discussion of the agent(s) responsible for communicating the findings of the investigation; the mechanism and format for communicating the findings of the investigation; the time frame within which the findings of the investigation must be communicated; and to whom the findings of the investigation must be communicated, including the Chief Executive Officer or the Executive Director.	69	✓	Privacy Breach Management Manual; Privacy Breach Management Policy
	In addition, the policy and procedures shall address whether the process to be followed in identifying, reporting, containing, notifying, investigating and remediating a privacy breach is different where the breach is both a privacy breach or suspected privacy breach, as well as an information security breach or suspected information security breach.	69	✓	Privacy Breach Management Manual; Privacy Breach Management Policy
	· Further, the policy and procedures must require that a log be maintained of privacy breaches and must identify the agent(s) responsible for maintaining the log and for tracking that the recommendations arising from the investigation of privacy breaches are addressed within the identified timelines. They should further address where documentation related to the identification, reporting, containment, notification, investigation and remediation of privacy breaches will	69	✓	Privacy Breach Management Manual; Privacy Breach Management Policy; Privacy Breach Management Form

	be retained and the agent(s) responsible for retaining this documentation.			
	· require agents to comply with the policy and its procedures and address how and by whom compliance will be enforced and the consequences of breach.	69	✓	Privacy Breach Management Manual; Privacy Breach Management Policy; Privacy Breach Management Form
	· stipulate that compliance will be audited in accordance with the *Policy and Procedures In Respect of Privacy Audits,* must set out the frequency with which the policy and procedures will be audited and must identify the agent(s) responsible for conducting the audit and for ensuring compliance with the policy and its procedures.	69	✓	Privacy Audit and Compliance Policy
	· In developing the policy and procedures, it is recommended that the prescribed person or prescribed entity have regard to the guidelines produced by the Information and Privacy Commissioner of Ontario entitled *What to do When Faced With a Privacy Breach: Guidelines for the Health Sector.*	69	✓	Privacy Breach Management Manual; Privacy Breach Management Policy; Privacy Breach Management Form
30	**Log of privacy breaches**			
	· CCO shall maintain a log of privacy breaches	70	✓	CCO's Privacy Policy; Privacy Breach Management Manual; Privacy Breach Management Policy; Privacy Breach Management Form; Log of Privacy Breaches

	· The log must set out: the date of the privacy breach, the date that the privacy breach was identified or suspected, Whether the privacy breach was internal or external, the nature of the PHI that was the subject matter of the privacy breach and the nature and extent of the privacy breach, the date that the privacy breach was contained and the nature of the containment measures, the date that the HIC or other organization that disclosed the PHI to CCO was notified, the date that the investigation of the privacy breach was completed, the agent(s) responsible for conducting the investigation, the recommendations arising from the investigation, the agent(s) responsible for addressing each recommendation, The date each recommendation was or is expected to be addressed, the manner in which each recommendation was or is expected to be addressed	70	✓	Log of Privacy Breaches
31	**Policy and procedures for privacy complaints**			
	· A policy and procedures must be developed and implemented to address the process to be followed in receiving, documenting, tracking, investigating, remediating and responding to privacy complaints	70	✓	CCO's Privacy Policy; Privacy Inquiries and Complaints Procedure
	· definition of the term “privacy complaint” shall be provided that, at a minimum, includes concerns or complaints relating to the privacy policies, procedures and practices implemented by the prescribed person or prescribed entity and related to the compliance of the prescribed person or prescribed entity with the Act and its regulation.	70	✓	Privacy Inquiries and Complaints Procedure

	· The information that must be communicated to the public relating to the manner in which, to whom and where individuals may direct privacy concerns or complaints shall also be identified. At a minimum, the name and/or title, mailing address and contact information of the agent(s) to whom concerns or complaints may be directed and information related to the manner in which and format in which privacy concerns or complaints may be directed to CCO should be made publicly available.	70	✓	CCO's Privacy Policy; Statement of Information Practices; Privacy Inquiries and Complaints Procedure
	· Individuals be advised that they may make a complaint regarding compliance with the Act and it's regulation to the IPC and that the mailing address and contact information for the Information and Privacy Commissioner of Ontario be provided. (Recommendation)	70	✓	CCO's Privacy Policy; Statement of Information Practices
	· establish the process to be followed in receiving privacy complaints. This shall include any documentation that must be completed, provided and/or executed by the individual making the privacy complaint; the agent(s) responsible for receiving the privacy complaint; the required content of the documentation, if any; and the nature of the information to be requested from the individual making the privacy complaint	71	✓	Privacy Inquiries and Complaints Procedure

	· Upon receipt of a privacy complaint, the policy and procedures shall require a determination to be made of whether or not the privacy complaint will be investigated. In this regard, the policy and procedures shall identify the agent(s) responsible for making this determination, the time frame within which this determination must be made and the process that must be followed and the criteria that must be used in making the determination, including any documentation that must be completed, provided and/or executed and the required content of the documentation	71	✓	Privacy Inquiries and Complaints Procedure
	· when an investigation will not be undertaken, the policy and procedures must require that a letter be provided to the individual making the privacy complaint acknowledging: receipt of the privacy complaint, providing a response to the privacy complaint, advising that an investigation of the privacy complaint will not be undertaken, advising the individual that he or she may make a complaint to the IPC if there are reasonable grounds to believe that the prescribed person or prescribed entity has contravened or is about to contravene the Act or its regulation, providing contact information for the IPC	71	✓	Privacy Inquiries and Complaints Procedure

	· when an investigation will be undertaken a letter must be provided to the individual making the privacy complaint acknowledging: receipt of the privacy complaint, advising that an investigation of the privacy complaint will be undertaken, explaining the privacy complaint investigation procedure, indicating whether the individual will be contacted for further information concerning the privacy complaint, setting out the projected time frame for completion of the investigation, identifying the nature of the documentation that will be provided to the individual following the investigation	71	✓	Privacy Inquiries and Complaints Procedure
	· identify the agent(s) responsible for sending the above noted letters to the individuals making privacy complaints and the time frame within which the letters will be sent to the individuals	71	✓	Privacy Inquiries and Complaints Procedure
	· Where an investigation of a privacy complaint will be undertaken, the policy and procedures must identify the agent(s) responsible for investigating the privacy complaint, the nature and scope of the investigation and (i.e. document reviews, interviews, site visits, inspections) the process that must be followed in investigating the privacy complaint. This shall include a discussion of the documentation that must be completed, provided and/or executed in undertaking the investigation; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation.	71	✓	Privacy Inquiries and Complaints Procedure

	· The role of the agent(s) that have been delegated day-to-day authority to manage the privacy and security program	71	✓	Privacy Inquiries and Complaints Procedure
	· The process for addressing the recommendations arising from the investigation of privacy complaints, the agent(s) responsible for assigning other agent(s) to address the recommendations, for establishing timelines to address the recommendations, for monitoring and ensuring the implementation of the recommendations shall also be addressed in the policy and procedures.		✓	Privacy Inquiries and Complaints Procedure
	· set out the nature of the documentation that will be completed, provided and/or executed at the conclusion of the investigation of the privacy complaint including the agent(s) responsible for completing, preparing and/or executing the documentation; the agent(s) to whom the documentation must be provided; and the required content of the documentation.	72	✓	Privacy Inquiries and Complaints Procedure
	· address the manner and format in which the findings of the investigation of the privacy complaint, including recommendations arising from the investigation and the status of implementation of the recommendations, are communicated. This shall include a discussion of the agent(s) responsible for communicating the findings of the investigation; the mechanism and format for communicating the findings of the investigation; the time frame within which the findings of the investigation must be communicated; and to whom the findings must be communicated, including the Chief Executive Officer or the Executive Director.	72	✓	Privacy Inquiries and Complaints Procedure

	· require the individual making the privacy complaint to be notified, in writing, of the nature and findings of the investigation and of the measures taken, if any, in response to the privacy complaint. The individual making the privacy complaint shall also be advised that he or she may make a complaint to the Information and Privacy Commissioner of Ontario if there are reasonable grounds to believe that the Act or its regulation has been or is about to be contravened. The contact information for the Information and Privacy Commissioner of Ontario shall also be provided. The agent(s) responsible for providing the written notification to the individual making the privacy complaint and the time frame within which the written notification must be provided, shall also be addressed.	72	✓	Privacy Inquiries and Complaints Procedure
	The policy and procedures should also address whether any other person or organization must be notified of privacy complaints and the results of the investigation of privacy complaints, and if so, the manner by which, the format in which and the time frame within which the notification must be provided and the agent(s) responsible for providing the notification.	72	✓	Privacy Inquiries and Complaints Procedure
	· require that a log be maintained of privacy complaints and identify the agent(s) responsible for maintaining the log and for tracking whether the recommendations arising from the investigation of privacy complaints are addressed within the identified timelines. They should further address where documentation related to the receipt, investigation, notification and remediation of privacy complaints will be retained and the	72	✓	Privacy Inquiries and Complaints Procedure

	agent(s) responsible for retaining this documentation.			
	· require agents to comply with the policy and its procedures and address how and by whom compliance will be enforced and the consequences of breach.	72	✓	Privacy Breach Management Manual; Privacy Breach Management Policy
	· stipulate that compliance will be audited in accordance with the *Policy and Procedures In Respect of Privacy Audits*, must set out the frequency with which the policy and procedures will be audited and must identify the agent(s) responsible for conducting the audit and for ensuring compliance with the policy and its procedures.	72	✓	Privacy Audit and Compliance Policy
	The relationship between this policy and its procedures and the Policy and Procedures for Privacy Breach Management shall also be addressed.	72	✓	Privacy Audit and Compliance Policy
32	**Log of privacy complaints**			
	· CCO shall maintain a log of privacy complaints received.	73	✓	CCO's Privacy Policy; Privacy Inquiries and Complaints Procedure; Log of Privacy Inquiries and Complaints
	· The log must set out:	73		

	· The date that the privacy complaint was received and the nature of the privacy complaint	73	✓	Log of Privacy Inquiries and Complaints
	· The determination as to whether or not the privacy complaint will be investigated and the date that the determination was made;	73	✓	Log of Privacy Inquiries and Complaints
	· The date that the individual making the complaint was advised that the complaint will not be investigated and was provided a response to the complaint;	73	✓	Log of Privacy Inquiries and Complaints
	· The date that the individual making the complaint was advised that the complaint will be investigated	73	✓	Log of Privacy Inquiries and Complaints
	· The agent(s) responsible for conducting the investigation	73	✓	Log of Privacy Inquiries and Complaints
	· The dates that the investigation was commenced and completed	73	✓	Log of Privacy Inquiries and Complaints
	· The recommendations arising from the investigation	73	✓	Log of Privacy Inquiries and Complaints
	· The agent(s) responsible for addressing each recommendation	73	✓	Log of Privacy Inquiries and Complaints

	· The date each recommendation was or is expected to be addressed	73	✓	Log of Privacy Inquiries and Complaints
	· The manner in which each recommendation was or is expected to be addressed	73	✓	Log of Privacy Inquiries and Complaints
	· The date that the individual making the privacy complaint was advised of the findings of the investigation and the measures taken, if any, in response to the privacy complaint.	73	✓	Log of Privacy Inquiries and Complaints
33	**Policy and procedures for privacy inquiries**			
	· A policy and procedures must be developed and implemented to address the process to be followed in receiving, documenting, tracking and responding to privacy inquiries	74	✓	CCO's Privacy Policy; Privacy Inquiries and Complaints Procedure
	· A definition of the term "privacy inquiry" shall be provided, at a minimum, includes inquiries relating to the privacy policies, procedures and practices implemented by the prescribed person or prescribed entity and related to the compliance of the prescribed person or prescribed entity with the Act and its regulation.	74	✓	Privacy Inquiries and Complaints Procedure
	· The information that must be communicated to the public relating to the manner in which, to whom and where individuals may direct privacy inquiries shall also be identified. At a minimum, the information communicated to the public shall include the name and/or title, mailing address and contact information of the agent(s) to whom privacy inquiries may be directed; information relating to the manner in which privacy	74	✓	Privacy Inquiries and Complaints Procedure

	inquiries may be directed to the prescribed person or prescribed entity; and information as to where individuals may obtain further information about the privacy policies, procedures and practices implemented by the prescribed person or prescribed entity.			
	· establish the process to be followed in receiving and responding to privacy inquiries. This shall include the agent(s) responsible for receiving and responding to privacy inquiries; any documentation that must be completed, provided and/or executed; the required content of the documentation; and the format and content of the response to the privacy inquiry. The role of the agent(s) that have been delegated day-to-day authority to manage the privacy program and the security program shall also be identified.	74	✓	Privacy Inquiries and Complaints Procedure
	· require agents to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach.	74	✓	Privacy Inquiries and Complaints Procedure
	· stipulate that compliance will be audited in accordance with the Policy and Procedures In Respect of Privacy Audits, must set out the frequency with which the policy and procedures will be audited and must identify the agent(s) responsible for conducting the audit and for ensuring compliance with the policy and its procedures.	74	✓	Privacy Inquiries and Complaints Procedure, Privacy Audit and Compliance Policy
	The relationship between this policy and its procedures and the Policy and Procedures for Privacy Complaints and the Policy and Procedures for Privacy Breach Management shall also be addressed.	74	✓	Privacy Inquiries and Complaints Procedure

Table 2 - Security Checklist

IPC 2017 Triennial Review - Requested Security Documentation				
Req.	**Minimum Content of Required Documentation**	**Page Ref# in Manual**	**Req't Met**	**Identifying CCO Document**
1	**Information security policy**			
	• An overarching information security policy, or equivalent, must be developed and implemented in relation to PHI received by CCO under the *Act*.	75	✓	Enterprise information Security Policy
	• require that steps be taken that are reasonable in the circumstances to ensure that the PHI is protected	75	✓	Enterprise information Security Policy
	• undertake organization-wide threat and risk assessments of all information security assets	75	✓	Enterprise information Security Policy
	• information security program to be developed and implemented consisting of administrative, technical and physical safeguards	75	✓	Enterprise Information Security Policy; Information Security Program Framework
	• the information security program must:	75		
	• effectively address the threats and risks identified	75	✓	Enterprise Information Security Policy; Information Security Program Framework;
	• be amenable to independent verification	75	✓	Enterprise Information Security Policy; Information Security Program Framework;
	• be consistent with established security frameworks and control objectives	75	✓	Enterprise Information Security Policy; Information Security Program Framework;

	• address the duties and responsibilities of agents in respect of the information security program	75	✓	Enterprise Information Security Policy; Information Security Program Framework;
	• the policy must consist of the following control objectives and security policies, procedures and practices:	75		
	• A security governance framework	75	✓	Enterprise Information Security Policy;
	• ongoing review of the security policies, procedures and practices	75	✓	Enterprise Information Security Policy;
	• ensuring the physical security of the premises	75	✓	Enterprise Information Security Policy;
	• include policies and procedures for the secure retention, transfer and disposal of records of PHI including policies and procedures related to mobile devices, remote access and security of data at rest	75	✓	Enterprise Information Security Policy; Information Security Program Framework; Incident Management Framework; Logging, Monitoring, and Auditing Standard;
	• establishing access control and authorization	75	✓	Enterprise Information Security Policy; Logical Access Control Standard;
	• information systems acquisition, development and maintenance	76	✓	Enterprise Information Security Policy; IM/IT Gating Process and Project Lifecycle Methodology; Acquisition, Development, and Application Security Standard;
	• for monitoring	76	✓	Enterprise Information Security Policy; Logging, Monitoring, and Auditing Standard;
	• for network security management • acceptable use of information technology	76 76	✓ ✓	Enterprise Information Security Policy; Enterprise Information Security Policy; Information Security Code of Conduct and Acceptable Use Policy; Acceptable Use of Social Media Policy;

	• back-up and recovery	76	✓	Enterprise Information Security Policy; Data Backup Policy;
	• information security breach management	76	✓	Enterprise Information Security Policy;
	• establishing protection against malicious and mobile code	76	✓	Enterprise Information Security Policy;
	• outline the information security infrastructure implemented by CCO	76	✓	Enterprise Information Security Policy;
	• require a credible program to be implemented for continuous assessment and verification of the effectiveness of the security program	76	✓	Enterprise Information Security Policy;
	• address how and by whom compliance will be enforced and the consequences of breach	76	✓	Enterprise Information Security Policy; Information Security Code of Conduct and Acceptable Use Policy;
	• stipulate that compliance will be audited	76	✓	Enterprise Information Security Policy; Logging, Monitoring, and Auditing Standard;
	• refer to more detailed policies and procedures developed and implemented to address the requirements for control objectives and security policies, procedures and practices	76	✓	Enterprise Information Security Policy;
	• require agents to notify CCO if an agent believes there may have been a breach of this policy or any of the security policies	77	✓	Enterprise Information Security Policy;
2	**Policy and procedures for ongoing review of security policies, procedures and practices**			
	• A policy and associated procedures must be developed and	77	✓	Enterprise Information Security Policy;

	implemented for the ongoing review of the security policies, procedures and practices put in place by CCO			
	• The policy and procedure must identify:	77		
	• the frequency of the review	77	✓	Enterprise Information Security Policy;
	• the agent(s) responsible for undertaking the review	77	✓	Enterprise Information Security Policy;
	• the procedure to be followed in undertaking the review	77	✓	Enterprise Information Security Policy;
	• the time frame in which the review will be undertaken	77	✓	Enterprise Information Security Policy;
	• the security policies, procedures and practices implemented by CCO must be reviewed on an annual basis	77	✓	Information Security Framework; Enterprise Information Security Policy;
	• In undertaking the review and determining whether amendments and/or new security policies are necessary CCO must have regard to:	77		
	• orders, guidelines, fact sheets and best practices issued by the IPC	77	✓	Enterprise Information Security Policy;
	• evolving industry security standards and best practices	77	✓	Enterprise Information Security Policy;
	• technological advancements	77	✓	Enterprise Information Security Policy;
	• amendments to the Act and its regulation relevant to CCO	77	✓	Enterprise Information Security Policy;
	• recommendations arising from privacy and security audits, PIAs and	77	✓	Enterprise Information Security Policy;

	investigations into privacy complaints/breaches			
	• in undertaking the review and determining whether amendments and/or new security policies, procedures and practices are necessary, CCO must have regard to recommendations arising from information security breaches	77	✓	Enterprise Information Security Policy; Incident Management Framework;
	• whether the security policies, procedures and practices of CCO continue to be consistent with its actual practices	77	✓	Enterprise Information Security Policy;
	• consistency between the security and privacy policies, procedures and practices	77	✓	Enterprise Information Security Policy;
	• procedure to be followed in communicating the amended or newly developed security policies, procedures and practices	77	✓	Enterprise Information Security Policy;
	• procedure to be followed in reviewing and amending the communication materials available to the public	77	✓	Enterprise Information Security Policy;
	• complying with the policy and its procedures and addressing how and by whom compliance will be enforced and the consequences of breach	77	✓	Enterprise Information Security Policy; Information Security Code of Conduct and Acceptable Use Policy;
	• stipulate that compliance will be audited	78	✓	Enterprise Information Security Policy; Logging, Monitoring, and Auditing Standard;
3	**Policy and procedures for ensuring physical security of PHI**			

	• A policy/procedures must be developed and implemented addressing physical safeguards implemented by CCO to protect PHI	78	✓	Enterprise Information Security Policy
	• physical safeguards shall include controlled access to the premises and to where PHI records are retained	78	✓	Enterprise Information Security Policy; CCO's Video Monitoring Policy
	• compliance with the policy and its procedures and address how and by whom compliance will be enforced and the consequences of breach.	78	✓	Enterprise Information Security Policy; Information Security Code of Conduct and Acceptable Use Policy
	• stipulate that compliance will be audited	78	✓	Enterprise Information Security Policy
	• the premises of CCO be divided into varying levels of security	78	✓	Data Centre Access and Usage Policy
	• in order to access locations within the premises where records of PHI are retained, individuals be required to pass through multiple levels of security.	78	✓	Enterprise Information Security Policy; Data Centre Access and Usage Policy; Visitor Access Policy; Access Data Centre Authorization - Employee; Access Data Centre Authorization - Contractor
	• require agents to notify CCO at the first reasonable opportunity, in accordance with the Policy and Procedures for Information Security Breach Management, if an agent breaches or believes there may have been a breach of the policy or associated procedures	78	✓	Enterprise Information Security Policy
	• set out the various levels of access that may be granted to the premises	78	✓	Enterprise Information Security Policy; Data Centre Access and Usage Policy; Visitor Access Policy; Access Data Centre Authorization - Employee;

				Access Data Centre Authorization - Contractor
	• this policy must identify the agent(s) responsible for receiving, reviewing, granting and terminating access by agents to the premises and to locations	79	✓	Automated HCMS process
	• the process to be followed and the requirements that must be satisfied includes	79		
	• any documentation that must be completed, provided and/or executed	79	✓	Automated HCMS process
	• the agent(s) responsible for completing, providing and/or executing the documentation	79	✓	Automated HCMS process
	• the agent(s) to whom the documentation must be provided	79	✓	Automated HCMS process
	• the required content of the documentation	79	✓	Enterprise Information Security Policy; Logical Access Control Standard; Internal Data Access Requests (IDAR) Process
	• criteria that must set out by the agent(s) responsible for approving and determining the appropriate level of access	79	✓	Logical Access Control Standard

	• criteria that must be considered by the agent (s) responsible for approving and determining the appropriate level of access must be based on the "need to know" principle and must ensure that access is only provided to agents who routinely require such access for their employment, contractual or other responsibilities. In the event that an agent only requires such access for a specified period, the Policy must establish a process for ensuring that access is permitted only for that specified period	79	✓	Enterprise Information Security Policy; Logical Access Control Standard; Internal Data Access Requests (IDAR) Process
	• this policy/procedure must:	79		
	• set out the manner in which the determination relating to access and the level of access is documented	79	✓	Enterprise Information Security Policy; Logical Access Control Standard; Internal Data Access Requests (IDAR) Process
	• whom this determination will be communicated	79	✓	Enterprise Information Security Policy; Logical Access Control Standard; Internal Data Access Requests (IDAR) Process
	• any documentation that must be completed, provided and/or executed by the agent(s) responsible for making the determination	79	✓	Enterprise Information Security Policy; Logical Access Control Standard; Internal Data Access Requests (IDAR) Process;
	• the required content of the documentation	79	✓	Enterprise Information Security Policy; Logical Access Control Standard; Internal Data Access Requests (IDAR) Process

	• address the agent(s) responsible and the process to be followed in providing identification cards, access cards and/or keys to the premises and to locations within the premises	79	✓	Photo Identification Request Form; Automated HCMS process
	• require agents to notify CCO at the first reasonable opportunity of the theft, loss or misplacement of identification cards, access cards and/or keys and shall set out the process that must be followed in this regard	79	✓	Photo ID Badge Request; Access Card Procedure
	• this shall include a discussion of the agent(s) to whom the notification must be provided	79	✓	Photo ID Badge Request; Access Card Procedure
	• the nature and format of the notification	79	✓	Photo ID Badge Request; Access Card Procedure
	• the documentation that must be completed, provided and/or executed	79	✓	Photo ID Badge Request; Access Card Procedure
	• the agent(s) responsible for completing, providing and/or executing the documentation	79	✓	Photo ID Badge Request; Access Card Procedure
	• the agent to whom the documentation must be provided	79	✓	Photo ID Badge Request; Access Card Procedure
	• the required content of the documentation	79	✓	Photo ID Badge Request; Access Card Procedure
	• the safeguards that are required to be implemented as a result of the theft, loss or misplacement of	79	✓	Access Card Procedure

	identification cards, access cards and/or keys and the agent(s) responsible for implementing these safeguards shall also be outlined			
	• the circumstances in which and the procedure that must be followed in issuing temporary or replacement identification cards, access cards and/or keys and the agent(s) responsible for their issuance	79	✓	Access Card Procedure
	• this shall include a discussion of any documentation that must be completed, provided and/or executed	79	✓	Access Card Procedure
	• the agent(s) responsible for completing, providing and/or executing the documentation	79	✓	Access Card Procedure
	• the agent to whom the documentation must be provided	80	✓	Access Card Procedure
	• the required content of the documentation	80	✓	Access Card Procedure
	• the agent(s) to whom temporary identification cards, access cards and/or keys shall be returned	80	✓	Access Card Procedure
	• the time frame for return	80	✓	Access Card Procedure
	• the process to be followed in the event that temporary identification cards, access cards and/or keys are not	80	✓	Access Card Procedure

	returned, including the agent(s) responsible for implementing the process and the time frame within which the process must be implemented, shall also be addressed			
	• require agents to notify CCO of the termination of their employment and to return their identification cards, access cards and/or keys	80	✓	Automated HCMS process
	• require that access to the premises be terminated upon the cessation of the relationship	80	✓	Automated HCMS process
	• an agent's supervisor must notify CCO when the agent no longer requires access to location(s) where records of PHI are retained	80	✓	Automated HCMS process
	• agent's supervisor will notify CCO when the agent no longer requires such access	80	✓	Automated HCMS process
	• The policy and procedure must identify:	80		
	• the agent(s) to whom the notification must be provided	80	✓	Automated HCMS process;
	• the nature and format of the notification	80	✓	Automated HCMS process
	• the time frame within which the notification must be provided	80	✓	Automated HCMS process
	• the process that must be followed in providing the notification • the agent(s) responsible for terminating access	80 80	✓ ✓	Automated HCMS rocess Automated HCMS process

	• the procedure to be followed in terminating access	80	✓	Automated HCMS process
	• the method by which access will be terminated	80	✓	Automated HCMS process
	• the time frame within which access must be terminated.	80	✓	Automated HCMS process
	• Audits must be conducted of agents with access to the premises of CCO	80	✓	Privacy Audit and Compliance Policy
	• identify the agent(s) responsible for conducting the audits and for ensuring compliance with the policy and its procedures	81	✓	Privacy Audit and Compliance Policy
	• identify the agent(s) responsible for maintaining such a log	81	✓	Privacy Audit and Compliance Policy
	• address where documentation related to the receipt, review, approval and termination of access to the premises at CCO where PHI is retained and the agent(s) responsible for maintaining this documentation.	81	✓	Privacy Audit and Compliance Policy
	• address the agent(s) responsible and the process to be followed in identifying, screening and supervising visitors to CCO	81	✓	Visitor Access Procedure
	• the policy and procedures will set out: • the identification that is required to be worn by visitors	81 81	✓	Visitor Access Procedure

	• any documentation that must be completed, provided and/or executed by agent(s) responsible for identifying, screening and supervising visitors	81	✓	Visitor Access Procedure
	• the documentation that must be completed, provided and/or executed by visitors	81	✓	Visitor Access Procedure
	• address the duties of agent(s) responsible for identifying, screening and supervising visitors	81	✓	Visitor Access Procedure
	• address the process to be followed when the visitor does not return the identification provided	81	✓	Visitor Access Procedure
	• address where documentation related to the identification, screening and supervision of visitors will be retained	81	✓	Visitor Access Procedure
4	**Log of agents with access to the premises of CCO**			
	• a log must be maintained of agents granted approval to access the premises of CCO	81	✓	Key Logging System; Visitor Logging System ; Automated HCMS process;
	• the log must include:	82	✓	
	• the name of the agent granted approval to access the premises	82	✓	Key Logging System; Visitor Logging System ; Automated HCMS process
	• the level and nature of the access granted	82	✓	Key Logging System; Visitor Logging System ; Automated HCMS process
	• the locations within the premises to which access is granted	82	✓	Key Logging System; Visitor Logging System ; Automated HCMS process
	• the date that the access was granted	82	✓	Key Logging System; Visitor Logging System ; Automated HCMS process

	• the identification numbers on the identification cards, access cards and/or keys	82	✓	Key Logging System; Visitor Logging System ; Automated HCMS process
	• the date of the next audit of access	82	✓	Key Logging System; Visitor Logging System ; Automated HCMS process
	• the date that the identification cards, access cards and/or keys were returned to CCO	82	✓	Key Logging System; Visitor Logging System ; Automated HCMS process
5	**Policy and procedures for secure retention of records of PHI**			
	• A policy and procedures must be developed and implemented with respect to the secure retention of records of PHI in paper and electronic format	82	✓	Enterprise Information Security Policy; Information Classification and Handling Standard (Draft); Information Classification and Handling Guideline (Draft); Privacy Policy; Data Use & Disclosure Standard; Policy on Retention of Records Containing PHI
	• identify the retention period for records of PHI in both paper and electronic format, including various categories thereof	82		
	• for records of PHI used for research purposes, CCO must ensure that the records of PHI are not being retained for a period longer than that set out in the written research plan approved by a research ethics board	82	✓	Application for Disclosure of Information from CCO for Research Purposes; Data Use & Disclosure Standard
	• for records of PHI collected pursuant to a Data Sharing Agreement, the policy and procedures must prohibit the records from being retained for a period longer than that set out in the Data Sharing Agreement.	82	✓	Data Sharing Agreement Template; Data Sharing Agreement Initiation Procedure; Data Sharing Agreement Standard; Privacy Policy; Data Use & Disclosure Standard

	• in any event, the policy and procedures must mandate that records of PHI be retained for only as long as necessary to fulfill the purposes for which the PHI was collected.	82	✓	Data Sharing Agreement Template; Data Sharing Agreement Initiation Procedure; Data Sharing Agreement Standard; Privacy Policy; Data Use & Disclosure Standard
	• require the records of PHI to be retained in a secure manner and must identify the agent(s) responsible for ensuring the secure retention of these records	82	✓	Enterprise Information Security Policy, Information Classification and Handling Standard (Draft), Information Classification and Handling Guideline (Draft); Privacy Policy; Data Use & Disclosure Standard;
	• identify the precise methods by which records of PHI in paper and electronic format are to be securely retained, including records retained on various media	82	✓	Information Classification and Handling Guideline (Draft)
	• require agents of CCO to take steps that are reasonable in the circumstances to ensure that PHI is protected against theft, loss and unauthorized use or disclosure and to ensure that records of PHI are protected against unauthorized copying, modification or disposal	82	✓	Enterprise Information Security Policy; Information Classification and Handling Standard (Draft); Information Classification and Handling Guideline (Draft); Privacy Policy; Data Use & Disclosure Standard;
	• the reasonable steps that must be taken by agents shall also be outlined in the policy and procedures	82	✓	Information Classification and Handling Guideline (Draft)
	• If a third party service provider is contracted to retain records of PHI on behalf of CCO the policy must address:	82		

	• the circumstances in which and the purposes for which records of PHI will be transferred to the third party service provider for secure retention.	82	✓	Services Agreement - Schedules for Third Party Agreements; Data Backup Policy; Data Backup Procedure; Data Use & Disclosure Standard
	• the procedure to be followed in securely transferring the records of PHI to the third party service provider	82	✓	Services Agreement - Schedules for Third Party Agreements; Data Backup Policy; Data Backup Procedure; Information Classification and Handling Guideline (Draft); Secure Transfer of PHI Policy; Secure Transfer of PHI Standard;
	• the procedure to be followed in securely retrieving the records from the third party service provider, including the secure manner in which the records will be transferred and retrieved, the conditions pursuant to which the records will be transferred and retrieved and the agent(s) responsible for ensuring the secure transfer and retrieval of the records, i.e. the procedures shall comply with the Policy and Procedures for Secure Transfer of Records of PHI	83	✓	Services Agreement - Schedules for Third Party Agreements; Data Backup Policy; Data Backup Procedure; Information Classification and Handling Guideline (Draft); Secure Transfer of PHI Policy; Secure Transfer of PHI Standard;
	• address the documentation that is required to be maintained in relation to the transfer of records of PHI to the third party service	83	✓	Services Agreement - Schedules for Third Party Agreements; Data Backup Policy; Data Backup Procedure; Information Classification and Handling Guideline (Draft); Secure Transfer of PHI Policy; Secure Transfer of PHI Standard;

	provider for secure retention			
	• require the agent(s) responsible for ensuring the secure transfer to document the date, time and mode of transfer	83	✓	Services Agreement - Schedules for Third Party Agreements; Data Backup Policy; Data Backup Procedure; Information Classification and Handling Guideline (Draft); Secure Transfer of PHI Policy; Secure Transfer of PHI Standard;
	• maintain a repository of written confirmations received from the third party service provider upon receipt of the records of PHI	83	✓	Services Agreement - Schedules for Third Party Agreements; Data Backup Policy; Data Backup Procedure; Information Classification and Handling Guideline (Draft); Secure Transfer of PHI Policy; Secure Transfer of PHI Standard;
	• require a detailed inventory ~~is required~~ to be maintained of records of ~~for the~~ PHI being securely retained by the third party service provider	83	✓	Open Media Logs; HP Data Protectors Session Logs; Information Classification and Handling Guideline (Draft); Services Agreement - Schedules for Third Party Agreements; Data Backup Policy; Data Backup Procedure; Secure Transfer of PHI Policy; Secure Transfer of PHI Standard;
	• require a detailed inventory to be maintained of records of PHI retrieved by CCO	83	✓	Open Media Logs; HP Data Protectors Session Logs; Services Agreement - Schedules for Third Party Agreements; Data Backup Policy; Data Backup Procedure; Information Classification and Handling Guideline (Draft); Secure Transfer of PHI Policy; Secure Transfer of PHI Standard;
	• identify the agent(s) responsible for maintaining the detailed inventory and the agent(s) responsible for ensuring that the Template Agreement for All Third Party Service Providers has been executed prior	83	✓	Log of Third Party Service Providers with Access to Personal Health Information; Data Use & Disclosure Standard; Services Agreement - Schedules for Third Party Agreements; Data Backup Policy; Data Backup Procedure; Information Classification and Handling Guideline (Draft); Secure

	to transferring the records of PHI for secure retention			Transfer of PHI Policy; Secure Transfer of PHI Standard;
	• where a third party service provider is contracted to retain records of PHI, the policy and procedures must require that a written agreement be executed with the third party service provider containing the relevant language from the *Template Agreement For All Third Party Service Providers*	83	✓	Data Use & Disclosure Standard; Privacy Policy; Information Classification and Handling Standard (Draft)
	• require agents to comply with the policy and its procedures	83	✓	Data Use & Disclosure Standard; Data Sharing Agreement Standard; CCO's Data Sharing Agreement Initiation Procedure; Services Agreement - Schedules for Third Party Agreements; Enterprise Information Security Policy; Privacy Policy;
	• address how and by whom compliance will be enforced	83	✓	Enterprise Information Security Policy; Privacy Policy; Security Audit, Testing and Compliance Policy; Privacy Audit and Compliance Standard; CCO's Data Sharing Agreement Standard; Data Sharing Agreement Initiation Procedure;
	• address the consequences of breach.	83	✓	Privacy Breach Management Policy; Information Security Code of Conduct and Acceptable Use Policy; Enterprise Information Security Policy; Privacy Policy;

	• stipulate that compliance will be audited in accordance with the Policy and Procedures In Respect of Security Audits,	83	✓	Enterprise Information Security Policy; Privacy Policy; Security Audit, Testing and Compliance Standard; Privacy Audit and Compliance Policy; Data Sharing Agreement Initiation Procedure; Data Sharing Agreement Standard;
	• set out the frequency with which the policy and procedures will be audited	83	✓	Enterprise Information Security Policy; Privacy Policy; Security Audit, Testing and Compliance Standard; Privacy Audit and Compliance Policy; Data Sharing Agreement Standard; Data Sharing Agreement Initiation Procedure;
	• identify the agent(s) responsible for conducting the audit and for ensuring compliance with the policy and its procedures	83	✓	Enterprise Information Security Policy; Privacy Policy; Security Audit, Testing and Compliance Standard; Privacy Audit and Compliance Policy; Data Sharing Agreement Standard; Data Sharing Agreement Initiation Procedure;
	• require agents to notify CCO at the first reasonable opportunity, in accordance with the Policy and Procedures for Information Security Breach Management, if an agent believes there may have been a breach of this policy or its procedures	83	✓	Privacy Breach Management Policy; Enterprise Information Security Policy; Privacy Policy; Information Security Code of Conduct and Acceptable Use Policy;
6	**Policy and procedures for secure retention of records of PHI on mobile devices**			
	• identify whether and in what circumstances, if any, CCO permits PHI to be retained on a mobile device.	84	✓	Digital PHI Handling Standard; Information Classification and Handling Standard (draft); Data Backup Policy;
	• require agents to comply with the policy and its procedures and address how and by whom compliance will be	84	✓	Enterprise Information Security Policy; Information Security Code of Conduct and Acceptable Use Policy; Data Backup Policy;

	enforced and the consequences of breach.			
	• set out the circumstances, in which PHI is retained on a mobile device, is permitted.	84	✓	Digital PHI Handling Standard; Digital PHI Handling Procedure; Data Backup Policy; Information Classification and Handling Standard;
	• state whether approval is required prior to retaining PHI on a mobile device.	84	✓	Digital PHI Handling Standard; Digital PHI Handling Procedure; Information Classification and Handling Standard;
	• If approval is required:	84		
	• a discussion of any documentation that must be completed, provided and/or executed	84	✓	Digital PHI Handling Standard; Digital PHI Handling Procedure;
	• the agent(s) responsible for completing, providing and/or executing the documentation	84	✓	Digital PHI Handling Standard; Digital PHI Handling Procedure;
	• the agent(s) to whom this documentation must be provided	84	✓	Digital PHI Handling Standard; Digital PHI Handling Procedure;
	• the required content of the documentation	84	✓	Digital PHI Handling Standard; Digital PHI Handling Procedure;
	• have regard to orders, factsheets and guidelines issued by the IPC	84	✓	Enterprise Information Security Policy; Digital PHI Handling Standard;
	• the policy and procedure should set out:	85		
	• the manner in which the decision approving or denying the request is documented;	85	✓	Digital PHI Handling Standard; Digital PHI Handling Procedure;
	• the method by which and the format in which the decision will be communicated	85	✓	Digital PHI Handling Standard; Digital PHI Handling Procedure;

	• to whom the decision will be communicated.	85	✓	Digital PHI Handling Standard; Digital PHI Handling Procedure;
	• address the requirements and criteria for making a decision on a request for the retention of PHI on a mobile device	85	✓	Digital PHI Handling Standard; Digital PHI Handling Procedure;
	• prior to approval the agent(s) responsible for making the decision must ensure that de-identified information will not serve the purpose	85	✓	Digital PHI Handling Standard; Digital PHI Handling Procedure;
	• require mobile devices containing PHI to be encrypted as well as password-protected using strong and complex passwords that are in compliance with the Policy and Procedure relating to Passwords	85	✓	Digital PHI Handling Standard; Digital PHI Handling Procedure; Mobile Device and Pager Policy; Cryptography Standard; Logical Access Control Standard;
	• identify the conditions or restrictions to retain PHI on a mobile device. The agent must:	85		
	• require that a mandatory standardized password-protected screen saver be enabled after a defined period of inactivity	85	✓	This is done in practice at CCO through technical controls.
	• identify the agent(s) responsible for encrypting mobile devices and for ensuring that the mandatory standardized password-protected screen saver is enabled	85	✓	This is done in practice at CCO through technical controls.
	• Be prohibited from retaining PHI on a mobile device if de-identified and/or	85	✓	

	aggregate information, will serve the purpose			
	• De-identify the PHI to the fullest extent possible	85	✓	Digital PHI Handling Standard; Digital PHI Handling Procedure;
	• Be prohibited from retaining more PHI on a mobile device than is reasonably necessary for the identified purpose;	85	✓	Digital PHI Handling Standard; Digital PHI Handling Procedure;
	• Be prohibited from retaining PHI on a mobile device for longer than necessary to meet the identified purpose	85	✓	Digital PHI Handling Standard; Digital PHI Handling Procedure;
	• Ensure that the strong and complex password for the mobile device is different from passwords for the files containing the PHI	86	✓	Digital PHI Handling Standard; Digital PHI Handling Procedure;
	• detail the steps that must be taken by agents to protect the PHI retained on a mobile device	86	✓	Digital PHI Handling Standard; Digital PHI Handling Procedure; Cryptography Standard; Logical Access Control Standard;
	• ensure the PHI on a mobile device in compliance with the Policy and Procedures for Secure Retention of Records of Personal Health Information	86	✓	Digital PHI Handling Standard; Digital PHI Handling Procedure;
	• securely delete PHI retained on a mobile device in accordance with the process	86	✓	Digital PHI Handling Standard; Digital PHI Handling Procedure; Digital Media Disposal Guideline; Digital Media Disposal Procedure; Digital Media Disposal Standard; Cryptography Standard
	• If CCO does not permit PHI to be retained on a mobile device, the policy and procedures must expressly prohibit the	86	✓	Information Security Code of Conduct and Acceptable Use Policy; Mobile Device and Pager Policy;

	retention of PHI on a mobile device			
	• indicate whether or not PHI may be accessed remotely through a secure connection or virtual private network.	86	✓	Digital PHI Handling Standard; Cryptography Standard;
	• If CCO permits PHI to be accessed remotely, the policy and procedures must set out the circumstances in which this is permitted	86	✓	Digital PHI Handling Standard; Digital PHI Handling Procedure;
	• identify whether approval is required prior to accessing PHI remotely through a secure connection or virtual private network.	86	✓	Digital PHI Handling Standard; Digital PHI Handling Procedure;
	• If approval is required identify the process that must be followed for making a decision on a request for remote access to PHI	86	✓	Digital PHI Handling Standard; Digital PHI Handling Procedure;
	• address the requirements and criteria that must be considered by the agent(s) responsible for determining whether to approve or deny the request for remote access.	86	✓	Digital PHI Handling Standard; Digital PHI Handling Procedure;
	• prior to approval require the agent(s) responsible for making a decision to ensure that , namely de-identified and/or aggregate information, will not serve the identified purpose and that no more	86	✓	Digital PHI Handling Standard; Digital PHI Handling Procedure;

	PHI will be accessed than is reasonably necessary to meet the identified purpose			
	• require the agent(s) responsible for making the decision to ensure that the use of the PHI has been approved	87	✓	Digital PHI Handling Standard; Digital PHI Handling Procedure;
	• identify the manner in which the decision approving or denying the request is documented; the method by which and the format in which the decision will be communicated; and to whom the decision will be communicated	87	✓	Digital PHI Handling Standard; Digital PHI Handling Procedure;
	• identify the conditions or restrictions with which agents granted approval to access PHI remotely must comply.	87	✓	Digital PHI Handling Standard; Digital PHI Handling Procedure;
7	**Policy and procedure for secure transfer of records of PHI**			
	• A policy and procedures must be developed and implemented with respect to the secure transfer of records of PHI in paper and electronic format.	87	✓	Secure Transfer of Personal Health Information Policy; Secure Transfer of Personal Health Information Standard; Cryptography Standard; Exchanging Personal Health Information Policy Suite
	• require records of PHI to be transferred in a secure manner and set out the secure methods of transfer in paper and electronic format	87	✓	Secure Transfer of Personal Health Information Policy; Secure Transfer of Personal Health Information Standard; Cryptography Standard; Exchanging Personal Health Information Policy Suite
	• require agents to use the approved methods of transferring records of PHI	87	✓	Secure Transfer of Personal Health Information Policy; Secure Transfer of Personal Health Information Standard; Cryptography Standard; Exchanging Personal Health Information Policy Suite

	• outline the procedures that must be followed in transferring records of PHI through each of the approved methods. This includes:	87		
	• a discussion of the conditions pursuant to which records of PHI will be transferred	87	✓	Secure Transfer of Personal Health Information Policy; Secure Transfer of Personal Health Information Standard; Cryptography Standard; Exchanging Personal Health Information Policy Suite
	• the agent(s) responsible for ensuring the secure transfer	87	✓	Secure Transfer of Personal Health Information Policy; Secure Transfer of Personal Health Information Standard; Cryptography Standard; Exchanging Personal Health Information Policy Suite
	• any documentation that is required to be completed, provided and/or executed in relation to the secure transfer	87	✓	Secure Transfer of Personal Health Information Policy; Secure Transfer of Personal Health Information Standard; Cryptography Standard; Exchanging Personal Health Information Policy Suite
	• the agent(s) responsible for completing, providing and/or executing the documentation	87	✓	Secure Transfer of Personal Health Information Policy; Secure Transfer of Personal Health Information Standard; Cryptography Standard; Exchanging Personal Health Information Policy Suite
	• and the required content of the documentation.	87	✓	Secure Transfer of Personal Health Information Policy; Secure Transfer of Personal Health Information Standard; Cryptography Standard; Exchanging Personal Health Information Policy Suite
	• whether the agent transferring records of PHI is required to document the date, time and mode of transfer	87	✓	Secure Transfer of Personal Health Information Policy; Secure Transfer of Personal Health Information Standard; Cryptography Standard; Exchanging Personal Health Information Policy Suite

	• the recipient of the records of PHI	87	✓	Secure Transfer of Personal Health Information Policy; Secure Transfer of Personal Health Information Standard; Cryptography Standard; Exchanging Personal Health Information Policy Suite
	• and the nature of the records of PHI transferred	87	✓	Secure Transfer of Personal Health Information Policy; Secure Transfer of Personal Health Information Standard; Cryptography Standard; Exchanging Personal Health Information Policy Suite
	• address whether confirmation of receipt of the records of PHI is required from the recipient	87	✓	Secure Transfer of Personal Health Information Policy; Secure Transfer of Personal Health Information Standard; Cryptography Standard; Exchanging Personal Health Information Policy Suite
	• the manner of obtaining and recording acknowledgement of receipt of the records of PHI and the agent(s) responsible for doing so	87	✓	Secure Transfer of Personal Health Information Policy; Secure Transfer of Personal Health Information Standard; Cryptography Standard; Exchanging Personal Health Information Policy Suite
	• outline the safeguards for transferring records of PHI	88	✓	CCO's Information Security Policy CCO's Cryptography Standard CCO's Logical Access Control Standard CCO's Information Classification and Handling Standard (Draft) CCO's Information Classification and Handling Guideline (Draft)
	• ensure that the procedures and safeguards required to be implemented in respect of the secure transfer of records of PHI are consistent with:	88		

	• Orders, guidelines, factsheets issued by the IPC	88	✓	Enterprise Information Security Policy; Secure Transfer of Personal Health Information Policy;
	• Evolving privacy and security standards and best practices	88	✓	Enterprise Information Security Policy; Information Security Program Framework; Secure Transfer of Personal Health Information Policy;
	• require agents to comply with the policy and its procedures and address how compliance will be enforced and the consequences of breach.	88	✓	Enterprise Information Security Policy; Information Security Code of Conduct and Acceptable Use Policy; Information Classification and Handling Standard
	• stipulate that compliance will be audited	88	✓	Enterprise Information Security Policy; Security Audit, Testing and Compliance Standard; Logging, Monitoring, and Auditing Standard; Information Classification and Handling Standard
	• require agents to notify CCO if an agent believes there may have been a breach of this policy or its procedures.	88	✓	Enterprise Information Security Policy; Information Classification and Handling Standard;
8	**Policy and procedures for secure disposal of records of PHI**			
	• A policy and procedures must be developed and implemented with respect to the secure disposal of records of PHI in both paper and electronic format in order to ensure that reconstruction of these records is not reasonably foreseeable in the circumstances.	88	✓	Enterprise Information Security Policy; Operational Security Standard; Digital Media Disposal Standard; Digital Media Disposal Procedure; Information Classification and Handling Guideline (Draft); Privacy Policy; Hard-Copy PHI Disposal Procedure

	• require records of PHI to be disposed of in a secure manner and must provide a definition of secure disposal that is consistent with the Act and its regulation	88	✓	Enterprise Information Security Policy; Operational Security Standard; Digital Media Disposal Standard; Digital Media Disposal Procedure; Information Classification and Handling Guideline (Draft); Privacy Policy; Hard-Copy PHI Disposal Procedure
	• identify the precise method by which records of PHI in paper format are required to be securely disposed of	88	✓	Hard-Copy PHI Disposal Procedure
	• identify the precise method by which records of PHI in electronic format, including records retained on various media, are required to be securely disposed of	89	✓	Digital Media Disposal Standard; Digital Media Disposal Procedure
	• ensure that the method of secure disposal adopted is consistent with:	89	✓	
	• the Act and its regulation	89	✓	Enterprise Information Security Policy; Operational Security Standard; Digital Media Disposal Standard; Digital Media Disposal Procedure; Information Classification and Handling Guideline (Draft); Privacy Policy; Hard-Copy PHI Disposal Procedure
	• orders issued by the IPC of Ontario under the Act and its regulation, including Order HO-001 and Order HO-006; and with guidelines, fact sheets and best practices	89	✓	Enterprise Information Security Policy; Operational Security Standard; Digital Media Disposal Standard; Digital Media Disposal Procedure; Information Classification and Handling Guideline (Draft); Privacy

	issued by the IPC of Ontario pursuant to the Act and its regulation, including Fact Sheet 10: Secure Destruction of Personal information			Policy; Hard-Copy PHI Disposal Procedure
	• address the secure retention of records of PHI pending their secure disposal in accordance with the Policy and Procedures for Secure Retention of Records of PHI	89	✓	Enterprise Information Security Policy; Operational Security Standard; Digital Media Disposal Standard; Digital Media Disposal Procedure; Information Classification and Handling Guideline (Draft); Privacy Policy; Hard-Copy PHI Disposal Procedure
	• require the physical segregation of records of PHI intended for secure disposal from other records intended for recycling	89	✓	Digital Media Disposal Standard; Digital Media Disposal Procedure; Hard-Copy PHI Disposal Procedure
	• require that an area be designated for the secure retention of records of PHI pending their secure disposal	89	✓	Digital Media Disposal Standard; Digital Media Disposal Procedure; Hard-Copy PHI Disposal Procedure
	• require the records of PHI to be retained in a clearly marked and locked container pending their secure disposal	89	✓	Digital Media Disposal Standard; Digital Media Disposal Procedure; Hard-Copy PHI Disposal Procedure
	• identify the agent(s) responsible for ensuring the secure retention of records of PHI pending their secure disposal	89	✓	Enterprise Information Security Policy; Operational Security Standard; Digital Media Disposal Standard; Digital Media Disposal Procedure; Information Classification and Handling Standard; Information Classification and Handling Guideline

				(Draft); Privacy Policy; Hard-Copy PHI Disposal Procedure
	• In the event that records of PHI or certain categories of records of PHI will be securely disposed of by a designated agent, who is not a third party service provider, the policy and procedures must:	89	✓	
	• identify the designated agent responsible for securely disposing of the records of PHI	89	✓	Enterprise Information Security Policy; Operational Security Standard; Digital Media Disposal Standard; Digital Media Disposal Procedure; Services Agreement - Schedules for Third Party Agreements; Information Classification and Handling Standard; Information Classification and Handling Guideline (Draft); Privacy Policy; Hard-Copy PHI Disposal Procedure
	• identify the responsibilities of the designated agent in securely disposing of the records	89	✓	Enterprise Information Security Policy; Operational Security Standard;-Digital Media Disposal Standard; Digital Media Disposal Procedure; Services Agreement - Schedules for Third Party Agreements; Information Classification and Handling Standard; Information Classification and Handling Guideline (Draft); Privacy Policy; Hard-Copy PHI Disposal Procedure
	• identify the time frame within which, the circumstances in which and the conditions pursuant to which the	89	✓	Enterprise Information Security Policy; Operational Security Standard; Digital Media Disposal Standard; Digital Media Disposal Procedure; Services Agreement - Schedules for Third Party

	records of PHI must be securely disposed of			Agreements; Information Classification and Handling Standard; Information Classification and Handling Guideline (Draft); Privacy Policy; Hard-Copy PHI Disposal Procedure
	• require the designated agent to provide a certificate of destruction: identifying the records of PHI to be securely disposed of; confirming the secure disposal of the records of PHI; setting out the date, time and method of secure disposal employed; and bearing the name and signature of the agent(s) who performed the secure disposal	89	✓	Digital Media Disposal Standard; Digital Media Disposal Procedure; Services Agreement - Schedules for Third Party Agreements; Hard-Copy PHI Disposal Procedure
	• address the time frame within which and the agent(s) to whom certificates of destruction must be provided following the secure disposal of the records of PHI	89	✓	Digital Media Disposal Standard; Digital Media Disposal Procedure; Hard-Copy PHI Disposal Procedure
	• In the event that records of PHI or certain categories of records of PHI will be securely disposed of by an agent that is a third party service provider, the policy and procedures must detail the procedure to be followed by CCO in securely transferring the	89	✓	Digital Media Disposal Standard; Digital Media Disposal Procedure; Services Agreement - Schedules for Third Party Agreements; Hard-Copy PHI Disposal Procedure

	records of PHI to the third party service provider for secure disposal			
	• At a minimum, the policy and procedures must identify the secure manner in which the records of PHI will be transferred to the third party service provider	90	✓	Digital Media Disposal Standard; Digital Media Disposal Procedure; Services Agreement - Schedules for Third Party Agreements; Hard-Copy PHI Disposal Procedure
	• identify the conditions pursuant to which the records will be transferred	90	✓	Digital Media Disposal Standard; Digital Media Disposal Procedure; Services Agreement - Schedules for Third Party Agreements; Hard-Copy PHI Disposal Procedure
	• identify the agent(s) responsible for ensuring the secure transfer of records	90	✓	Digital Media Disposal Standard; Digital Media Disposal Procedure; Services Agreement - Schedules for Third Party Agreements; Hard-Copy PHI Disposal Procedure
	• In this regard, the policy and procedures shall comply with the Policy and Procedures for Secure Transfer of Records of Personal Health Information.	90	✓	Digital Media Disposal Standard; Digital Media Disposal Procedure; Services Agreement - Schedules for Third Party Agreements; Hard-Copy PHI Disposal Procedure
	• require the agent(s) responsible for ensuring the secure transfer of records of PHI to document the date, time and mode of transfer of the records of PHI	90	✓	Digital Media Disposal Standard; Digital Media Disposal Procedure; Services Agreement - Schedules for Third Party Agreements; Hard-Copy PHI Disposal Procedure

	• require the agent(s) responsible for ensuring the secure transfer of records of PHI to maintain a repository of written confirmations received from the third party service provider evidencing receipt of the records of personal health information	90	✓	Digital Media Disposal Standard; Digital Media Disposal Procedure; Services Agreement - Schedules for Third Party Agreements; Hard-Copy PHI Disposal Procedure
	• maintain a detailed inventory related to the records of PHI transferred to the third party service provider for secure disposal	90	✓	Digital Media Disposal Standard; Digital Media Disposal Procedure; Services Agreement - Schedules for Third Party Agreements; Hard-Copy PHI Disposal Procedure
	• the policy and procedures must identify the agent(s) responsible for maintaining this inventory	90	✓	Digital Media Disposal Standard; Digital Media Disposal Procedure; Services Agreement - Schedules for Third Party Agreements; Hard-Copy PHI Disposal Procedure
	• where a third party service provider is retained to securely dispose of records of personal health information, the policy and procedures must require that a written agreement be executed with the third party service provider containing the relevant language from the Template Agreement For All Third Party Service Providers	90	✓	Digital Media Disposal Standard; Digital Media Disposal Procedure; Services Agreement - Schedules for Third Party Agreements; Hard-Copy PHI Disposal Procedure; Data Use & Disclosure Standard; Privacy Policy; Information Classification and Handling Standard

	• identify the agent(s) responsible for ensuring that the agreement has been executed prior to the transfer of records of PHI for secure disposal	90	✓	Digital Media Disposal Standard; Digital Media Disposal Procedure; Services Agreement - Schedules for Third Party Agreements; Hard-Copy PHI Disposal Procedure; Data Use & Disclosure Standard; Privacy Policy; Information Classification and Handling Standard
	• outline the procedure to be followed in tracking:	90	✓	
	• tracking the dates that records of PHI are transferred for secure disposal	90	✓	Digital Media Disposal Standard; Digital Media Disposal Procedure; Services Agreement - Schedules for Third Party Agreements; Hard-Copy PHI Disposal Procedure
	• tracking the dates that certificates of destruction are received, whether from the third party service provider or from the designated agent that is not a third party service provider	90	✓	Digital Media Disposal Standard; Digital Media Disposal Procedure; Services Agreement - Schedules for Third Party Agreements; Hard-Copy PHI Disposal Procedure
	• the agent(s) responsible for conducting such tracking	90	✓	Digital Media Disposal Standard; Digital Media Disposal Procedure; Services Agreement - Schedules for Third Party Agreements; Hard-Copy PHI Disposal Procedure
	• outline the process to be followed where a certificate of destruction is not received within the time set out in the policy and its procedures or within the time set out in the agreement with the	90	✓	Digital Media Disposal Standard; Digital Media Disposal Procedure; Services Agreement - Schedules for Third Party Agreements; Hard-Copy PHI Disposal Procedure; Data Use & Disclosure Standard;

	third party service provider and the agent(s) responsible for implementing this process			
	• outline the agent(s) responsible for implementing this process	90	✓	Digital Media Disposal Standard; Digital Media Disposal Procedure; Services Agreement - Schedules for Third Party Agreements; Hard-Copy PHI Disposal Procedure; Data Use & Disclosure Standard;
	• address where certificates of destruction will be retained and the agent(s) responsible for retaining the certificates of destruction	90	✓	Digital Media Disposal Standard; Digital Media Disposal Procedure; Hard-Copy PHI Disposal Procedure
	• require agents to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach.	90	✓	Enterprise Information Security Policy; Privacy Policy; Services Agreement - Schedules for Third Party Agreements; Hard-Copy PHI Disposal Procedure; Security Audit, Testing and Compliance Standard; Privacy Audit and Compliance Policy;
	• stipulate that compliance will be audited in accordance with the Policy and Procedures In Respect of Security Audits	90	✓	Enterprise Information Security Policy; Privacy Policy; Digital Media Disposal Procedure; Services Agreement - Schedules for Third Party Agreements; Security Audit, Testing and Compliance Standard; Privacy Audit and Compliance Policy;
	• must set out the frequency with which the policy and procedures will be audited	90	✓	Enterprise Information Security Policy; Privacy Policy; Digital Media Disposal Procedure; Services Agreement - Schedules for Third Party Agreements; Security Audit, Testing and Compliance Standard; Privacy Audit and Compliance Policy;

	• must identify the agent(s) responsible for conducting the audit	90	✓	Enterprise Information Security Policy; Privacy Policy; Digital Media Disposal Procedure; Services Agreement - Schedules for Third Party Agreements; Security Audit, Testing and Compliance Standard; Privacy Audit and Compliance Policy;
	• must identify the agent(s) responsible for ensuring compliance with the policy and its procedures	90	✓	Enterprise Information Security Policy; Privacy Policy; Digital Media Disposal Procedure; Services Agreement - Schedules for Third Party Agreements; Security Audit, Testing and Compliance Standard; Privacy Audit and Compliance Policy
	• require agents to notify CCO at the first reasonable opportunity, in accordance with the Policy and Procedures for Information Security Breach Management, if an agent breaches or believes there may have been a breach of this policy or its procedures	91	✓	Enterprise Information Security Policy; Privacy Policy; Services Agreement - Schedules for Third Party Agreements; Privacy Breach Management Policy; Information Security Code of Conduct and Acceptable Use Policy
9	**Policy and procedures relating to passwords**			
	• A policy and procedures must be developed and implemented with respect to passwords for authentication and passwords for access to information systems, technologies, equipment, resources, applications and programs regardless of whether they are owned, leased or operated by CCO	91	✓	Logical Access Control Standard

	• identify the required minimum and maximum length of the password, the standard mandated for password composition and any other restrictions imposed on passwords	91	✓	Logical Access Control Standard
	• the frequency with which passwords must be changed, the consequences arising from a defined number of failed log-in attempts and the imposition of a mandatory system-wide password-protected screen saver after a defined period of inactivity	91	✓	Logical Access Control Standard
	• address the time frame within which passwords will automatically expire	91	✓	Logical Access Control Standard
	• identify the administrative, technical and physical safeguards that must be implemented by agents in respect of passwords	91	✓	Logical Access Control Standard
	• ensure that the policy and procedures it has developed in this regard, are consistent with:	91		
	• any orders, factsheets, and guidelines issued by the IPC	91	✓	Enterprise Information Security Policy
	• with evolving privacy and security standards and best practices	91	✓	Enterprise Information Security Policy
	• require agents to comply with the policy and its procedures and address how and by whom compliance will be enforced and the consequences of breach.	91	✓	Enterprise Information Security Policy; Information Security Code of Conduct and Acceptable Use Policy

	• stipulate that compliance will be audited	91	✓	Enterprise Information Security Policy; Logical Access Control Standard; Logging, Monitoring, and Auditing Standard
	• require agents to notify CCO if an agent believes there may have been a breach of this policy or its procedures.	92	✓	Enterprise Information Security Policy
10	**Policy and procedures for maintaining and reviewing system control and audit logs**			
	• A policy and procedures must be developed and implemented for the creation, maintenance and ongoing review of system control and audit logs.	92	✓	Logging, Monitoring, and Auditing Standard
	• must be conisistant with evolving industry standards	92	✓	Logging, Monitoring, and Auditing Standard
	• must be conisistant with the number and nature of agents with access to PHI and with the threats and risks associated with the PHI	92	✓	Logging, Monitoring, and Auditing Standard
	• require CCO to ensure that all information systems involving PHI have the functionality to log access, use, modification and disclosure of PHI	92	✓	Logging, Monitoring, and Auditing Standard
	• set out the types of events that are required to be audited and the nature and scope of the information that must be contained in system control and audit logs	92	✓	Logging, Monitoring, and Auditing Standard

	• identify the agent(s) responsible for ensuring that the types of events that are required to be audited are in fact audited and that the nature and scope of the information that is required to be contained in system control and audit logs is in fact logged	92	✓	Logging, Monitoring, and Auditing Standard
	• CCO must be required to ensure that the system control and audit logs cannot be accessed by unauthorized persons or amended or deleted in any way	92	✓	Logging, Monitoring, and Auditing Standard
	• the system control and audit logs set out:	92		
	• the date and time that PHI is accessed	92	✓	Logging, Monitoring, and Auditing Standard
	• the date and time of the disconnection	92	✓	Logging, Monitoring, and Auditing Standard
	• the nature of the disconnection	92	✓	Logging, Monitoring, and Auditing Standard
	• the name of the user accessing PHI	92	✓	Logging, Monitoring, and Auditing Standard
	• the network name or identification of the computer through which the connection is made	92	✓	Logging, Monitoring, and Auditing Standard
	• the operations or actions that create, amend, delete or retrieve PHI	92	✓	Logging, Monitoring, and Auditing Standard
	• the policy and procedure will:	92		
	• identify the length of time that system control and audit logs are required to be retained	92	✓	Logging, Monitoring, and Auditing Standard
	• the agent(s) responsible for retaining	92	✓	Logging, Monitoring, and Auditing Standard

	the system control and audit logs			
	• where the system control and audit logs will be retained	92	✓	Logging, Monitoring, and Auditing Standard
	• address the review of system control and audit logs including:	93	✓	Logging, Monitoring, and Auditing Standard
	• the agent(s) responsible for reviewing the system control and audit logs	93	✓	Logging, Monitoring, and Auditing Standard
	• the frequency with which and the circumstances in which system control and audit logs are required to be reviewed	93	✓	Logging, Monitoring, and Auditing Standard
	• the process to be followed in conducting the review.	93	✓	Logging, Monitoring, and Auditing Standard
	• The agent(s) responsible for reviewing system control and audit logs shall be required to notify CCO of a privacy/security breach	93	✓	Enterprise Information Security Policy; Logging, Monitoring, and Auditing Standard
	• address the findings arising from the review of system control and audit logs	93	✓	Logging, Monitoring, and Auditing Standard
	• addresses the agent(s) responsible for assigning other agent(s) to address the findings arising from the review of system control and audit logs, for establishing timelines to address the findings , for addressing the findings and for montitoring and ensuring that the findngs have been addressed	93	✓	Incident Management Framework; Logging, Monitoring, and Auditing Standard
	• the policy and procedure will set out :	93		

	• the nature of the documentation following the review of system control and audit logs	93	✓	Logging, Monitoring, and Auditing Standard
	• the agent(s) responsible for completing, providing and/or executing the documentation	93	✓	Logging, Monitoring, and Auditing Standard
	• the agent(s) to whom the documentation must be provided	93	✓	Logging, Monitoring, and Auditing Standard
	• the time frame within which the documentation must be provided	93	✓	Logging, Monitoring, and Auditing Standard
	• the required content of the documentation	93	✓	Logging, Monitoring, and Auditing Standard
	• communicating and addressing the findings of the review including the agent(s) responsible for communicating the findings of the review of system control and audit logs; the mechanism and format for communicating the findings of the review; the time frame within which the findings of the review must be communicated; and to whom the findings of the review must be communicated	93	✓	Incident Management Framework
	• tracking the findings of the review of system control and audit logs	93	✓	Logging, Monitoring, and Auditing Standard
	• require agents to comply with the policy and its procedures and address how and by whom compliance will be	93	✓	Enterprise Information Security Policy; Information Security Code of Conduct and Acceptable Use Policy

	enforced and the consequences of breach			
	• stipulate that compliance will be audited	93	✓	Enterprise Information Security Policy; Logging, Monitoring, and Auditing Standard
	• notify CCO if an agent believes there may have been a breach of this policy or its procedures.	93-94	✓	Enterprise Information Security Policy
11	**Policy and procedure for patch management**			
	• A policy and procedures must be developed and implemented for patch management	94	✓	Operational Security Standard; Operational Security - Patch Management Standard; Operational Security - Patching Procedure
	• identify the agent(s) responsible for monitoring the availability of patches on behalf of CCO	94	✓	Operational Security Standard; Operational Security - Patch Management Standard; Operational Security - Patching Procedure
	• identify the frequency with which such monitoring must be conducted	94	✓	Operational Security Standard; Operational Security - Patch Management Standard; Operational Security - Patching Procedure
	• identify the procedure that must be followed in this regard	94	✓	Operational Security Standard; Operational Security - Patch Management Standard; Operational Security - Patching Procedure
	• ~~identify~~ the agent(s) responsible for analyzing the patch and making a determination as to whether or not the patch should be implemented must be identified	94	✓	Operational Security Standard; Operational Security - Patch Management Standard; Operational Security - Patching Procedure
	• discuss the process that must be followed	94	✓	Operational Security Standard; Operational Security - Patch Management Standard; Operational Security - Patching Procedure
	• discuss the criteria that must be considered by the agent(s) responsible for undertaking this analysis and making this determination	94	✓	Operational Security Standard; Operational Security - Patch Management Standard; Operational Security - Patching Procedure

	• in circumstances where a determination is made that the patch should not be implemented, the policy and procedures shall require the responsible agent(s) to document:	94	✓	Operational Security Standard; Operational Security - Patch Management Standard; Operational Security - Patching Procedure
	• the description of the patch	94	✓	Operational Security Standard; Operational Security - Patch Management Standard; Operational Security - Patching Procedure
	• the date that the patch became available	94	✓	Operational Security Standard; Operational Security - Patch Management Standard; Operational Security - Patching Procedure
	• the severity level of the patch	94	✓	Operational Security Standard; Operational Security - Patch Management Standard; Operational Security - Patching Procedure
	• the information system, technology, equipment, resource, application or program to which the patch relates	94	✓	Operational Security Standard; Operational Security - Patch Management Standard; Operational Security - Patching Procedure
	• the rationale for the determination that the patch should not be implemented	94	✓	Operational Security Standard; Operational Security - Patch Management Standard; Operational Security - Patching Procedure
	• in circumstances where a determination is made that the patch should be implemented, the policy and procedures shall identify the agent(s) responsible for determining the time frame for implementation of the patch, and the priority of the patch.	94	✓	Operational Security Standard; Operational Security - Patch Management Standard; Operational Security - Patching Procedure
	• set out the criteria upon which these determinations are to be made	94	✓	Operational Security Standard; Operational Security - Patch Management Standard; Operational Security - Patching Procedure

	• set out the process by which these determinations are to be made	94	✓	Operational Security Standard; Operational Security - Patch Management Standard; Operational Security - Patching Procedure
	• set out the documentation that must be completed, provided and/or executed in this regard	94	✓	Operational Security Standard; Operational Security - Patch Management Standard; Operational Security - Patching Procedure
	• set out the process for patch implementation	94	✓	Operational Security Standard; Operational Security - Patch Management Standard; Operational Security - Patching Procedure
	• the agent(s) responsible for patch implementation	94	✓	Operational Security Standard; Operational Security - Patch Management Standard; Operational Security - Patching Procedure
	• any documentation that must be completed, provided and/or executed by the agent(s) responsible for patch implementation	94	✓	Operational Security Standard; Operational Security - Patch Management Standard; Operational Security - Patching Procedure
	• the policy and procedures shall address:	94		
	• the circumstances in which patches must be tested	94	✓	Operational Security Standard; Operational Security - Patch Management Standard; Operational Security - Patching Procedure
	• the time frame within which patches must be tested	94	✓	Operational Security Standard; Operational Security - Patch Management Standard; Operational Security - Patching Procedure
	• the procedure for testing	94	✓	Operational Security Standard,; Operational Security - Patch Management Standard; Operational Security Patching Procedure
	• the agent(s) responsible for testing	94	✓	Operational Security Standard,; Operational Security - Patch Management Standard; Operational Security Patching Procedure
	• the documentation that must be completed, provided and/or executed by the	94	✓	Operational Security Standard,; Operational Security - Patch Management Standard; Operational Security Patching Procedure

	agent(s) responsible for testing			
	• the policy and procedures must also require documentation to be maintained in respect of patches that have been implemented and must identify the agent(s) responsible for maintaining this documentation. At a minimum, the documentation must include:	94	✓	Operational Security Standard; Operational Security - Patch Management Standard; Operational Security - Patching Procedure
	• a description of the patch	94	✓	Operational Security Standard; Operational Security - Patch Management Standard; Operational Security - Patching Procedure
	• the date that the patch became available	94	✓	Operational Security Standard; Operational Security - Patch Management Standard; Operational Security - Patching Procedure
	• the severity level and priority of the patch	94	✓	Operational Security Standard; Operational Security - Patch Management Standard; Operational Security - Patching Procedure
	• the information system, technology, equipment, resource, application or program to which the patch relates	94	✓	Operational Security Standard; Operational Security - Patch Management Standard; Operational Security - Patching Procedure
	• the date that the patch was implemented	94	✓	Operational Security Standard; Operational Security - Patch Management Standard; Operational Security - Patching Procedure
	• the agent(s) responsible for implementing the patch	94	✓	Operational Security Standard; Operational Security - Patch Management Standard; Operational Security - Patching Procedure
	• the date, if any, when the patch was tested	95	✓	Operational Security Standard; Operational Security - Patch Management Standard; Operational Security - Patching Procedure

	• the agent(s) responsible for testing	95	✓	Operational Security Standard; Operational Security - Patch Management Standard; Operational Security - Patching Procedure
	• whether or not the testing was successful	95	✓	Operational Security Standard; Operational Security - Patch Management Standard; Operational Security - Patching Procedure
	• CCO must require agents to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach.	95	✓	Enterprise Information Security Policy; Information Security Code of Conduct and Acceptable Use Policy
	• the policy and procedures must also stipulate that compliance will be audited in accordance with the Policy and Procedures In Respect of Security Audits	95	✓	Operational Security Standard; Enterprise Information Security Policy; Security Audit, Testing and Compliance Standard;
	• must set out the frequency with which the policy and procedures will be audited	95	✓	Operational Security Standard; Enterprise Information Security Policy; Security Audit, Testing and Compliance Standard;
	• must identify the agent(s) responsible for conducting the audit and for ensuring compliance with the policy and its procedures	95	✓	Operational Security Standard; Enterprise Information Security Policy; Security Audit, Testing and Compliance Standard;
	• the policy and procedures must also require agents to notify CCO at the first reasonable opportunity, in accordance with the Policy and Procedures for Information Security Breach Management, if an agent breaches or believes there may have	95	✓	Enterprise Information Security Policy; Information Security Code of Conduct and Acceptable Use Policy

	been a breach of this policy or its procedures.			
12	**Policy and procedures related to change management**			
	• A policy and procedures must be developed and implemented for determining the approval or denial of a request for a change to the operational environment of CCO	95	✓	Enterprise Information Security Policy; Change Management Policy; IT Change Subcommittee Terms of Reference
	• identify the agent(s) responsible and the process that must be followed for making this determination	95	✓	Enterprise Information Security Policy; Change Management Policy; IT Change Subcommittee Terms of Reference
	• identify the criteria that must be considered when deciding to approve or deny a request for a change to the operational environment	95	✓	Enterprise Information Security Policy; Change Management Policy; IT Change Subcommittee Terms of Reference
	• the policy and procedure will:	95		
	• set out the manner in which the decision approving or denying the request for a change to the operational environment	95	✓	Enterprise Information Security Policy; Change Management Policy; IT Change Subcommittee Terms of Reference
	• document the the reasons for the decision	95	✓	Enterprise Information Security Policy; Change Management Policy; IT Change Subcommittee Terms of Reference
	• set out the method and the format in which the decision will be communicated	95	✓	Enterprise Information Security Policy; Change Management Policy; IT Change Subcommittee Terms of Reference
	• set out to whom the decision will be communicated	95	✓	Enterprise Information Security Policy; Change Management Policy; IT Change Subcommittee Terms of Reference

	• where a request for change to the operational environment is not approved, it is required to:	95		
	• document the change to the operational environment requested	95	✓	Enterprise Information Security Policy; Change Management Policy; IT Change Subcommittee Terms of Reference
	• the name of the agent requesting the change	95	✓	Enterprise Information Security Policy; Change Management Policy; IT Change Subcommittee Terms of Reference
	• the date that the change was requested	95	✓	Enterprise Information Security Policy; Change Management Policy; IT Change Subcommittee Terms of Reference
	• the rationale for the determination that the change should not be implemented	95	✓	Enterprise Information Security Policy; Change Management Policy; IT Change Subcommittee Terms of Reference
	• where a request for change to the operational environment is approved, the responsible agent is required to:	96		
	• determine the time frame for implementing the change	96	✓	Enterprise Information Security Policy; Change Management Policy; IT Change Subcommittee Terms of Reference
	• the priority assigned to the change requested	96	✓	Enterprise Information Security Policy; Change Management Policy; IT Change Subcommittee Terms of Reference
	• the policy and procedure will:	96		
	• set out the criteria upon which these determinations are to be made	96	✓	Enterprise Information Security Policy; Change Management Policy; IT Change Subcommittee Terms of Reference
	• the process by which these determinations are to be made	96	✓	Enterprise Information Security Policy; Change Management Policy; IT Change Subcommittee Terms of Reference

	• any documentation that must be completed, provided and/or executed in this regard	96	✓	Enterprise Information Security Policy; Change Management Policy; IT Change Subcommittee Terms of Reference
	• the process for implementation of the change to the operational environment	96	✓	Enterprise Information Security Policy; Change Management Policy; IT Change Subcommittee Terms of Reference
	• the agent(s) responsible for implementation	96	✓	Enterprise Information Security Policy; Change Management Policy; IT Change Subcommittee Terms of Reference
	• any documentation that must be completed, provided and/or executed by the agent(s) responsible for implementation.	96	✓	Enterprise Information Security Policy; Change Management Policy; IT Change Subcommittee Terms of Reference
	• identify the circumstances in which changes to the operational environment must be tested	96	✓	Enterprise Information Security Policy; Change Management Policy; IT Change Subcommittee Terms of Reference
	• the time frame within which changes must be tested	96	✓	Enterprise Information Security Policy; Change Management Policy; IT Change Subcommittee Terms of Reference
	• the procedure for testing	96	✓	Enterprise Information Security Policy; Change Management Policy; IT Change Subcommittee Terms of Reference
	• the agent(s) responsible for testing	96	✓	Enterprise Information Security Policy; Change Management Policy; IT Change Subcommittee Terms of Reference
	• the documentation that must be completed, provided and/or executed by the agent(s) responsible for testing.	96	✓	Enterprise Information Security Policy; Change Management Policy; IT Change Subcommittee Terms of Reference
	• require documentation to be maintained of changes	96	✓	Enterprise Information Security Policy; Change Management Policy; IT

	that have been implemented			Change Subcommittee Terms of Reference
	• identify the agent(s) responsible for maintaining this documentation	96	✓	Enterprise Information Security Policy; Change Management Policy; IT Change Subcommittee Terms of Reference
	• compliance with the policy and its procedures and how compliance will be enforced and the consequences of breach.	96	✓	Enterprise Information Security Policy; Change Management Policy; IT Change Subcommittee Terms of Reference
	• stipulate that compliance will be audited	96	✓	Enterprise Information Security Policy; Change Management Policy; IT Change Subcommittee Terms of Reference
	• require agents to notify CCO if an agent believes there may have been a breach of this policy or its procedures.	96	✓	Enterprise Information Security Policy; Change Management Policy; IT Change Subcommittee Terms of Reference
13	**Policy and procedures for back-up and recovery of records of PHI**			
	• A policy and procedures must be developed and implemented for the back-up and recovery of records of PHI	96	✓	Data Backup Policy; Data Backup Procedure
	• The policy will:	97		
	• identify the nature and types of back-up storage devices maintained by CCO	97	✓	Data Backup Policy; Data Backup Procedure
	• the frequency with which records of PHI are backed-up	97	✓	Data Backup Policy; Data Backup Procedure
	• the agent(s) responsible for the back-up and recovery of records of PHI	97	✓	Data Backup Policy; Data Backup Procedure

	• the process that must be followed and the requirements that must be satisfied in this regard	97	✓	Data Backup Policy; Data Backup Procedure
	• specify the documentation that must be completed, provided and/or executed for the back-up and recovery of records of PHI; the agent (s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation	97	✓	Data Backup Policy; Data Backup Procedure
	• address testing the procedure for back-up and recovery of records of PHI	97	✓	Data Backup Policy; Data Backup Procedure
	• the agent(s) responsible for testing	97	✓	Data Backup Policy; Data Backup Procedure
	• the frequency with which the procedure is tested	97	✓	Data Backup Policy; Data Backup Procedure
	• the process that must be followed in conducting such testing	97	✓	Data Backup Policy; Data Backup Procedure
	• identify the agent(s) responsible for ensuring that back-up storage devices containing records of PHI are retained in a secure manner,	97	✓	Data Backup Policy; Data Backup Procedure

	• the location where they are required to be retained and the length of time that they are required to be retained	97	✓	Data Backup Policy; Data Backup Procedure
	• require that the backed-up records of PHI must be retained in compliance with the Policy and Procedure for Secure Retention of Records of PHI and identify the agent(s) responsible for ensuring they are retained in a secure manner	97	✓	Data Backup Policy; Data Backup Procedure
	• if a third party service provider is contracted to retain backed-up records of PHI, the policy and associated procedures must:	97		
	• require the backed-up records of PHI to be transferred in a secure manner	97	✓	Services Agreement - Schedules for Third Party Agreements; Data Backup Policy; Data Backup Procedure; HP Data Protectors Session Logs; Open Media Logs;

	•detail the procedure to be followed in:	97		
	• securely transferring the backed-up records of PHI to the third party	97	✓	Services Agreement - Schedules for Third Party Agreements; Data Backup Policy; Data Backup Procedure
	• securely retrieving the backed-up records from the third party	97	✓	Services Agreement - Schedules for Third Party Agreements; Data Backup Policy; Data Backup Procedure
	• ensuring the secure transfer and retrieval of the backed-up records	97	✓	Services Agreement - Schedules for Third Party Agreements; Data Backup Policy; Data Backup Procedure
	• address the documentation that is required to be maintained in relation to the transfer of backed-up records of PHI	97	✓	Services Agreement - Schedules for Third Party Agreements; Data Backup Policy; Data Backup Procedure
	• the secure transfer shall document the date, time and mode of transfer	97	✓	Services Agreement - Schedules for Third Party Agreements; Data Backup Policy; Data Backup Procedure; HP Data Protectors Session Logs; Open Media Logs;

	• maintain a repository of written confirmations received from the third party upon receipt of the backed-up records of PHI	97	✓	Services Agreement - Schedules for Third Party Agreements; Data Backup Policy; Data Backup Procedure; HP Data Protectors Session Logs; Open Media Logs;
	• execute a written agreement with the third party	97	✓	Services Agreement - Schedules for Third Party Agreements; Information Classification and Handling Standard
	• identify the agent(s) responsible for ensuring that the agreement has been executed prior to transferring the backed-up records of PHI to the third party	98	✓	Services Agreement - Schedules for Third Party Agreements; Information Classification and Handling Standard
	• address the need for the availability of backed-up records of PHI	98	✓	Data Backup Policy ;
	• require agents to comply with the policy and its procedures and address how and by whom compliance will be enforced and the consequences of breach.	98	✓	Enterprise Information Security Policy; Data Backup Policy
	• stipulate that compliance will be audited	98	✓	Enterprise Information Security Policy; Data Backup Policy
	• agents to notify CCO if an agent believes there may have been a breach of this policy or its procedures.	98	✓	Enterprise Information Security Policy ;
14	**Policy and procedures on the acceptable use of technology**			
	• A policy and procedures must be developed and implemented outlining the acceptable use of information systems, technologies, equipment, resources, applications and programs regardless of whether they are owned, leased or	98	✓	Enterprise Information Security Policy; Information Security Code of Conduct and Acceptable Use Policy; Acceptable Use of Social Media Policy

	operated by the prescribed person or prescribed entity			
	• sets out the uses that are prohibited without exception, the uses that are permitted without exception, and the uses that are permitted only with prior approval	98	✓	Enterprise Information Security Policy; Information Security Code of Conduct and Acceptable Use Policy; Acceptable use of social media Policy
	• For those uses that are permitted only with prior approval, the policy and procedures must identify the agent(s) responsible for receiving, reviewing and determining whether to approve or deny the request and the process that must be followed and the requirements that must be satisfied in this regard.	98	✓	Enterprise Information Security Policy; Information Security Code of Conduct and Acceptable Use Policy; Acceptable use of social media policy.
	•the criteria that must be conisdered by the agent(s) responsible for determining whether to approve or deny the request	98	✓	Enterprise Information Security Policy; Information Security Code of Conduct and Acceptable Use Policy; Acceptable use of social media policy.
	• identify the conditions or restrictions with which agents granted approval must comply.	98	✓	Enterprise Information Security Policy; Information Security Code of Conduct and Acceptable Use Policy; Acceptable use of social media policy.
	• the policy and procedures should:	98		
	• set out the manner in which the decision approving or denying the request	98	✓	Enterprise Information Security Policy; Information Security Code of Conduct and Acceptable Use Policy; Acceptable use of social media policy.
	• the reasons for the decision are documented	98	✓	Enterprise Information Security Policy; Information Security Code of Conduct and Acceptable Use Policy; Acceptable use of social media policy.

	• the method by which and the format in which the decision will be communicated	98	✓	Enterprise Information Security Policy; Information Security Code of Conduct and Acceptable Use Policy; Acceptable use of social media policy.
	• whom the decision will be communicated.	99	✓	Enterprise Information Security Policy; Information Security Code of Conduct and Acceptable Use Policy; Acceptable use of social media policy.
	•require agents to comply with the policy and its procedures and address how and by whom compliance will be enforced and the consequences of breach.	99	✓	Enterprise Information Security Policy; Information Security Code of Conduct and Acceptable Use Policy; Acceptable use of social media policy.
	• stipulate that compliance will be audited	99	✓	Enterprise Information Security Policy; Information Security Code of Conduct and Acceptable Use Policy; Acceptable use of social media policy; Logging, Monitoring, and Auditing Standard
	• require agents to notify CCO at the first reasonable opportunity, if an agent breaches or believes there may have been a breach of the Policy or its procedures	99	✓	Enterprise Information Security Policy ;
15	**Policy and procedures in respect of security audits**			
	• A policy and procedures must be developed and implemented that sets out the types of security audits that are required to be conducted	99	✓	Security Audit, Testing and Compliance Standard; Security Risk Management Standard; Operational Security Standard
	• the audits required to be conducted shall include:	99		

	• audits to assess compliance with the security policies, procedures and practices implemented by CCO	99	✓	Security Audit, Testing and Compliance Standard; Security Risk Management Standard; Operational Security Standard
	• threat and risk assessments	99	✓	Security Audit, Testing and Compliance Standard; Security Risk Management Standard; Operational Security Standard
	• security reviews or assessments	99	✓	Security Audit, Testing and Compliance Standard; Security Risk Management Standard; Operational Security Standard
	• vulnerability assessments	99	✓	Security Audit, Testing and Compliance Standard; Security Risk Management Standard; Operational Security Standard
	• penetration testing	99	✓	Security Audit, Testing and Compliance Standard; Security Risk Management Standard; Operational Security Standard
	• ethical hacks and reviews of system control and audit logs	99	✓	Security Audit, Testing and Compliance Standard; Security Risk Management Standard; Operational Security Standard
	• The policy and procedure must set out:	99		Security Audit, Testing and Compliance Standard; Security Risk Management Standard; Operational Security Standard
	• the purposes of the security audit	99	✓	Security Audit, Testing and Compliance Standard; Security Risk Management Standard; Operational Security Standard

	• the nature and scope of the security audit	99	✓	Security Audit, Testing and Compliance Standard; Security Risk Management Standard; Operational Security Standard
	• the agent(s) responsible for conducting the security audit	99	✓	Security Audit, Testing and Compliance Standard; Security Risk Management Standard; Operational Security Standard
	• the frequency with which and the circumstances in which each security audit is required to be conducted.	99	✓	Security Audit, Testing and Compliance Standard; Security Risk Management Standard; Operational Security Standard
	• set out the process to be followed in conducting the audit	99	✓	Security Audit, Testing and Compliance Standard; Security Risk Management Standard; Operational Security Standard
	• discuss the documentation that must be gathered for each security audit	99	✓	Security Audit, Testing and Compliance Standard; Security Risk Management Standard; Operational Security Standard
	• the agent(s) responsible for completing, providing and/or executing the documentation	99	✓	Security Audit, Testing and Compliance Standard; Security Risk Management Standard; Operational Security Standard
	• the agent(s) to whom this documentation must be provided	99	✓	Security Audit, Testing and Compliance Standard; Security Risk Management Standard; Operational Security Standard
	• the required content of the documentation.	99	✓	Security Audit, Testing and Compliance Standard; Security Risk Management Standard; Operational Security Standard

	• the role of the agent(s) that have been delegated day-to-day authority to manage the privacy program and the security program	100	✓	Enterprise Information Security Policy; Privacy Policy
	• the process that must be followed in addressing the recommendations arising from security audits	100	✓	Security Audit, Testing and Compliance Standard; Security Risk Management Standard
	• the nature of the documentation that must be gathered at the conclusion of the security audit	100	✓	Security Audit, Testing and Compliance Standard; Security Risk Management Standard
	• the manner and format in which the findings and status of security audits are communicated	100	✓	Security Audit, Testing and Compliance Standard; Security Risk Management Standard
	• a log be maintained of security audits	100	✓	Security Audit, Testing and Compliance Standard; Security Risk Management Standard
	• the agent(s) responsible for maintaining the log	100	✓	Security Audit, Testing and Compliance Standard; Security Risk Management Standard
	• tracking that the recommendations arising from the security audits are addressed within the identified time frame	100	✓	Security Audit, Testing and Compliance Standard; Security Risk Management Standard
	• the agent(s) responsible for conducting the security audit to notify CCO at the first reasonable opportunity of an information security or privacy breach	100	✓	Security Audit, Testing and Compliance Standard; Security Risk Management Standard
	• address where documentation related to security audits will be retained and the agent(s) responsible for retaining this documentation.	100	✓	Security Audit, Testing and Compliance Standard; Security Risk Management Standard

16	**Log of security audits**			
	• maintain a log of security audits that have been completed. The log shall set out:	100		
	• the nature and type of the security audit conducted	100	✓	Security Risk Management Standard; Operational Security Standard; Information Security Program Framework; Log of Security Audits
	• the date that the security audit was completed	100	✓	Security Risk Management Standard; Operational Security Standard; Information Security Program Framework; Log of Security Audits
	• the agent(s) responsible for completing the security audit	100	✓	Security Risk Management Standard; Operational Security Standard; Information Security Program Framework; Log of Security Audits
	• the recommendations arising from the security audit	100	✓	Security Risk Management Standard; Operational Security Standard; Information Security Program Framework; Log of Security Audits

	• the agent(s) responsible for addressing each recommendation	100	✓	Security Risk Management Standard; Operational Security Standard; Information Security Program Framework; Log of Security Audits
	• the date that each recommendation was or is expected to be addressed	100	✓	Security Risk Management Standard; Operational Security Standard; Information Security Program Framework; Log of Security Audits
	• the manner in which each recommendation was or is expected to be addressed.	100	✓	Security Risk Management Standard; Operational Security Standard; Information Security Program Framework; Log of Security Audits
17	**Policy and procedures for information security breach management**			
	• A policy and procedures must be developed and implemented to address the identification, reporting, containment, notification, investigation and remediation of information security breaches and must provide a definition of the term “information security breach.”	101	✓	Incident Management Framework; Information Security Incident and Breach Response Standard; Enterprise Information Security Policy; Information Security Code of Conduct and Acceptable Use Policy
	• an information security breach shall be defined to include a contravention of the security policies, procedures or practices implemented by the prescribed person or prescribed entity	101	✓	Incident Management Framework; Information Security Incident and Breach Response Standard; Enterprise Information Security Policy
	• the policy and procedures shall impose a mandatory requirement on agents to notify CCO of an information security breach or suspected information security breach	101	✓	Incident Management Framework; Information Security Incident and Breach Response Standard; Enterprise Information Security Policy; Information Security Code of Conduct and Acceptable Use Policy
	• the policy and procedure shall:	101		

	• identify the agent(s) who must be notified of the information security breach or suspected breach	101	✓	Incident Management Framework; Information Security Incident and Breach Response Standard; Enterprise Information Security Policy; Information Security Code of Conduct and Acceptable Use Policy
	• provide contact information for the agent(s) who must be notified	101	✓	Incident Management Framework; Information Security Incident and Breach Response Standard; Enterprise Information Security Policy; Information Security Code of Conduct and Acceptable Use Policy
	• stipulate the time frame within which notification must be provided	101	✓	Incident Management Framework; Information Security Incident and Breach Response Standard; Enterprise Information Security Policy; Information Security Code of Conduct and Acceptable Use Policy
	• stipulate whether the notification must be provided verbally and/or in writing	101	✓	Incident Management Framework; Information Security Incident and Breach Response Standard; Enterprise Information Security Policy; Information Security Code of Conduct and Acceptable Use Policy
	• stipulate the nature of the information that must be provided upon notification.	101	✓	Incident Management Framework; Information Security Incident and Breach Response Standard; Enterprise Information Security Policy; Information Security Code of Conduct and Acceptable Use Policy
	• address the documentation that must be gathered completed, provided and/or executed with respect to notification	101	✓	Incident Management Framework; Information Security Incident and Breach Response Standard; Enterprise Information Security Policy; Information Security Code of Conduct and Acceptable Use Policy
	• address the agent(s) responsible for completing, providing and/or executing the documentation	101	✓	Incident Management Framework; Information Security Incident and Breach Response Standard; Enterprise Information Security Policy; Information Security Code of Conduct and Acceptable Use Policy

	• address the agent(s) to whom this documentation must be provided	101	✓	Incident Management Framework; Information Security Incident and Breach Response Standard; Enterprise Information Security Policy; Information Security Code of Conduct and Acceptable Use Policy
	• address the required content of the documentation	101	✓	Incident Management Framework; Information Security Incident and Breach Response Standard; Enterprise Information Security Policy; Information Security Code of Conduct and Acceptable Use Policy
	• upon notification, the policy and procedures shall require a determination to be made:	101		
	• whether an information security breach has in fact occurred	101	✓	Incident Management Framework; Information Security Incident and Breach Response Standard
	• if so, what if any PHI was has been breached	101	✓	Incident Management Framework; Information Security Incident and Breach Response Standard
	• of the extent of the information security breach	101	✓	Incident Management Framework; Information Security Incident and Breach Response Standard
	• whether the breach is an information security breach or privacy breach or both	101	✓	Incident Management Framework; Information Security Incident and Breach Response Standard
	• The agent(s) responsible for making these determinations must also be identified	101	✓	Incident Management Framework; Information Security Incident and Breach Response Standard
	• the policy and procedures must address the process to be followed where the breach is a privacy breach and as well as an information security breach	101	✓	Incident Management Framework; Information Security Incident and Breach Response Standard; Privacy Breach Management Policy
	• the policy and procedures must address the process to be followed when the breach is	101	✓	Incident Management Framework; Information Security Incident and Breach Response Standard; Privacy Breach Management Policy

	reported as an information security breach but is determined to be a privacy breach.			
	• the policy and procedures must address when senior management, including the Chief Executive Officer or the Executive Director, will be notified. This shall include:	101	✓	Incident Management Framework; Information Security Incident and Breach Response Standard
	• a discussion of the agent(s) responsible for notifying senior management	101	✓	Incident Management Framework; Information Security Incident and Breach Response Standard
	• the time frame within which notification must be provided	101	✓	Incident Management Framework; Information Security Incident and Breach Response Standard
	• the manner in which this notification must be provided	101	✓	Incident Management Framework; Information Security Incident and Breach Response Standard
	• the nature of the information that must be provided to senior management upon notification	101	✓	Incident Management Framework; Information Security Incident and Breach Response Standard
	• the policy and procedures:	101		
	• shall require that containment be initiated immediately	101	✓	Incident Management Framework; Information Security Incident and Breach Response Standard
	• shall identify the agent(s) responsible for containment	101	✓	Incident Management Framework; Information Security Incident and Breach Response Standard
	• shall identify the procedure that must be followed in this regard, including any documentation that must be completed, provided and/or executed by the agent(s) responsible for containing the breach and	101	✓	Incident Management Framework; Information Security Incident and Breach Response Standard

	the required content of the documentation			
	• in undertaking containment, the policy and procedures must ensure that reasonable steps are taken in the circumstances to ensure that additional information security breaches cannot occur through the same means.	101	✓	Incident Management Framework; Information Security Incident and Breach Response Standard
	• The agent(s) responsible and the process to be followed in reviewing the containment measures implemented and determining whether the information security breach has been effectively contained or whether further containment measures are necessary, must be identified in the policy and procedures. The policy and procedures shall also address:	102	✓	Incident Management Framework; Information Security Incident and Breach Response Standard
	• any documentation that must be completed, provided and/or executed by the agent(s) responsible for reviewing the containment measures	102	✓	Incident Management Framework; Information Security Incident and Breach Response Standard
	• the agent(s) to whom this documentation must be provided	102	✓	Incident Management Framework; Information Security Incident and Breach Response Standard
	• the required content of the documentation.	102	✓	Incident Management Framework; Information Security Incident and Breach Response Standard

	• the HIC or other organization that disclosed the PHI to CCO to be notified at the first reasonable opportunity whenever PHI is or is believed to be stolen, lost or accessed by unauthorized persons and whenever required pursuant to the agreement with the HIC or other organization. In particular, the policy and procedures shall set out:	102	✓	Incident Management Framework; Information Security Incident and Breach Response Standard; Enterprise Information Security Policy; Information Security Code of Conduct and Acceptable Use Policy; Privacy Policy; Privacy Breach Management Policy
	• the agent(s) responsible for notifying the HIC or other organization	102	✓	Incident Management Framework; Information Security Incident and Breach Response Standard; Enterprise Information Security Policy; Information Security Code of Conduct and Acceptable Use Policy; Privacy Policy; Privacy Breach Management Policy
	• the format of the notification	102	✓	Incident Management Framework; Information Security Incident and Breach Response Standard; Enterprise Information Security Policy; Information Security Code of Conduct and Acceptable Use Policy; Privacy Policy; Privacy Breach Management Policy
	• the nature of the information that will be provided upon notification	102	✓	Incident Management Framework; Information Security Incident and Breach Response Standard; Enterprise Information Security Policy; Information Security Code of Conduct and Acceptable Use Policy; Privacy Policy; Privacy Breach Management Policy
	• at a minimum, the policy and procedures must require the HIC or other organization to be advised of:	102	✓	Incident Management Framework; Information Security Incident and Breach Response Standard; Enterprise Information Security Policy; Information Security Code of Conduct and Acceptable Use Policy

	• the extent of the information security breach	102	✓	Incident Management Framework; Information Security Incident and Breach Response Standard; Enterprise Information Security Policy; Information Security Code of Conduct and Acceptable Use Policy
	• the nature of the PHI at issue, if any	102	✓	Incident Management Framework; Information Security Incident and Breach Response Standard; Enterprise Information Security Policy; Information Security Code of Conduct and Acceptable Use Policy; Privacy Policy; Privacy Breach Management Policy
	• the measures implemented to contain the information security breach	102	✓	Incident Management Framework; Information Security Incident and Breach Response Standard; Enterprise Information Security Policy; Information Security Code of Conduct and Acceptable Use Policy
	• further actions that will be undertaken with respect to the information security breach, including investigation and remediation	102	✓	Incident Management Framework; Information Security Incident and Breach Response Standard; Enterprise Information Security Policy; Information Security Code of Conduct and Acceptable Use Policy
	• the policy and procedures shall also set out:	102	✓	
	• whether any other persons or organizations must be notified of the information security breach	102	✓	Incident Management Framework; Information Security Incident and Breach Response Standard; Enterprise Information Security Policy
	• the agent(s) responsible for notifying the other persons or organizations	102	✓	Incident Management Framework; Information Security Incident and Breach Response Standard; Enterprise Information Security Policy
	• the format of the notification	102	✓	Incident Management Framework; Information Security Incident and Breach Response Standard; Enterprise Information Security Policy
	• the nature of the information that must be provided upon notification	102	✓	Incident Management Framework; Information Security Incident and

				Breach Response Standard; Enterprise Information Security Policy
	• the time frame for notification	102	✓	Incident Management Framework; Information Security Incident and Breach Response Standard; Enterprise Information Security Policy
	• the policy and procedures must further identify:	102	✓	
	• the agent(s) responsible for investigating the information security breach	102	✓	Incident Management Framework; Information Security Incident and Breach Response Standard; Enterprise Information Security Policy
	• the nature and scope of the investigation (i.e. document reviews, interviews, site visits, inspections)	102	✓	Incident Management Framework; Information Security Incident and Breach Response Standard
	• the process that must be followed in investigating the information security breach.	102	✓	Incident Management Framework; Information Security Incident and Breach Response Standard
	• this shall include a discussion of the documentation that must be completed, provided and/or executed in undertaking the investigation	102	✓	Incident Management Framework; Information Security Incident and Breach Response Standard
	• the agent(s) responsible for completing, providing and/or executing the documentation	102	✓	Incident Management Framework; Information Security Incident and Breach Response Standard
	• the agent(s) to whom this documentation must be provided	102	✓	Incident Management Framework; Information Security Incident and Breach Response Standard
	• the required content of the documentation	102	✓	Incident Management Framework; Information Security Incident and Breach Response Standard
	• the role of the agent(s) that have been delegated day-to-day authority to manage the privacy program and the security	102	✓	Privacy Policy; Enterprise Information Security Policy

	program shall also be identified			
	• the policy and procedures shall also identify the agent(s) responsible for:	102	✓	
	• assigning other agent(s) to address the recommendations	102	✓	Incident Management Framework; Information Security Incident and Breach Response Standard; Security Risk Management Standard
	• establishing timelines to address the recommendations	102	✓	Incident Management Framework; Information Security Incident and Breach Response Standard; Security Risk Management Standard
	• addressing the recommendations	102	✓	Incident Management Framework; Information Security Incident and Breach Response Standard; Security Risk Management Standard
	• monitoring and ensuring that the recommendations are implemented within the stated timelines	102	✓	Incident Management Framework; Information Security Incident and Breach Response Standard; Security Risk Management Standard
	• the policy and procedures shall also set out:	102	✓	
	• the nature of the documentation that must be completed, provided and/or executed at the conclusion of the investigation of the information security breach	102	✓	Incident Management Framework; Information Security Incident and Breach Response Standard
	• the agent(s) responsible for completing, providing and/or executing the documentation	102	✓	Incident Management Framework; Information Security Incident and Breach Response Standard
	• the agent(s) to whom this documentation must be provided	102	✓	Incident Management Framework; Information Security Incident and Breach Response Standard
	• the required content of the documentation	102	✓	Incident Management Framework; Information Security Incident and Breach Response Standard

	• the policy and procedures must also address the manner and format in which the findings of the investigation of the information security breach, including the recommendations arising from the investigation and the status of the implementation of the recommendations, are communicated. This shall include:	103	✓	Incident Management Framework; Information Security Incident and Breach Response Standard
	• a discussion of the agent(s) responsible for communicating the findings of the investigation	103	✓	Incident Management Framework; Information Security Incident and Breach Response Standard
	• the mechanism and format for communicating the findings of the investigation	103	✓	Incident Management Framework; Information Security Incident and Breach Response Standard
	• the time frame within which the findings of the investigation must be communicated	103	✓	Incident Management Framework; Information Security Incident and Breach Response Standard
	• to whom the findings of the investigation must be communicated, including the Chief Executive Officer or the Executive Director	103	✓	Incident Management Framework; Information Security Incident and Breach Response Standard
	• the policy and procedures must:	103	✓	
	• require that a log be maintained of information security breaches	103	✓	Incident Management Framework; Information Security Incident and Breach Response Standard
	• identify the agent(s) responsible for maintaining the log	103	✓	Incident Management Framework; Information Security Incident and Breach Response Standard
	• track that the recommendations arising from the investigation of	103	✓	Incident Management Framework; Information Security Incident and Breach Response Standard

	information security breaches are addressed within identified timelines			
	• address where documentation related to the identification, reporting, containment, notification, investigation and remediation of information security breaches will be retained	103	✓	Incident Management Framework; Information Security Incident and Breach Response Standard
	• address the agent(s) responsible for retaining this documentation.	103	✓	Incident Management Framework; Information Security Incident and Breach Response Standard
	• CCO must:	103	✓	
	• require agents to comply with the policy and its procedures	103	✓	Incident Management Framework; Information Security Incident and Breach Response Standard; Enterprise Information Security Policy; Information Security Code of Conduct and Acceptable Use Policy
	• address how and by whom compliance will be enforced	103	✓	Incident Management Framework; Information Security Incident and Breach Response Standard; Enterprise Information Security Policy; Information Security Code of Conduct and Acceptable Use Policy
	• the consequences of a breach	103	✓	Incident Management Framework; Information Security Incident and Breach Response Standard; Enterprise Information Security Policy; Information Security Code of Conduct and Acceptable Use Policy
	• the policy and procedures must:	103	✓	
	• stipulate that compliance will be audited in accordance with the Policy and Procedures In Respect of Security Audits	103	✓	Enterprise Information Security Policy; Security Audit, Testing and Compliance Standard
	• set out the frequency with which the policy and procedures will be audited	103	✓	Enterprise Information Security Policy; Security Audit, Testing and Compliance Standard

	• identify the agent(s) responsible for conducting the audit and for ensuring compliance with the policy and its procedures	103	✓	Enterprise Information Security Policy; Security Audit, Testing and Compliance Standard
18	**Log of information security breaches**			
	• CCO shall maintain a log of information security breaches setting out:	103		
	• The date of the information security breach;	103	✓	Security Incident Log
	• The date that the information security breach was identified or suspected;	103	✓	Security Incident Log
	• The nature of the PHI that was the subject matter of the breach and the nature and extent of the information security breach;	103	✓	Security Incident Log
	• The date that the information security breach was contained and the nature of the containment measures;	103	✓	Security Incident Log
	• The date that the HIC or other organization that disclosed the PHI to CCO was notified	103	✓	Security Incident Log
	• The date that the investigation the breach was completed;	104	✓	Security Incident Log
	• The agent(s) responsible for conducting the investigation;	104	✓	Security Incident Log
	• The recommendations arising from the investigation;	104	✓	Security Incident Log
	• The agent(s) responsible for addressing each recommendation;	104	✓	Security Incident Log

	• The date each recommendation was or is expected to be addressed	104	✓	Security Incident Log
	• The manner in which each recommendation was or is expected to be addressed.	104	✓	Security Incident Log

Table 3 - Human Resources Checklist

IPC 2017 Triennial Review - Requested Human Resources Documentation				
Req.	**Minimum Content of Required Documentation**	**Page Ref# in Manual**	**Req't Met**	**Identifying CCO Document**
1	**Policy and procedures for privacy training and awareness**			
	• A policy and procedures must be developed and implemented requiring agents of CCO to attend initial privacy orientation as well as ongoing privacy training.	105	✓	CCO's Privacy Policy; Privacy and Security Training and Awareness Procedure
	• The policy and procedures:	105		
	• the time frame agents must complete the initial privacy orientation	105	✓	Privacy and Security Training and Awareness Procedure
	• address the frequency of ongoing privacy training	105	✓	Privacy and Security Training and Awareness Procedure
	• complete the initial privacy orientation prior to being given access to PHI	105	✓	Privacy and Security Training and Awareness Procedure
	• attend ongoing privacy training provided by CCO on an annual basis.	105	✓	Privacy and Security Training and Awareness Procedure
	• identify the agent(s) responsible for preparing and delivering the initial privacy orientation and ongoing privacy training	105	✓	Privacy and Security Training and Awareness Procedure

	• the process that must be followed in notifying the agent(s) responsible for preparing and delivering the initial privacy orientation	105	✓	Privacy and Security Training and Awareness Procedure
	• include a discussion of the agent(s) responsible for providing notification	105	✓	Privacy and Security Training and Awareness Procedure
	• time frame within which notification must be provided	105	✓	Privacy and Security Training and Awareness Procedure
	• the format of the notification	105	✓	Privacy and Security Training and Awareness Procedure
	• the content of the initial privacy orientation to ensure that it is formalized and standardized.	105	✓	Privacy and Security Training and Awareness Procedure
	• require the initial privacy training to include:	105		
	• A description of the status of CCO under the Act and the duties and responsibilities that arise as a result of that status	105	✓	Privacy and Security Training and Awareness Procedure
	• the nature of the PHI collected and from whom this information is typically collected	105	✓	Privacy and Security Training and Awareness Procedure
	• the purposes for which PHI is collected and used and how this collection and use is permitted by the Act and its regulation	105	✓	Privacy and Security Training and Awareness Procedure
	• Limitations placed on access and use of PHI by agents	105	✓	Privacy and Security Training and Awareness Procedure
	• the procedure that must be followed when an agent is requested to disclose PHI	105	✓	Privacy and Security Training and Awareness Procedure
	• An overview of the privacy policies, procedures and practices that have been implemented by CCO	105	✓	Privacy and Security Training and Awareness Procedure

	• The consequences of breaches of policies, breaches of procedures, and breaches of practices implemented	105	✓	Privacy and Security Training and Awareness Procedure
	• An explanation of the privacy program	106	✓	Privacy and Security Training and Awareness Procedure
	• The administrative, technical and physical safeguards implemented by CCO to protect PHI	106	✓	Privacy and Security Training and Awareness Procedure
	• The duties and responsibilities when implementing the administrative, technical and physical safeguards put in place by CCO	106	✓	Privacy and Security Training and Awareness Procedure
	• A discussion of the nature and purpose of the Confidentiality Agreement that agents must execute and the key provisions of the Confidentiality Agreement	106	✓	Privacy and Security Training and Awareness Procedure
	• An explanation of the Policy and Procedures for Privacy Breach Management	106	✓	Privacy and Security Training and Awareness Procedure
	• duties and responsibilities when involved with privacy breaches.	106	✓	Privacy and Security Training and Awareness Procedure
	• The policy and procedure shall require:	106		
	• the ongoing privacy training to be formalized and standardized	106	✓	Privacy and Security Training and Awareness Procedure
	• role-based training	106	✓	Privacy and Security Training and Awareness Procedure
	• any new privacy policies, procedures and practices and significant amendments to existing privacy policies	106	✓	Privacy and Security Training and Awareness Procedure

	• ongoing privacy training must have regard to any recommendations with respect to privacy training made in PIAs, privacy audits and the investigation of privacy breaches and privacy complaints	106	✓	Privacy and Security Training and Awareness Procedure
	• that a log be maintained to track attendance at the initial privacy orientation and the agent responsible for maintaining the log	106	✓	Privacy and Security Training and Awareness Procedure
	• that a log be maintained to track ongoing privacy training and the agent responsible for maintaining the log	106	✓	Log of Privacy and Security Training Completion
	• An outline of the process to be followed in tracking attendance at the initial privacy orientation	106	✓	Privacy and Security Training and Awareness Procedure
	• the documentation that must be completed, provided and/or executed to verify attendance at initial and ongoing privacy training, the agent(s) responsible for doing so; the agent to whom this documentation must be provided; and the required content of the documentation.	106	✓	Privacy and Security Training and Awareness Procedure
	• identify the procedure to be followed and the agent(s) responsible for identifying the agent(s) who do not attend the intial or ongoing training and for ensuring such agent(s) attend the training, including the time frame following the date of the privacy orientation or the ongoing privacy training within which this procedure must be implemented	106	✓	Privacy and Security Training and Awareness Procedure
	• address where documentation related to attendance at the initial privacy orientation and the	106	✓	Privacy and Security Training and Awareness Procedure

	ongoing privacy training is to be retained			
	• policy and procedure shall:	107		
	• discuss the other mechanisms implemented by CCO to foster a culture of privacy	107	✓	Privacy and Security Training and Awareness Procedure
	• to raise awareness of the privacy program	107	✓	Privacy and Security Training and Awareness Procedure
	• discuss the frequency with which CCO communicates with its agents in relation to privacy	107	✓	Privacy and Security Training and Awareness Procedure
	• the method and nature of the communication	107	✓	Privacy and Security Training and Awareness Procedure
	• the agent(s) responsible for the communication	107	✓	Privacy and Security Training and Awareness Procedure
	• require agents to comply with the policy and its procedures and address how and by whom compliance will be enforced and the consequences of breach~~. compliance with the policy and procedure is required~~	107	✓	Privacy and Security Training and Awareness Procedure
	• stipulate that compliance will be audited, the frequency with which the policy and procedures will be audited and identify the agent responsible for conducting the audit and for ensuring compliance with the procedure	107	✓	Privacy Audit and Compliance Policy
	• require agents to notify CCO at the first reasonable opportunity if an agent breaches, or believes there may have been a breach of this policy or its procedures.	107	✓	Privacy Breach Management Policy
2	**Log of attendance at initial privacy orientation and ongoing privacy training**			

	• maintain a log of the attendance at the initial and ongoing training	107	✓	Privacy and Security Training and Awareness Procedure; Log of Privacy and Security Training Completion
3	**Policy and procedures for security training and awareness**			
	• A policy and procedures must be developed and implemented ~~for~~ to require completion of initial security orientation as well as ongoing security training.	107	✓	CCO's Privacy Policy; Enterprise Information Security Policy; Privacy & Security Training and Awareness Procedures
	• set out the time frame within which agents must complete the initial security orientation and the frequency of ongoing security training	107	✓	CCO's Privacy Policy; Enterprise Information Security Policy; Privacy & Security Training and Awareness Procedures
	• require an agent to complete the initial security orientation prior to being given access to PHI and complete ongoing security training on an annual basis	107	✓	CCO's Privacy Policy; Enterprise Information Security Policy; Privacy & Security Training and Awareness Procedures
	• identify the agent(s) responsible for preparing and delivering the security orientation and training	107	✓	CCO's Privacy Policy; Enterprise Information Security Policy; Privacy & Security Training and Awareness Procedures

	• set out the process that must be followed in notifying the agent(s) responsible for preparing and delivering the intial security orientation when an agent has commenced or will commence an employment, contractual or other relationship with CCO, including the agent(s) responsible for providing notification, the time frame within which notificaiton must be provided, and the format of the notification	108	✓	CCO's Privacy Policy; Enterprise Information Security Policy; Privacy & Security Training and Awareness Procedures
	• the security orientation shall include:	108		
	• An overview of the security policies, procedures and practices that have been implemented by CCO, and an explanaiton of the obligations ariding from these policies, procedures, and practices.	108	✓	Privacy and Security Training and Awareness Procedures; Core Privacy and Security Training eLearning Curriculum
	• The consequences of breach of the security policies, procedures and practices implemented;	108	✓	Privacy and Security Training and Awareness Procedures; Core Privacy and Security Training eLearning Curriculum
	• An explanation of the security program, including the key activities of the program and the agent(s) delegated day-to-day authority to manage the security program	108	✓	Privacy and Security Training and Awareness Procedures; Core Privacy and Security Training eLearning Curriculum
	• The administrative, technical and physical safeguards implemented by CCO to protect PHI	108	✓	Privacy and Security Training and Awareness Procedures; Core

				Privacy and Security Training eLearning Curriculum
	• duties and responsibilities of agents implementing the safeguards	108	✓	Privacy and Security Training and Awareness Procedures; Core Privacy and Security Training eLearning Curriculum
	• duties and responsibilities imposed on agents in identifying, reporting, containing and particapting in the investigation and remediation of security breaches	108	✓	Privacy and Security Training and Awareness Procedures; Core Privacy and Security Training eLearning Curriculum
	• the policy and procedure shall require:	108		
	•ongoing security training to be formalized and standardized	108	✓	Privacy and Security Training and Awareness Procedures; Core Privacy and Security Training eLearning Curriculum
	• role-based training	108	✓	Privacy and Security Training and Awareness Procedures; Core Privacy and Security Training eLearning Curriculum
	• address any new security policies, procedures and practices	108	✓	Privacy and Security Training and Awareness Procedures; Core Privacy and Security Training eLearning Curriculum

	• must have regard to any recommendations with respect to security training made in PIAs, the investigation of inofmraiton security breaches and the conduct of security audits including penetration testing, ethical hacks and reviews of system control and audit logs	108	✓	Privacy and Security Training and Awareness Procedures; Core Privacy and Security Training eLearning Curriculum
	• a log be maintained to track attendance and identify the agent responsible for maintaining the log	109	✓	Privacy and Security Training and Awareness Procedures; Core Privacy and Security Training eLearning Curriculum ; Log of Privacy and Security Training Completion
	• The process to be followed in tracking attendance	109	✓	Privacy and Security Training and Awareness Procedures; Core Privacy and Security Training eLearning Curriculum ; Log of Privacy and Security Training Completion
	• documentation completed to verify attendance	109	✓	Privacy and Security Training and Awareness Procedures; Core Privacy and Security Training eLearning Curriculum ;
	• the agent(s) responsible for completing the documentation	109	✓	Privacy and Security Training and Awareness Procedures; Core Privacy and Security Training eLearning Curriculum

	• the agent to whom this documentation must be provided	109	✓	Privacy and Security Training and Awareness Procedures; Core Privacy and Security Training eLearning Curriculum
	• the required content of the documentation	109	✓	Privacy and Security Training and Awareness Procedures; Core Privacy and Security Training eLearning Curriculum
	• identify the agent responsible for identifying agents who do not complete the initial training, the procedure for those who do not attend training, and the timeframe in which this must be implemented	109	✓	Privacy and Security Training and Awareness Procedures; Core Privacy and Security Training eLearning Curriculum
	• address where documentation related to attendance will be retained	109	✓	Privacy and Security Training and Awareness Procedures; Core Privacy and Security Training eLearning Curriculum
	• the policy and procedure shall:	109		
	• discuss the other mechanisms implemented by CCO to raise awareness of the security program, and the security policies, procedures and practices implemented	109	✓	Information Security Policy; Information Security Code of Conduct and Acceptable Use Policy
	• discuss the frequency CCO communicates with its agents in relation to information security, the method and nature of the commmunication and the agent responsible for the communication	109	✓	Information Security Policy; Information Security Code of Conduct and Acceptable Use Policy

	• require agents to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach, including what those consequences are and by whom the consequences will be enforced.	109	✓	Information Security Policy; Information Security Code of Conduct and Acceptable Use Policy
	• stipulate that compliance will be audited, set out the frequency with which the policy and procedures will be audited and identify the agent responsible for conducting the audit and ensuring compliance with the policy and its procedures	109	✓	Information Security Policy; Information Security Code of Conduct and Acceptable Use Policy
	• to notify CCO at the first reasonable opportunity if an agent breaches, or believes there may have been a breach of this policy or its procedures.	109	✓	Information Security Policy; Information Security Code of Conduct and Acceptable Use Policy
4	**Log of attendance at initial security orientation and ongoing security training**			
	• maintain a log of the attendance of agents at the initial and ongoing security training.	110	✓	Information Security Policy; Information Security Code of Conduct and Acceptable Use Policy; Log of Privacy and Security Training Completion
5	**Policy and procedures for the execution of confidentiality agreements by agents**			
	• require agents to execute a Confidentiality Agreement at the commencement of their employment, contractual or other relationship with CCO, and before being given access to PHI.	110	✓	Confidentiality Policy
	• recommended that the policy and procedures require that a Confidentiality Agreement be	110	✓	Confidentiality Policy

	executed by agents on an annual basis			
	• the policy and procedure must:	110		
	• identify the agents(s) responsible for ensuring that Confidentiality Agreement is executed with each agent of CCO at commencement of employment, contractual or other relationship.	110	✓	Confidentiality Policy
	• outline the process that must be followed in notifying the responsible agent(s) each time an agent starts an employment or contractual relationship with CCO	110	✓	**For employees:** HCMS System **For third parties under contract with CCO:** CCO Procurement Policy **For volunteers and secondees:** HCMS System
	• outline the process that must be followed where an executed Confidentiality Agreement is not received within a defined period of time following the commencement of the employment, contractual or other relationship or following the date that the Confidentiality Agreement must be executed on an annual basis	110	✓	Confidentiality Policy
	• outline the process that must be followed by the responsible agent(s) in tracking the execution of Confidentiality Agreements	110	✓	Confidentiality Policy
	• require that a log be maintained of executed Confidentiality Agreements	110	✓	Confidentiality Policy

	• comply with the policy and its procedures and address how compliance will be enforced and the consequences of breach.	110	✓	Confidentiality Policy
	• set out the frequency with which the policy and its procedures will be audited	111	✓	Confidentiality Policy
	• requirement to notify CCO if an agent believes there may have been a breach of this policy or its procedures.	111	✓	Confidentiality Policy
6	**Template confidentiality agreement with agents**			
	• The Confidentiality Agreement must:			
	• describe the status of CCO under the Act and outline the responsibilities arising from this status.	111	✓	Statement of Confidentiality; Service Agreements - Template Schedule for Third Party Agreements
	• state that individuals executing the agreement are agents of the CCO in respect of PHI and outline the responsibilities arising from this status.	111	✓	Statement of Confidentiality; Service Agreements - Template Schedule for Third Party Agreements
	• require agents to comply with the provisions of the Act and regulation, and with the terms of the agreement.	111	✓	Statement of Confidentiality; Service Agreements - Template Schedule for Third Party Agreements
	• have agents acknowledge they have read, understood and agree to comply with privacy and security policies	111	✓	Statement of Confidentiality; Service Agreements - Template Schedule for Third Party Agreements
	• provide a definition of personal health information consistent with the Act	111	✓	Statement of Confidentiality; Service Agreements - Template Schedule

				for Third Party Agreements
	• identify the purposes for which agents are permitted to collect, use and disclose PHI on behalf of CCO	112	✓	Statement of Confidentiality; Service Agreements - Template Schedule for Third Party Agreements
	• In identifying the purposes for which agents are permitted to collect, use or disclose PHI CCO must ensure that each collection, use or disclosure identified in the Confidentiality Agreement is permitted by the Act	112	✓	Statement of Confidentiality; Service Agreements - Template Schedule for Third Party Agreements
	• the Confidentiality Agreement must prohibit agents from collecting and using PHI except as permitted in the Agreement and from disclosing such information except as permitted in the Agreement or as required by law	112	✓	Statement of Confidentiality
	• prohibit agents from collecting, using or disclosing PHI if other information will serve the purpose	112	✓	Statement of Confidentiality; Service Agreements - Template Schedule for Third Party Agreements
	• require agents to securely return all property of CCO	112	✓	Statement of Confidentiality; Service Agreements - Template Schedule for Third Party Agreements
	• stipulate the time frame the property of CCO must be securely returned, the secure manner in which the property must be returned and to whom the property must be securely returned.	112	✓	Statement of Confidentiality; Service Agreements - Template Schedule for Third Party Agreements

	• notify CCO if the agent believes that there may have been a breach of the Confidentiality Agreement or CCO privacy or security policies and procedures	112	✓	Statement of Confidentiality; Service Agreements - Template Schedule for Third Party Agreements
	• outline the consequences of breach of the agreement and address how compliance will be enforced	112	✓	Statement of Confidentiality; Service Agreements - Template Schedule for Third Party Agreements
	• stipulate that compliance with the Confidentiality Agreement will be audited and set out the manner in which compliance will be audited.	112	✓	Tracked via Privacy & Security eLearning module
7	**Log of executed confidentiality agreements with agents**			
	• maintain a log of Confidentiality Agreements that have been executed by agents	112-113	✓	**For employees:** Payroll System log, Tracked via Privacy & Security eLearning Module **For third parties:** Contract Management System **For volunteers and secondees:** Tracked via Privacy & Security eLearning Module
8	**Job descriptions for the position(s) delegated day-to-day authority to manage the privacy program**			
	• A job description for the positions that manage the privacy program on behalf of CCO must be developed	113	✓	Assistant General Counse& Director, Privacy; Privacy Specialist; Senior Privacy Specialist, Group Manager, Privacy
	• The job description shall:	113		
	• set out the reporting relationship to the Chief	113	✓	Assistant General Counsel & Director,

	Executive Officer or the Executive Director			
	• · identify the responsibilities and obligations of the position(s) in respect of the privacy program, which shall include:	113		Job descriptions for Assistant General Counsel & Director, Privacy; Privacy Specialist; Senior Privacy Specialist, Group Manager, Privacy
	• Developing, implementing, reviewing and amending privacy policies, procedures and practices	113	✓	
	• Ensuring compliance with privacy policies, procedures and practices	113	✓	
	• Ensuring transparency of privacy policies, procedures and practices	113	✓	
	• Facilitating compliance with the *Act* and its regulation;	113	✓	
	• Ensuring agents are aware of the *Act* and its regulation	113	✓	
	• Ensuring agents are aware of the privacy policies, procedures	113	✓	
	• ensuring the delivery of the privacy training	113	✓	
	• Conducting, reviewing and approving PIAs	113	✓	
	• Responding to privacy complaints and inquiries	113	✓	
	• Receiving, documenting, tracking, investigating and remediating privacy breaches or suspected privacy breaches	114	✓	
	• Conducting privacy audits	114	✓	

9	**Job descriptions for the position(s) delegated day-to-day authority to manage the security program**			
	• A job description for the position(s) that have been delegated day-to-day authority to manage the security program	114	✓	Job descriptions for Senior Information Security Advisor; Group Manager, Information Security; Information Security Advisor
	• the reporting relationship of the day-to-day authority to the Chief Executive Officer or the Executive Director	114	✓	CCO's Job Description for Senior Team Lead, Enterprise Information Security Office
	• identify the responsibilities and obligations of the position(s) in respect of the security program, which shall include:	114	✓	Job descriptions for Senior Information Security Advisor; Group Manager, Information Security; Security Advisor
	• Developing, implementing, reviewing and amending security policies, procedures and practices.	114	✓	
	• Ensuring compliance with the security policies	114	✓	
	• Ensuring agents are aware of the security policies	114	✓	
	• delivery of the initial security orientation	114	✓	
	• the ongoing security training and fostering a culture of information security awareness	114	✓	
	• investigating and remediating information security breaches	114	✓	
	• Conducting security audits pursuant	114	✓	
10	**Policy and procedures for termination or cessation of the employment or contractual relationship**			

	• require agents, as well as their supervisors, to notify CCO of the termination of the employment, contractual or other relationship.	114	✓	Termination of Employment Policy; Employee Exit Process; HCMS System
	• identify the agent(s) to whom notification of the termination of the employment, contractual or other relationship must be provided, the nature and format of the notification, the time frame within which notification must be provided and the process that must be followed in providing notification	114-115	✓	Termination of Employment Policy; Employee Exit Process; HCMS System
	• require agents to securely return all property of CCO on or before the date of termination	114	✓	Employee Exit Process; HCMS System
	• the policy and procedure shall :	115		
	•Define property	115	✓	Employee Exit Process; HCMS System
	• identify the agent(s) to whom the property must be securely returned, the secure method by which the property must be returned and the time frame within which the property must be securely returned.	115	✓	Employee Exit Process; HCMS System
	• the documentation that must be completed, provided and/or executed and the required content of the documentation.	115	✓	Employee Exit Process; HCMS System
	• the agent(s) responsible for completing, providing and/or executing the documentation	115	✓	Employee Exit Process; HCMS System

	• the procedures to be followed in the event that the property of CCO is not securely returned upon termination of the employment, contractual or other relationship, incuding the agent responsible for implementing the procedure and the time frame following termination within which the procedure must be implemented	115	✓	Employee Exit Check List; HCMS System; CCO's termination monthly reports
	• that access to locations where records of PHI are retained be immediately terminated and the agents responsible for terminating access	115	✓	Employee Exit Process; HCMS System
	• the procedure to be followed in terminating access	115	✓	Employee Exit Process; HCMS System
	• the time frame within which access must be terminated	115	✓	Employee Exit Process; HCMS System
	• the documentation that must be completed	115	✓	Employee Exit Process; HCMS System
	• require agents to comply with the policy and its procedures and address how compliance will be enforced	115	✓	Employee Exit Process; HCMS System
	▪ Stipulate that compliance will be audited and set out the frequency with the policy and procedures will be audited and the agent responsible for conducting the audit and for ensuring compliance with the poicy and its procedures.	115	✓	Privacy Audit and Compliance Policy; CCO termination monthly report.
	• require agents to notify CCO if an agent believes there may have been a breach of this policy or its procedures.	115	✓	Employee Exit Process; HCMS System
11	**Policy and procedures for discipline and corrective action**			

	• develop and implement a policy and associated procedures for discipline and corrective action in respect of PHI	116	✓	Privacy Breach Management Policy; Code of Conduct; Information Security Code of Conduct and Acceptable Use Policy
	• address the investigation of disciplinary matters including:	116		
	• person(s) responsible for conducting the investigation	116	✓	Privacy Breach Management Policy; Code of Conduct
	• procedure that must be followed in the investigation	116	✓	Privacy Breach Management Policy; Code of Conduct
	• documentation that must be completed in the investigation process, the required content of the documentation and the agent(s) responsible for completing, providing, and/or executing the documentation	116	✓	Privacy Breach Management Policy; Code of Conduct
	• to whom the results of the investigation must be reported	116	✓	Privacy Breach Management Policy; Code of Conduct
	• The types of discipline that may be imposed by CCO	116	✓	Privacy Breach Management Policy; Code of Conduct
	• the factors considered determining the appropriate discipline	116	✓	Code of Conduct
	• agent(s) responsible for determining the appropriate discipline	116	✓	Code of Conduct; Progressive Discipline Policy
	• the procedure to be followed in making this determination and the agent(s) that must be consulted in making this determination	116	✓	Code of Conduct; Progressive Discipline Policy

	• identify the documentation that must be completed in relation to discipline imposed	116	✓	Code of Conduct; Progressive Discipline Policy
	• retention of documentation related to the discipline and corrective action taken	116	✓	Code of Conduct; Progressive Discipline Policy; Record Series on "Employee Management: Individual Employee Files"

Table 4 - Organization and Other Checklist

IPC 2017 Triennial Review - Requested Organizational and Other Documentation				
Req.	**Minimum Content of Required Documentation**	**Page Ref# in Manual**	**Req't Met**	**Identifying CCO Document**
1	**Privacy governance and accountability framework**			
	• compliance with the Act and with the privacy policies, procedures and practices implemented CCO	117	✓	CCO's Privacy Policy
	• the Chief Executive Officer or the Executive Director is accountable for CCO's compliance with the Act	117	✓	CCO's Privacy Policy
	• the Chief Executive Officer or the Executive Director is accountable for ensuring that CCO and its agents comply with the privacy policies, procedures and practices implemented	117	✓	CCO's Privacy Policy
	• day-to-day authority to manage the privacy program	117	✓	CCO's Privacy Policy; Annual Privacy Report
	• nature of the reporting relationship to the Chief Executive Officer or the Executive Director must be described	117	✓	CCO's Privacy Policy

	• the responsibilities of the delegated day-to-day authority	117	✓	CCO's Privacy Policy
	• The role of the Board of Directors in respect of the privacy program	117	✓	CCO's Privacy Policy, Charter - CCO Board of Directors
	· whether the privacy program is overseen by a committee of the Board of Directors, the frequency with which and the method and manner by which the Board of Directors is updated with respect to the privacy program, the agent(s) responsible for providing such update and the matters with respect to which the Board of Directors is required to be updated	117	✓	Annual Privacy Report; Charter - Information Management and Information Technology Committee of the Board of Directors
	• updates on the initiatives undertaken by the privacy program provided to the Board of Directors	117	✓	Annual Privacy Report
	• updates to the Board of Directors must include privacy training; the development and implementation of privacy policies, procedures, and practices; a discussion of the privacy audits and PIAs conducted, including the results of and recommendations arising from the privacy audits and PIAs and the status of implementation of the recommendations; and any privacy breaches and privacy complaints that were investigated, including the results of and any recommendations arising from these investigations and the status of implementation of the recommendations.	117	✓	Annual Privacy Report

	• the privacy governance and accountability framework be accompanied by a privacy governance organizational chart.	117	✓	CCO's Privacy Policy; Privacy Governance Framework
	• the manner in which the privacy governance and accountability framework will be communicated	118	✓	CCO's Privacy Policy; Annual Privacy Report; Privacy Governance Framework
2	**Security governance and accountability framework**			
	• compliance with the Act and with the security policies, procedures and practices implemented by CCO	118	✓	Enterprise Information Security Policy; Information Security Program Framework; Charter - CCO Board of Directors; CCO Board of Directors Orientation Handbook
	• the Chief Executive Officer or the Executive Director is accountable for ensuring the security of PHI	118	✓	Information Security Program Framework; Charter - CCO Board of Directors
	• the Chief Executive Officer or the Executive Director is accountable for ensuring that CCO and its agents comply with the security policies, procedures and practices implemented	118	✓	Information Security Program Framework; Charter - CCO Board of Directors
	• day-to-day authority to manage the security program	118	✓	CCO Board of Directors Orientation Handbook; Information Security Program Framework, Charter - CCO Board of Directors
	• the nature of the reporting relationship to the CEO or the Executive Director	118	✓	Information Security Program Framework; Charter - CCO Board of Directors

	• the responsibilities of the delegated day-to-day authority	118	✓	Enterprise Information Security Policy; Information Security Program Framework; CCO Board of Directors Orientation Handbook; Charter - CCO Board of Directors
	• The role of the Board of Directors in respect of the security program	118	✓	CCO Board of Directors Orientation Handbook; Charter - CCO Board of Directors
	· whether the security program is overseen by a committee of the Board of Directors, the frequency with which and the method and manner by which the Board of Directors is updated with respect to the security program, the agent(s) responsible for providing such update and the matters with respect to which the Board of Directors is required to be updated	118	✓	Charter - Information Management and Information Technology Committee of the Board of Directors
	• updates on the initiatives undertaken by the security program provided to the Board of Directors	118	✓	Information Security Program Framework
	· updates to the Board of Directors must include security training; the development and implementation of security policies, procedures, and practices; a discussion of the security audits, including the results of and recommendations arising from the security audits and the status of implementing of the recommendations; and any information security breaches	118	✓	Information Security Program Framework

	investigated, including the results of and any recommendations arising from these investigations and the status of implementation of the recommendations			
	• the security governance and accountability framework be accompanied by a security governance organizational chart	119	✓	Information Security Program Framework
	• the manner in which the security governance and accountability framework will be communicated	119	✓	Information Security Program Framework
3	**Terms of reference for committees with roles with respect to the privacy program and/or security program**			
	• terms of reference for each committee that has a role in respect of the privacy and/or the security program	119	✓	Information Management and Information Technology Steering Committee Terms of Reference; Data Analytics Management Committee Terms of Reference; Data Disclosure Subcommittee Terms of Reference; Data Disclosure Working Group Terms of Reference; Information Technology Management and Architecture Committee Terms of Reference

	• the terms of reference:	119	✓	Information Management and Information Technology Steering Committee Terms of Reference; Data Analytics Management Committee Terms of Reference; Data Disclosure Subcommittee Terms of Reference; Data Disclosure Working Group Terms of Reference; Information Technology Management and Architecture Committee Terms of Reference
	• the membership of the committee	119	✓	Information Management and Information Technology Steering Committee Terms of Reference; Data Analytics Management Committee Terms of Reference; Data Disclosure Subcommittee Terms of Reference; Data Disclosure Working Group Terms of Reference; Information Technology Management and Architecture Committee Terms of Reference

	• the chair of the committee	119	✓	Information Management and Information Technology Steering Committee Terms of Reference; Data Analytics Management Committee Terms of Reference; Data Disclosure Subcommittee Terms of Reference; Data Disclosure Working Group Terms of Reference; Information Technology Management and Architecture Committee Terms of Reference
	• the mandate and responsibilities of the committee in respect of the privacy and/or the security	119	✓	Information Management and Information Technology Steering Committee Terms of Reference; Data Analytics Management Committee Terms of Reference; Data Disclosure Subcommittee Terms of Reference; Data Disclosure Working Group Terms of Reference; Information Technology Management and Architecture Committee Terms of Reference

	• the frequency with which the committee meets	119	✓	Information Management and Information Technology Steering Committee Terms of Reference; Data Analytics Management Committee Terms of Reference; Data Disclosure Subcommittee Terms of Reference; Data Disclosure Working Group Terms of Reference; Information Technology Management and Architecture Committee Terms of Reference
	• to whom the committee reports	119	✓	Information Management and Information Technology Steering Committee Terms of Reference; Data Analytics Management Committee Terms of Reference; Data Disclosure Subcommittee Terms of Reference; Data Disclosure Working Group Terms of Reference; Information Technology Management and Architecture Committee Terms of Reference

	• the types of reports produced by the committee	119	✓	Information Management and Information Technology Steering Committee Terms of Reference; Data Analytics Management Committee Terms of Reference; Data Disclosure Subcommittee Terms of Reference; Data Disclosure Working Group Terms of Reference; Information Technology Management and Architecture Committee Terms of Reference
	• the format of the reports	119	✓	Information Management and Information Technology Steering Committee Terms of Reference; Data Analytics Management Committee Terms of Reference; Data Disclosure Subcommittee Terms of Reference; Data Disclosure Working Group Terms of Reference; Information Technology Management and Architecture Committee Terms of Reference

	• to whom these reports are presented	119	✓	Information Management and Information Technology Steering Committee Terms of Reference; Data Analytics Management Committee Terms of Reference; Data Disclosure Subcommittee Terms of Reference; Data Disclosure Working Group Terms of Reference; Information Technology Management and Architecture Committee Terms of Reference
	• the frequency of these reports	119	✓	Information Management and Information Technology Steering Committee Terms of Reference; Data Analytics Management Committee Terms of Reference; Data Disclosure Subcommittee Terms of Reference; Data Disclosure Working Group Terms of Reference; Information Technology Management and Architecture Committee Terms of Reference
4	**Corporate risk management framework**			

	• a comprehensive and integrated corporate risk management framework	119	✓	Privacy and Information Security Risk Management Procedure; Privacy Risk Register; Security Risk Management Standard; ERM Framework; Enterprise Risk Register
	• identify, assess, mitigate and monitor risks, including risks that may negatively affect the ability of CCO to protect PHI	119	✓	Privacy and Information Security Risk Management Procedure; Privacy Risk Register; Security Risk Management Standard; ERM Framework; Enterprise Risk Register
	• must address the agent (s) responsible and the process that must be followed in identifying risks that negatively affect the ability of CCO to protect PHI.	119	✓	Privacy and Information Security Risk Management Procedure; Privacy Risk Register; Security Risk Management Standard; ERM Framework; Enterprise Risk Register
	· This shall include person/organization that must be consulted in identifying the risk; documentation that must be completed, agents responsible for completing the documentation, the agent (s) to whom this documentation must be provided; and the required content of the documentation	119	✓	Privacy and Information Security Risk Management Procedure; Privacy Risk Register; Security Risk Management Standard; ERM Framework; Enterprise Risk Register

	• Address the agent (s) responsible and the process followed and criteria considered in ranking the risks and assessing likelihood and the potential impact. This shall include;	119	✓	Privacy and Information Security Risk Management Procedure; Privacy Risk Register; Security Risk Management Standard; ERM Framework; Enterprise Risk Register
	• the agent (s)/organizations consulted in assessing and ranking the risks and assessing likelihood and the potential impact, the documentation that must be completed for assessing, ranking and rationale, agent (s) responsible for completing the documentation, to whom the documentation must be provided and the content of the documentation	119	✓	Privacy and Information Security Risk Management Procedure; Privacy Risk Register; Security Risk Management Standard; ERM Framework; Enterprise Risk Register
	· Identify agent (s) responsible, the process that must be followed and the criteria considered in identifying strategies to mitigate the actual or potential risks to privacy, the process for implementing mitigation strategies and the agent/organization consulted in identifying and implementing the mitigation strategies	120	✓	Privacy and Information Security Risk Management Procedure; Privacy Risk Register; Security Risk Management Standard; ERM Framework; Enterprise Risk Register
	• documentation that must be completed, provided and/or executed in identifying, implementing, monitoring and implementation of the mitigation strategies, the agent responsible for documentation, to whom the documentation will be provided and the required content of the documentation	120	✓	Privacy and Information Security Risk Management Procedure; Privacy Risk Register; Security Risk Management Standard; ERM Framework

				Enterprise Risk Register
	• Address the manner and format in which the results of the corporate risk management process are communicated and reported.	120	✓	Privacy and Information Security Risk Management Procedure; Privacy Risk Register; Security Risk Management Standard; ERM Framework; Enterprise Risk Register;
	• This involves identifying agent (s) responsible for communication, the nature and format of communication, and to whom the results will be communicated.	120	✓	Privacy and Information Security Risk Management Procedure; Privacy Risk Register; Security Risk Management Standard; ERM Framework; Enterprise Risk Register;
	• The process for approval and endorsement of the results including agent(s) responsible for approval and endorsement be outlined	120	✓	Privacy and Information Security Risk Management Procedure; Privacy Risk Register; Security Risk Management Standard; ERM Framework; Enterprise Risk Register;
	• a corporate risk register be maintained and that the corporate risk register be reviewed on an ongoing basis	120	✓	Privacy and Information Security Risk Management Procedure; Privacy Risk Register; Security Risk Management Standard; ERM

				Framework; Enterprise Risk Register
	• the frequency with which the corporate risk register must be reviewed and the process that must be followed in reviewing and amending the risk register	120	✓	Privacy and Information Security Risk Management Procedure; Privacy Risk Register; Security Risk Management Standard; ERM Framework; Enterprise Risk Register
	• integration of risk management into the policies, procedures and practices and into the projects undertaken by CCO and the agent responsible for integration	120	✓	Privacy and Information Security Risk Management Procedure; Privacy Risk Register; Security Risk Management Standard; ERM Framework; Enterprise Risk Register
5	**Corporate risk register**			
	• develop and maintain a corporate risk register identifying risks that may negatively affect the ability of CCO to protect PHI	121	✓	Privacy Risk Register; Enterprise Risk Register
	• The risk register:	121	✓	Privacy Risk Register; Enterprise Risk Register
	• include an assessment of the risk	121	✓	Privacy Risk Register; Enterprise Risk Register
	• a ranking of the risk	121	✓	Privacy Risk Register; Enterprise Risk Register
	• the mitigation strategy to reduce the likelihood of the risk occurring	121	✓	Privacy Risk Register; Enterprise Risk Register

	• the date that the mitigation strategy was implemented	121	✓	Privacy Risk Register; Enterprise Risk Register
	• the agent(s) responsible for implementation of the mitigation strategy	121	✓	Privacy Risk Register; Enterprise Risk Register
6	**Policy and procedures for maintaining a consolidated log of recommendations**			
	• a consolidated and centralized log to be maintained of all recommendations arising from PIAs, privacy audits, security audits and the investigation of privacy complaints and privacy and security breaches.	121	✓	CCO's Privacy Policy; Privacy Audit and Review Standard; Enterprise Risk Register; Privacy Risk Register; Log of Privacy Impact Assessments; Log of Privacy Breaches; Log of Privacy Inquiries and Complaints; Log of IPC Recommendations; Log of Security Audits; Log of Security Incidents
	• the consolidated log must include recommendations made by the IPC that must be addressed by CCO prior to the next review of its practices and procedures	121	✓	Privacy Risk Register; Privacy and Information Security Risk Management Procedure; Log of IPC Recommendations
	• The policy and procedures:	121		
	• the frequency with which and the circumstances in which the consolidated and centralized log must be reviewed	121	✓	Privacy Risk Register; Privacy and Information Security Risk Management Procedure;
	• the agent(s) responsible for reviewing and amending the log	121	✓	Privacy Risk Register; Privacy and Information Security Risk Management Procedure

	• the process that must be followed in this regard	121	✓	Privacy Risk Register; Privacy and Information Security Risk Management Procedure
	• log be updated each time a recommendation has been addressed	121	✓	Privacy Risk Register; Privacy and Information Security Risk Management Procedure
	• log be reviewed on an ongoing basis	121	✓	Privacy Risk Register; Privacy and Information Security Risk Management Procedure
	• comply with the policy and its procedures and address how compliance will be enforced and the consequences of breach.	121	✓	Privacy Audit and Review Standard
	• compliance will be audited	121	✓	Privacy Audit and Review Standard
	• notify CCO if an agent believes there may have been a breach of this policy or its procedures.	121	✓	Privacy Breach Management Policy; Privacy Breach Management Manual
7	**Consolidated log of recommendations**			
	• maintain a consolidated and centralized log of all recommendations	122	✓	Privacy Risk Register
	• the name and date of the document, investigation, audit and/or review from which the recommendation arose.	122	✓	Privacy Risk Register
	• each recommendation:	122		
	• the recommendation made	122	✓	Privacy Risk Register
	• the manner in which the recommendation was addressed	122	✓	Privacy Risk Register
	• the date that the recommendation was addressed	122	✓	Privacy Risk Register

	• the agent(s) responsible for addressing the recommendation	122	✓	Privacy Risk Register
8	**Business continuity and disaster recovery plan**			
	• protect and ensure the availability of the information technology of CCO in the event of business interruptions including natural disasters	122	✓	Business Continuity Framework; Business Continuity Plan; Disaster Recovery Plan
	• The plan:	122		
	• notification of the interruption or threat	122	✓	Business Continuity Framework; Business Continuity Plan; Disaster Recovery Plan
	• documentation of the interruption or threat	122	✓	Business Continuity Framework; Business Continuity Plan; Disaster Recovery Plan
	• assessment of the severity of the interruption or threat	122	✓	Business Continuity Framework; Business Continuity Plan; Disaster Recovery Plan
	• activation of the business continuity	122	✓	Business Continuity Framework; Business Continuity Plan; Disaster Recovery Plan
	• disaster recovery plan	122	✓	Business Continuity Framework; Business Continuity Plan; Disaster Recovery Plan
	• recovery of PHI	122	✓	Business Continuity Framework; Business Continuity Plan; Disaster Recovery Plan
	• the persons or organizations that must be notified of business interruptions	122	✓	Business Continuity Framework; Business Continuity Plan; Disaster Recovery Plan

	• the time frame within which notification must be provided	122	✓	Business Continuity Framework; Business Continuity Plan; Disaster Recovery Plan
	• the manner and format of notification	122	✓	Business Continuity Framework; Business Continuity Plan; Disaster Recovery Plan
	• the nature of the information that must be provided upon notification	122	✓	Business Continuity Framework; Business Continuity Plan; Disaster Recovery Plan
	• documentation that must be completed	122	✓	Business Continuity Framework; Business Continuity Plan; Disaster Recovery Plan
	• a contact list of all agents that must be notified of business interruptions	122	✓	Business Continuity Plan; Disaster Recovery Plan
	•identify the agent(s) responsible for assessing the severity level	122	✓	Business Continuity Framework; Business Continuity Plan; Disaster Recovery Plan
	• the criteria pursuant to which this assessment is to be made	122	✓	Business Continuity Plan; Disaster Recovery Plan
	• the agents that must be consulted in assessing the severity level	122	✓	Business Continuity Framework; Business Continuity Plan; Disaster Recovery Plan
	• the documentation that must be completed	123	✓	Business Continuity Plan; Disaster Recovery Plan
	• the required content of the documentation	123	✓	Business Continuity Plan; Disaster Recovery Plan
	• the agent(s) to whom the documentation must be provided	123	✓	Business Continuity Framework; Business Continuity

				Plan; Disaster Recovery Plan
	• to whom the results of this assessment must be reported.	123	✓	Business Continuity Framework; Business Continuity Plan; Disaster Recovery Plan
	· agent(s) and process when conducting an initial impact assessment of the interruption this includes its impact on the technical and physical infrastructure and business processes of CCO; the agents and other persons or organizations that are required to be consulted in undertaking the assessment; the requirements that must be satisfied and the criteria that must be utilized in conducting the assessment; the documentation that must be completed, provided and/or executed; the agent(s) to whom the documentation must be provided; and the agent(s) to whom the results of the initial impact assessment must be communicated.	123	✓	Business Continuity Framework; Business Continuity Plan; Disaster Recovery Plan
	• agent(s) responsible for conducting a damage assessment	123	✓	Business Continuity Framework; Business Continuity Plan; Disaster Recovery Plan
	• the damage assessment:	123		
	• how the assessment will be conducted	123	✓	Business Continuity Plan; Disaster Recovery Plan
	• persons required to be consulted during the assessment	123	✓	Business Continuity Plan; Disaster Recovery Plan

	• requirements and the criteria when undertaking the assessment	123	✓	Business Continuity Plan; Disaster Recovery Plan
	• documentation that must be completed	123	✓	Business Continuity Plan; Disaster Recovery Plan
	• agent(s) to whom the documentation must be provided	123	✓	Business Continuity Plan; Disaster Recovery Plan
	• agent(s) to whom the results must be communicated.	123	✓	Business Continuity Plan; Disaster Recovery Plan
	• the plan:	123		
	• identify the agent(s) responsible for resumption and recovery	123	✓	Business Continuity Framework; Business Continuity Plan; Disaster Recovery Plan
	• the procedure that must be utilized in resumption and recovery	123	✓	Business Continuity Plan; Disaster Recovery Plan
	• the prioritization of resumption and recovery activities	123	✓	Business Continuity Plan; Disaster Recovery Plan
	• the criteria for the prioritization of resumption and recovery activities is determined	123	✓	Business Continuity Plan; Disaster Recovery Plan
	• the recovery time objectives for critical applications	123	✓	Business Continuity Plan; Disaster Recovery Plan
	• inventory of all critical applications	123	✓	Business Continuity Plan; Disaster Recovery Plan
	• the agent(s) responsible for the inventory	124	✓	Business Continuity Plan; Disaster Recovery Plan
	• the agent(s) consulted in developing the inventory	124	✓	Business Continuity Plan; Disaster Recovery Plan
	• determination of critical applications and business functions	124	✓	Business Continuity Plan; Disaster Recovery Plan

	• actions taken during business interruptions and threats to the operating capabilities of CCO	124	✓	Business Continuity Framework; Business Continuity Plan; Disaster Recovery Plan
	· testing, maintenance and assessment of the business continuity and disaster recovery plan this includes identifying the frequency of testing, the agent(s) responsible for amending the Plan as a result of the testing; the procedure to be followed testing, maintaining, assessing and amending the Plan; and the agent(s) responsible for approving the Plan and any amendment thereto	124	✓	Business Continuity Framework; Business Continuity Plan; Disaster Recovery Plan
	• the procedure to be followed in communicating the business continuity and disaster recovery plan	124	✓	Business Continuity Framework; Business Continuity Plan; Disaster Recovery Plan

Conclusion

CCO is committed to respecting personal privacy, safeguarding confidential information and ensuring the security of the PHI that it maintains. CCO meets these commitments through its comprehensive and multi-faceted privacy program. CCO continues to strive to improve and expand its Privacy Program to enrich its capacity to protect the privacy of those individuals whose PHI we hold and to ensure that CCO's privacy and security infrastructure is at the leading edge of industry standards.

CCO has demonstrated compliance with the IPC's requirements through its privacy program, which is supported by numerous departments across the organization. Specifically, the interplay of the governing documents implemented and maintained by the LPO, the EISO, the Strategic Sourcing Department, Facilities Department and the LPO and the Human Resources Departments, ensure that CCO has in place a robust privacy program and a strong culture of privacy and security across the entire organization.

The LPO and the EISO continue to work toward integration and harmonization of policies and practices to ensure not only a compliant organization, but effective and meaningful privacy and security programs. As the information needs of the healthcare sector evolve,

so too must our data protection efforts. CCO looks forward to a continuing relationship with the IPC to identify, define and manage PHI for the benefit of all Ontarians.

Sworn Affidavit

I, Michael Sherar, the President and Chief Executive Officer of Cancer Care Ontario, MAKE OATH AND SAY:

1. Cancer Care Ontario (CCO), a prescribed entity under subsection 18(1) of Ontario Regulation 329/04 to the Ontario *Personal Health Information Protection Act, 2004* (PHIPA) for the purposes of subsection 45(1) of PHIPA and a prescribed person under subsection 13(1) of Ontario Regulation 329/04 for the purposes of subsection 39(1)(c) of PHIPA, has in place policies, procedures and practices to protect the privacy of individuals whose personal health information is received and to maintain the confidentiality of that information.

2. The policies, procedures and practices implemented by CCO comply with PHIPA and the regulations thereto.

3. The policies, procedures and practices implemented by CCO comply with the *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities* that has been published by the Information and Privacy Commissioner of Ontario.

4. CCO has submitted a written report to the Information and Privacy Commissioner of Ontario in compliance with the *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities*.

5. CCO has taken steps that are reasonable in the circumstances to ensure compliance with the policies, procedures and practices implemented and to ensure that the personal health information received is protected against theft, loss and unauthorized use or disclosure and to ensure that records containing personal health information are protected against unauthorized copying, modification or disposal.

SWORN (OR AFFIRMED) BEFORE ME)
)
at the City of Toronto, in the Province)
)
of Ontario, on _____ 2016.)
)

_____

Michael Sherar, in his capacity as President and Chief Executive Officer of Cancer Care Ontario and not in his personal capacity

_____

Commissioner for Taking Affidavits
Alwin Kong

Appendix i – Supporting Documentation

1. ***Acceptable Use of Social Media Policy*** outlines the expected behaviour for Cancer Care Ontario (**CCO**) employees' participation in, and use of, Social Media.

2. ***Access Card Procedure*** outlines the procedures that must be followed by all CCO staff, including employees, students, third party service providers, secondees to CCO and independent contractors working for or on behalf of CCO (collectively, "CCO Staff") with respect to the use of CCO Photo Identification (**ID**) and elevator access cards.

3. ***Acquisition, Development, and Application Security Standard*** defines the security baseline for the acquisition and development phase in which applications are procured, designed, customized or developed.

4. ***Application for Disclosure of Information from CCO for Research Purposes*** is used specifically for researchers. It sets out the terms and conditions that a researcher must abide by when using personal health information (**PHI**) disclosed by CCO. This Application, along with the *CCO Non-Disclosure/Confidentiality Agreement*, forms the agreement between CCO and a researcher.

5. ***Architecture Review Board Terms of Reference*** sets out the responsibilities of the Architecture Review Board (**ARB**). The ARB is an approval board for CCO Enterprise Architecture and Information Technology (**IT**) Standards. One of the ARB's responsibilities to certify the physical design of a project is internally consistent and in alignment with the logical architecture and information, application, technology and security standards and methods.

6. ***Authorization to Access Data Centre Contractor Form*** is required to be completed by all CCO contractors who require specific access to data centres. The Form tracks the type of access granted to the data centre, the reasons for the access request, and it requires the signatures of the IT Manager, Chief Technology Office (**CTO**) and contractor.

7. ***Authorization to Access Data Centre Employee Form*** is required to be completed by all CCO employees who require specific access to data centres. The Form tracks the type of access granted to the data centre, the reasons for the access request, and it requires the signatures of the IT Manager, CTO and employee.

8. ***Business Continuity Framework*** contains supporting information for the *Business Continuity Plan* and *Disaster Recovery Plan* that is constant and not subject to frequent revisions. This document describes types of disaster scenarios and how Technology Services would move from operations to a continuity focus during time of

a business disruption or disaster. It outlines the phases of a disaster from response through to restoration.

9. ***Business Continuity Plan*** guides the business continuity operations for mission critical processes and services in the event of a threat or interruption that compromises the ability for CCO to meet minimum production requirements. Specifically, it provides all of the necessary lists, tasks, and reports used for response, resumption, or recovery in the event of a disaster. Additionally, it defines the roles and responsibilities for assigning available personnel and the activities to be conducted during each phase of a disaster. Contact processes for the fan out phase are delineated, message templates are included and can be found in the appendices.

10. ***Business Continuity Worksheet*** is used to document events and activities where disaster or the risk of disaster has been identified and the *Business Continuity Plan* has been activated.

11. ***Business Process for Data Requests*** outlines the procedures for receiving, processing, filing, deferring, rejecting, logging and following up on requests for CCO data including requests for PHI for research purposes.

12. ***CCO Board of Directors Orientation Handbook*** is provided to all CCO board members annually. The Handbook provides information to board members on the history of CCO, CCO's legislative compliance, the governance and corporate structure and a description of all programs at CCO.

13. ***Cancer Screening Program Privacy Breach Management Standard Operating Procedure*** applies to CCO in its capacity as a Prescribed Person (**PP**). This procedure, along with the *Privacy Breach Management Policy*, describes how the Cancer Screening Program (**CSP**) will identify, manage and resolve privacy breaches which occur as the result of misuse or improper/unauthorized collection, use and disclosure of PHI by CCO employees, consultants and contractors. Specifically, the procedure defines a privacy breach, identifies the parties which must be notified of a privacy breach, and outlines the steps to be taken by CCO once a privacy breach has occurred, including the nature and scope of the investigation of the breach, retrieval of PHI, and the steps taken to prepare privacy breach notification communications.

14. ***Cancer Screening Program Privacy Frequently Asked Questions*** are a list of frequently asked questions (**FAQs**) which the Legal & Privacy Office (**LPO**) receives regarding its privacy policies and practices in relation to the CSP program. It identifies the status of CCO under the *Personal Health Information Protection Act, 2004* (**PHIPA**) as a PP and the purposes of collection, use and disclosure of PHI within the custody and control of CCO for its CSP program, including how to access patient screening results and contact information.

15. ***Change Management Policy Suite*** controls and manages changes to IT systems and services in order to support the business while minimizing the risk of reduced service quality or disruption to services.
Change Management ensures that standardized methods and procedures are used for efficient and prompt handling of change-related incidents. It also controls and manages the implementation of the changes that are approved through the Change Management Process. The Change Management policy suite listed below aims to control and manage changes to IT systems and services to ensure that standardized methods and procedures are used for efficient and prompt handling of all changes so to minimize the impact of change-related incident upon service quality, and consequently improve the day-to-day operations of Technology Services.

Supporting documents include:

- *Change Management Policy*
- *Information Technology Change Subcommittee Terms of Reference*

16. ***Code of Conduct*** applies to all CCO employees and identifies the principles that guide the decisions and actions of all CCO employees in order to maintain an atmosphere that is conducive to excellent work practices.

17. ***Confidentiality Policy*** clearly establishes the requirement for persons working for or on behalf of CCO to preserve the confidentiality of all information not normally available to the public, including PHI.

18. ***Consulting Agreement*** is a Services Agreement that contains a template schedule entered into between CCO and consultants who will be permitted to access and use PHI. The template schedule, together with the baseline terms of the main Consulting Agreement, sets out the privacy and security responsibilities of the consultant in respect of PHI that it accesses, retains, transfers or disposes of on behalf of CCO.

19. ***Core Privacy & Security Training eLearning Curriculum*** is a web-based, in-depth, compulsory training program for new employees, including service providers with access to PHI, students, volunteers, researchers and others with access to CCO systems, addressing CCO's Privacy and Information Security Programs. All CCO employees, as well as consultants, students, volunteers, researchers and others with access to CCO systems, must complete the Core Privacy & Security Training Curriculum and accept the *Privacy and Security Acknowledgement Form* prior to receiving access to PHI at CCO.

20. ***Courier Transfer of Personal Health Information Procedure*** establishes the parameters and methods for the secure transfer of personal health information via courier.

21. ***Cryptography Standard*** broadly defines the cryptographic methods for addressing security requirements and generally defines acceptable means of using or implementing such methods. Compliance with this Standard will:

i. Ensure the consistent application of cryptographic safeguards across CCO;
ii. Establish a minimum baseline for cryptographic security at CCO that is in line with industry standards and best practices; and
iii. Facilitate necessary transitions to stronger or newer cryptographic methods as older methods become obsolete

22. ***Data Access Committee Terms of Reference*** outlines the major responsibilities of this committee. The Data Access Committee (**DAC**) is responsible for ensuring that data requests, including those made by researchers, are consistent with PHIPA. The DAC is also responsible for reviewing and approving data request related to the disclosure of PHI for research requests.

23. ***Data Backup Policy*** provides a standardized means of backing up and maintaining data that is critical to the viability and operation of CCO.

24. ***Data Backup Procedure*** defines the operational processes and standards relating to CCO's backup and recovery services.

25. ***Data Centre Access and Usage Policy*** provides administrative controls for accessing CCOs data centres and applies to all persons accessing the data centres. There are three levels of access to the data centre, based on the nature of work to be performed, its frequency, duration, and time of day at which access is required.

26. ***Data Linkage Policy*** (Draft) defines the circumstances in which the data linkage of records of PHI is permitted. The policy also outlines the purpose of linking data at CCO, and disclosure of that linked data by CCO.

27. ***Data Linkage Procedure*** (Draft) describes how requests for Data Linkage of CCO records of PHI are received, processed, and completed. The Procedure includes procedures related to the disclosure of data held by CCO in its capacity as a Prescribed Entity **(PE**) and data from CCO as a PP.

28. ***Data Sharing Agreement Initiation Form*** identifies the information required for review of a proposed data exchange, in addition to identifying the appropriate terms and conditions to be included in the completed data sharing agreement (**DSA**).

29. ***Data Sharing Agreement Procedure*** outlines the specific processes to be followed when a data exchange with an external party is being considered by CCO, or where a new use of data, for a purpose other than that set out in an existing DSA, is

proposed. The procedure prescribes the duties of each responsible party at CCO throughout the DSA lifecycle.

30. ***Data Sharing Agreement Standard*** defines the instances where a DSA is required at CCO, specifically where a data exchange with an external party is being considered or where a new use of data, for a purpose other than that set out in an existing DSA, is proposed.

31. ***Data Sharing Agreement Template*** specifies the terms and conditions that must be included in each DSA executed by CCO when collecting or disclosing PHI for purposes other than research.

32. ***Data Use & Disclosure Standard*** applies to disclosures and uses of PHI to internal and external users for research and non-research purposes. The Standard ensures disclosures of PHI comply with PHIPA and CCO's privacy obligations. The Data Use & Disclosure Standard sets out the circumstances in which PHI is permitted to be disclosed for research purposes.

33. ***Decision Criteria for Data Requests*** provides the criteria to be considered when determining whether to approve a request for PHI, de-identified and/or aggregate data for research purposes under section 44 of PHIPA.

34. ***De-Identification Guidelines*** (Under Revision) supplement CCO's *Data Use and Disclosure Standard* to enable employees to more clearly identify if individuals may be re-identified if data with small cell is disclosed. Analysts and developers use the Guidelines when they are asked to disclose reports or data sets containing de-identified information.

35. ***Digital Media Destruction Procedure*** describes the process used to securely dispose of digital media.

36. ***Digital Media Destruction Standard*** sets forth CCO's practices for securely disposing of digital storage media and any data contained within.

37. ***Disaster Recovery Plan*** is used in conjunction with the *Business Continuity Plan* and *Business Continuity Framework* to guide the decision making processes and set out priorities for those decisions. It contains a description of the roles of key staff, and system recovery dependencies. System recovery approaches for the class of services, vendor and key staff contact information are also found in the appendices along with the fan out procedure for Technology Services staff. It is supported by the Emergency Preparedness Database, specifically with respect to the creation of lists of staff and their relevant contact information. The list can be emailed or printed and delivered to managers so that they can call and log contact success. Communication and training plans have been developed to supplement Disaster Recovery.

38. ***Employee Exit Checklist*** includes a list of action items for managers to complete when an individual's employment, volunteer or other relationship with CCO has ended.

39. ***Employee Exit Process*** ensures that a systematic uniform exit procedure is followed for all employees, contractors, and volunteers, upon the cessation of their employment or other relationship with CCO. The process sets out the roles and responsibilities of departing employees, contractors, volunteers, managers and other departments, including the return of CCO property and deactivation of system access permissions, upon cessation of the individual's employment, volunteer or other relationship.

40. ***Enterprise Risk Management Framework*** sets out applicable risk management processes and documents the roles and responsibilities of CCO Staff and CCO's Board in identifying, assessing, mitigating (to the extent possible) and monitoring material risks, and outlines key aspects of CCO's risk management and reporting processes. It provides a comprehensive process to evaluate material risks to integrate and align existing risk management processes across CCO. It provides departments and programs with established risk assessment processes with the ability to identify, assess, mitigate (to the extent possible) and monitor risk in accordance with set standards.

41. ***Exchanging Encrypted Personal Health Information on Digital Media*** sets out the parameters for and roles and responsibilities of the parties involved in exchanges of PHI on Digital Media.

42. ***Exchanging Personal Health Information via Application Services Procedure*** sets out the parameters for and roles and responsibilities of the parties involved in exchanges of PHI via Applications Services.

43. ***Exchanging Personal Health Information via Secure Managed File Transfer Procedure*** sets out the responsibilities of the Business Unit when conducting exchanges of PHI via file transfer.

44. ***Exiting Employee Data Management*** sets out parameters for management of employee data after their departure.

45. ***Fax Transmission of Personal Health Information Procedure*** sets out the parameters and roles and responsibilities when conducting fax transmissions of PHI.

46. ***Hard Copy Personal Health Information Disposal Procedure*** sets forth CCO's requirements for the secure disposal of hard copy records containing PHI, including shredding service vendor contract requirements and shredding disposal requirements.

47. ***In-Person Transfer of Personal Health Information Procedure*** sets out the parameters and roles and responsibilities when conducting transfer of PHI in person.

48. ***Incident Management Framework*** provides guidance for the development of standards and procedure. It establishes a series of pre-determined process steps, which are initiated when CCO is notified about a potential incident which either threatens or could threaten the confidentiality, integrity or availability of CCO's information assets.

49. ***Information Management and Information Technology Stage – Gating Policy*** defines the stage-gate review process for approval of projects requiring Information Management (**IM**) and IT deliverables, services or resources, and to ensure that the appropriate review is conducted at critical transition points in the project lifecycle.

50. ***Information Management and Information Technology Stage – Gating Process and Project Lifecycle Methodology*** is used at CCO to review projects at various phases of the project lifecycle to ensure risk, status, expenditures and process are managed and all supporting business units are engaged.

51. ***Information Security Code of Conduct and Acceptable Use Policy*** supports CCO's commitment to safeguarding its information assets by establishing clear behavioural expectations for authorized individuals using CCO information systems and assets. This Code of Conduct fosters an understanding of security practices at CCO, including a practical understanding of the expectations of individuals who, in the course of their work at CCO, must protect the information they create, use, access, disclose or otherwise manage. The document defines high-level principles, provides pertinent examples of accepted behaviour, and establishes the responsibilities of management and employees.

52. ***Information Security Framework*** defines the foundational components of the information security program, and contains informational elements useful to the understanding, implementation, and administration of the program.

53. ***Information Security Incident & Breach Response Management Standard*** defines the baseline practices to address the identification, reporting, containment, notification, investigation and remediation of information incidents and breaches.

54. ***Information Security Policy*** is a framework of enforceable rules and best practices that regulate how CCO and its employees collaboratively support the enterprise information security objectives at all organizational levels. The policy is a concise statement of the requirements that must be met in order to satisfy those objectives, including:

i. The safeguarding of sensitive information assets and service assets;
ii. Documenting the corporate consensus on baseline information security;
iii. Managing organizational information security risks;
iv. Supporting CCO's policies and legislative compliance requirements;
v. Defining information security roles and responsibilities within CCO; and
vi. Defining and authorizing the consequences of violating the policy.

This governing policy is supported by a hierarchy of standards, procedures and guidelines.

55. ***Internal Data Access Policy*** describes the considerations applicable to users requesting direct access to record-level PHI in CCO's data holdings. Specifically, the policy prohibits access to or use of more PHI than is reasonably necessary to meet the identified purpose, sets out the process for approving or denying a request for access to and use of PHI, and identifies the conditions or restrictions for internal users who have been granted approval to access and use PHI.

56. ***Internal Data Access Procedure*** describes the process CCO will use to grant, deactivate, or change direct access to CCO data holdings for internal users (including CCO staff, consultants and contractors). It describes the process and tool (Internal Data Access Request or **IDAR**) used to request direct access to CCO data holdings of PHI for all internal users, including CCO employees, consultants and contractors.

57. ***Job Descriptions for the Position(s) Delegated Day-to-Day Authority to Manage the Privacy Program.*** CCO has detailed job descriptions for positions which have been delegated day-to-day duties with respect to the operations of its Privacy Program, including descriptions for the:

- Director, Legal & Privacy
- Sr. Privacy Specialist
- Manager, Privacy
- Privacy and Access Analyst
- Privacy Specialist

58. ***Job Description for the Position(s) Delegated Day-to-Day Authority to Manage the Security Program.*** CCO has prepared detailed job descriptions for positions which have been delegated day-to-day duties with respect to the operations of its Security Program, including descriptions for the:

- Group Manager, Information Security
- Technical Architect, Information Security
- Senior (**Sr.**) Information Security Specialist
- Technical Specialist, Information Security

59. ***Logging, Monitoring, and Auditing Standard*** defines the logging, monitoring and auditing requirements for CCO IT systems. The objectives are to:

i. Monitor accountability of users actions using IT systems;
ii. Detect unauthorized and inappropriate access to sensitive information (e.g., PHI);
iii. Detect information security incidents in a timely manner; and
iv. Provide forensic evidence for investigations of unauthorized or inappropriate use of CCO assets.

60. ***Logging, Monitoring, and Auditing System Threat Modeling Guide*** provides guidelines for identifying and documenting high-risk threat scenarios to CCO's critical assets and describes the process for identifying potential threats to CCO's critical assets and identifying detection controls (*e.g.,* monitoring rules).

61. ***Logical Access Control Standard*** sets the baseline security requirements for access control to systems and applications owned by, or under the security control of CCO. The objectives of the Standard are to:

i. Ensure compliance with both regulatory requirements and CCO's Information Security policies with regards to the protection of confidentiality, integrity and availability of information;
ii. Promote a culture in which responsibility for the use of IT resources is understood and users are held accountable for their actions; and
iii. Defines identification and authentication controls for logical access to information, computing resources and network facilities.

62. ***Mobile Device and Pager Policy*** defines the terms and conditions for authorizing personally owned mobile devices to access CCO corporate services, including a requirement for technical security controls.

63. ***Mobile Device and Pager Procedure*** sets out the process and standards for authorizing personally owned mobile devices to access CCO corporate services, including responsible parties.

64. ***New Employee Facilities & Information Technology Services Form*** is required to be completed by all new employees at CCO (including permanent full-time employees, permanent part-time employees, consultants, contractors, students, temporary employees and guest accounts). The Form tracks all related new employee information such as assigned business equipment, email account name, remote

access capability, as well as the employee's access privileges within the CCO premises.

65. ***Non-Disclosure/Confidentiality Agreement*** is used when CCO discloses information to researchers for research studies under section 44 of PHIPA. This Agreement sets out the terms and conditions pertaining to the protection of information provided by CCO to a researcher.

66. ***Operational Security Procedure***: ***Patching*** defines the steps taken for patching CCO systems, including the monitoring of availability of patches, implementation of patches, and required documentation.

67. ***Operational Security Standard*** sets baseline security requirements for secure operations of network and computing resources owned by, or under the control of CCO. In particular, this Standard aims to promote the following goals:

i. Compliance with regulatory requirements and CCO's Information Security policies with regards to the protection of confidentiality, integrity and availability of information;
ii. Define requirements for the secure operations of computing resources and network facilities (*e.g.,* vulnerability management, change management, etc.).

68. ***Personal Health Information Handling Standard*** defines CCO's baseline secure handling practices for PHI throughout the data lifecycle.

69. ***Personal Health Information Handling Procedure*** defines the procedures CCO follows with respect to handling of PHI, including decision criteria and roles for requesting and reviewing retention of PHI on mobile devices.

70. ***Personnel Action Form*** must be completed by managers and sent to CCO's Human Resources Department when a new employee is hired, when an employee transfers to another department, or when an employee is departing or taking a leave of absence. For new employees, the Form must be completed and provided to the Human Resources Department once the candidate has accepted CCO's offer of employment.

71. ***Photo Identification Request Form*** is required to be completed by all CCO employees. Photo identification (**ID**) cards are required in order to be granted access into all CCO buildings.

72. ***Physical Security Policy*** outlines the safeguarding of physical environments and sets out requirements with respect to facility access control, facility security, electronic device and media security and disposal, and hard copy (paper) record security and disposal.

73. ***Policy on Retention of Records Containing Personal Health Information*** sets out the obligations of CCO with respect to the retention of records of PHI and describes the purposes for retention of PHI.

74. ***Principles and Policies for the Protection of Personal Health Information at CCO (CCO's Privacy Policy)***, applies to CCO in its capacity as a PE and PP under PHIPA.
CCO's Privacy Policy is structured around the 10 privacy principles set out in the Canadian Standards Association Model Code for the Protection of PI ("CSA Model Code"). This Policy provides a general statement of CCO's position on each of the principles.
Each principle identifies the related supporting standards and procedures documents for operationalizing the principle in the CCO context.

75. ***Privacy and Information Security Risk Management Framework*** defines the approach by which CCO identifies, assesses, responds to and monitors privacy and security risks. It establishes a foundation for mitigating and managing privacy and security risks and sets the boundaries for risk-based decisions in respect of privacy and security within CCO. It provides a comprehensive process to evaluate privacy and security risks, and is used in conjunction with CCO's *Enterprise Risk Management Framework*.

76. ***Privacy and Security Training and Awareness Acknowledgement Form*** must be read and electronically accepted by all CCO employees, contractors, volunteers and students upon completion of privacy and security training. Acceptance of this signifies that the user agrees to the privacy and security responsibilities and obligations outlined in the form.

77. ***Privacy and Security Training and Awareness Procedure*** provides that all new CCO employees, service providers and other representatives such as consultants, students, volunteers and researchers with access to CCO systems, are advised of their privacy and security obligations through training and contractual means. It also describes the annual refresher training requirement for all CCO system users. Lastly, it outlines the repercussions for not completing the privacy and security training.

78. ***Privacy Audit and Compliance Policy*** describes how CCO reviews and measures the effectiveness of its IM practices, including the operational practices employed in the collection, use and disclosure of PHI by CCO, to ensure compliance with *CCO's Privacy Policy* and its supporting standards, procedures and guidelines.

79. ***Privacy Breach Management Policy*** describes the manner in which CCO will identify, manage and resolve privacy breaches resulting from the misuse or improper/unauthorized collection, use and disclosure of PHI that contravene PHIPA and/or CCO's privacy policies and procedures, and is supported by the *Privacy Breach Report Form*. Specifically, the procedure defines a privacy breach, imposes a mandatory requirement on CCO employees, consultants and contractors to notify CCO of a privacy breach, identifies when parties must be notified of a privacy breach, and outlines the steps to be taken by CCO once a privacy breach has occurred, including the nature and scope of the investigation of the breach.

80. ***Privacy Frequently Asked Questions*** are a list of frequently asked questions (**FAQs**) which the LPO receives regarding its privacy policies and practices. It identifies the status of CCO under PHIPA and the purposes of collection, use and disclosure of PHI within the custody and control of CCO. It also provides the LPO's contact information, should there be any further questions or concerns.

81. ***Privacy Governance Framework*** sets out the privacy governance structure at CCO, as well as the operational governance structure, outlining all of the core program controls. It outlines how CCO conducts ongoing monitoring and reporting and mandates an Annual Privacy Management, Oversight and Review Plan.

82. ***Privacy Impact Assessment Standard*** requires that CCO conduct and review privacy impact assessments (**PIAs**) on existing and proposed data holdings involving PHI, it describes the components of a PIA, when it is required at CCO, the scope of the assessment, the responsibilities of various departments for conducting PIAs at CCO, and the process and responsibilities for implementing PIA recommendations.

83. ***Privacy Inquiries and Complaints Procedure*** describes how CCO responds to inquiries and complaints received from individuals who are requesting information or challenging CCO's compliance with its information practices. Specifically, the procedure describes how an individual can make an inquiry or complaint, the steps which the LPO will follow in responding to and tracking the inquiry or complaint, and how compliance with the procedure is enforced at CCO.

84. ***Procurement Documentation and Records Management Procedure*** supplements CCO's *Procurement of Goods and Services Policy*, to describe how documentation relating to procurements at CCO, including agreements entered into between CCO and third party service providers, are to be managed.

85. ***Procurement of Goods and Services Policy*** ensures that CCO acquires the goods and services required to meet its business needs through the appropriate CCO procurement process.

86. ***Procurement Policy*** specifies the responsibilities of the Board, senior management and business units within CCO throughout each stage of the procurement process, and sets out requirements for the protection of PHI in the context of the procurement of goods/services that could result in privacy risk.

87. ***Progressive Discipline Policy*** identifies the type of conduct that may result in disciplinary action, and establishes the steps to be followed in the progressive discipline process. The *Privacy Breach Management Policy* complements the *Progressive Discipline Policy*, as it describes how CCO identifies, investigates, manages and resolves privacy breaches which occur as the result of misuse or improper/ unauthorized disclosure of PHI by CCO employees, consultants and contractors.

88. ***Secondment Policy*** sets out the necessary requirements for retaining an employee from an external organization who transfers to CCO temporarily to work in a job for a defined period of time, and where CCO reimburses the organization for the secondee while the individual continues to be employed by their organization, not CCO.

89. ***Secure Transfer of Personal Health Information Policy*** establishes an enterprise-wide framework of approved methods for the secure transfer of PHI into, within, and out of the custody of CCO. This policy governs the approved methods for the transfer of paper and electronic records containing PHI, and establishes accountability and enforcement measures that must be implemented to ensure that PHI is transferred in a secure manner.

90. ***Secure Transfer of Personal Health Information Standard*** sets out duties and responsibilities with respect to secure transfer of PHI, and defines the approved methods of securely transferring PHI.

91. ***Security Audit, Testing, and Compliance Standard:*** The standard defines the baseline practices for the audit and testing of CCO's information security. The internal audit and testing program is organized around the following core information system audit functions: compliance and conformance auditing, risk identification and control auditing, and operational auditing.

92. ***Security Operations Working Group Terms of Reference***: The Security Operations Working Group (**SOWG**) is established to facilitate and support the effective delivery of operational security work that spans Service Management, Operational Services, and the Enterprise Information Security Office (**EISO**).

93. ***Security Risk Management Standard*** defines the approach by which CCO identifies, assesses, responds to and monitors information security risks. The standard establishes a foundation for managing security risks, and delineates the boundaries for risk-based decisions within the organization. It applies strictly to the management of security risks within the purview of the Enterprise Information Security Program (**EISP**).

94. ***Services Agreement - Template Schedule for Third Party Agreements*** is a Services Agreement that contains a template schedule entered into between CCO and third parties retained by CCO, such as contractors, consultants and third party providers that will be permitted to access and use PHI. The template schedule, together with the baseline terms of the main Services Agreement, sets out the privacy and security responsibilities of the third party in respect of PHI that it accesses, retains, transfers or disposes of on behalf of CCO, or where the third party provides electronic services to enable CCO to collect, use or disclose PHI.

95. ***Statement of Confidentiality*** is an agreement between CCO and persons working for or on behalf of CCO to preserve the confidentiality of all information not normally available to the public, including all PHI that the individual has access to in the course of performing their duties or services.

96. ***Statement of Information Practices*** describe CCO's practices with respect to the collection, use and disclosure of PHI. It also provides information for the public on access to PHI and provides them with the LPO's contact information, should there be any further questions or concerns.

97. ***Termination Monthly Reports*** are created by CCO's Human Resources Department. It is sent on a monthly basis and summarizes a list of all employees who are no longer with CCO. This is used to ensure that system access has been suspended/deleted for those individuals who no longer work at CCO.

98. ***Termination of Employment Policy*** ensures that employees who have had their employment with CCO terminated are approached in a fair and equitable manner. The CCO *Employee Exit Process* and the CCO *Employee Exit Checklist* complement the *Termination of Employment Policy*, and describe the steps that managers must take in the case of termination of an employee.

99. ***Threat Risk Assessment Template*** is the EISO template for CCO's Threat Risk Assessment (**TRA**) Reports. It outlines the methodology involved in the security assessment, and provides a documentation structure for capturing the analysis of assets, threats, safeguards, vulnerabilities and risks.

100. ***Transfer of Personal Health Information by Regular Mail Procedure*** sets out the parameters for and roles and responsibilities when transferring PHI by regular mail.

101. ***Unpaid Student Intern Policy*** sets out the necessary requirements for retaining an unpaid student intern at CCO.

102. ***Video Monitoring Standard*** outlines the need and purpose for the use of video monitoring technologies on CCO premises, as well as the responsibilities for implementing and reviewing this policy. The *Video Monitoring Standard* has been drafted in conformance with the Information and Privacy Commissioner of Ontario (**IPC**)'s Guidelines for Using Video Surveillance in Public Places, as well as CCO's privacy and security policies.

103. ***Visitor Access Procedure*** outlines the procedures that must be followed by visitors and deliveries to CCO premises. Specifically, it stipulates the process for signing in (providing their name, date/time of their arrival, and the name of the CCO employee they are visiting) and obtaining a visitor's ID badge. The policy requires the Facilities Manager to maintain a log (*Visitor Logging System*) of all visitors to CCO's premises.

Appendix ii - Supporting Tools

1. ***CCO's Enterprise Information Security Office Program Logs*** include consolidated and centralized logs which track various components of the CCO security Program. Current logs include:

i. Log of Amended Policies & Procedures: controlled document library that tracks all interim amendments made to CCO's security policies, standards, and procedures. Communication of policy changes are also tracked, and include a description of the amendment made and the date it was communicated to CCO employees.
ii. Log of Security Audits: log of all security audits (TRAs, vulnerability assessments (VAs), penetration tests, security audits) initiated and/or completed at CCO. Results are logged into the Security Risk Register.
iii. Security Incident Log: log of information security breaches (including suspected breaches or "incidents").
iv. Open Media Logs: log of system backups.

2. ***CCO's Legal & Privacy Office Program Logs*** include consolidated and centralized logs which track various components of the CCO Privacy Program. Current logs include:

i. Log of Amended Policies & Procedures: tracks all amendments made to CCO's privacy policies and procedures, including a description of the amendment made and the date it was communicated to CCO employees.
ii. Log of Access Requests on the eCCO Data Access Request Tool: tracks executed Research Agreements between CCO and all researchers on the online eCCO Data Request Tool.
iii. Log of PIAs: tracks all PIAs initiated and/or completed at CCO, including identified risks and mitigating strategies.
iv. Log of Privacy Breaches: tracks all privacy incidents and breaches reported at CCO, including identified risks and mitigating strategies.
v. Log of Privacy Inquiries and Complaints: tracks all inquiries and complaints received by CCO in regards to the Privacy Program, including CSP.
vi. Log of IPC Recommendations: tracks the recommendations arising from the IPC's triennial reviews of CCO's IM practices and the manner in which these recommendations will be addressed.
vii. Log of Privacy and Security Training Completion: electronically tracks the completion of the privacy and security training curriculum through the electronic acceptance of a *Privacy and Security Acknowledgement Form*. Specifically, it electronically reconciles acceptance of the *Privacy and Security Acknowledgement Form* against the CCO Active Directory to ensure that all users of CCO systems have met their privacy training requirements.

viii. Log of Third Party Service Providers with Access to PHI ("Procurement Log"): tracks agreements with third parties that have access to PHI and includes the relevant dates associated with the agreement and transfer of data, the relevant business lead and responsibilities, a description of the services contracted for, and details regarding the return or destruction of the data.

3. ***CCO's Payroll System*** is maintained by CCO's Human Resources Department, and tracks all CCO employees who have executed CCO's *Statement of Confidentiality*.

4. ***Contract Management System*** is a centralized repository of agreements which CCO has entered into with third party service providers, together with supporting procurement-related documentation.

5. ***Data Sharing Agreements Log*** is a log of executed data sharing agreements (**DSAs**) in a DSA Summary chart which maintains up-to-date information related to DSAs executed by CCO, such as the name of the person or organization from whom the PHI was collected or to whom the PHI was disclosed, the date the DSA was executed, the date the PHI was collected or disclosed, the nature of the PHI subject to the DSA, and the retention period terms and related dates.

6. ***Visitor Logging System*** is maintained by CCO's Facilities Department and tracks all visitors (*i.e.,* anyone who is not an employee or authorized consultant to CCO) to CCO premises. The log records each visitor's first name, last name, company, title, check in (data and time), check out (date) and the CCO employee who is receiving the visitor.

7. ***Enterprise Risk Register*** contains logs of all enterprise risks, as well as recommendations to mitigate and manage those risks.

8. ***Internal Data Access Request*** tool is used for the logging of internal non-research-related access and use of PHI. Internal Data Access Request (**IDAR**) is a web-based interactive application allowing CCO employees to fill and submit request forms for direct data access, to the existing CCO data holdings. The IDAR tool logs the name of the employee, job title of the employee, the data holding the employee will have access to, the application that will be used by the individual to access the data, the type of database environment to be accessed, the type of data requested, the expiration of permissions to the data, and the current status of the employees' access permissions.

9. ***Key Logging System***is maintained by CCO's Facilities Department, and is based on the information provided in the *New Employee Facilities & Information Technology Services Form*, which documents each CCO employee's access permissions to the various floors of CCO's premises.

10. ***List of Data Linkages*** is maintained by the CCO's Informatics Department, and tracks the approved data linkages as defined by *CCO's Data Linkage Standard*.

11. ***Physical Security Access Card Log*** is maintained by the Facilities Coordinator and is a log of agents with access to CCO facilities. It is used at sites that do not have Key Scan Software. When notification from IT Service Desk is received, the Log is updated to reflect the termination of an employee/agent or change in access requirements.

12. ***Privacy Risk Register*** contains logs of all privacy risks, as well as recommendations to mitigate and manage those risks. The log includes risks or recommendations identified through PIAs, privacy audits, privacy reviews, complaint investigations, breach reports, and IPC reviews.

13. ***Security Risk Register*** registers security risks and the corresponding asset, vulnerability, and impact information. The log aggregates risks identified through TRAs, security audits, security reviews, incidents, and operational security activities.