



REPORT PREPARED FOR THE OFFICE OF THE INFORMATION
AND PRIVACY COMMISSIONER OF ONTARIO IN RESPECT
OF PHIPA REQUIREMENTS FOR REVIEW AND APPROVAL
OF PRESCRIBED PERSONS AND PRESCRIBED ENTITIES

INSTITUTE FOR CLINICAL EVALUATIVE SCIENCES (ICES)

Submission 31 August 2011



**REPORT PREPARED FOR THE OFFICE OF THE INFORMATION AND
PRIVACY COMMISSIONER OF ONTARIO IN RESPECT OF PHIPA
REQUIREMENTS FOR REVIEW AND APPROVAL OF PRESCRIBED
PERSONS AND PRESCRIBED ENTITIES**

INSTITUTE FOR CLINICAL EVALUATIVE SCIENCES (ICES)

**SUBMISSION
31 AUGUST 2011**

Table of Contents

Introduction	5
Background.....	5
Part 1 - Privacy Documentation	12
1. Privacy Policy in Respect of ICES' Status as Prescribed Entity	12
2. Policy and Procedures for Ongoing Review of Privacy Policies, Procedures and Practices.....	20
3. Policy on the Transparency of Privacy Policies, Procedures and Practices	21
4. Policy and Procedures for the Collection of PHI.....	22
5. List of Data Holdings Containing PHI.....	25
6. Policy and Procedures for Statements of Purpose for Data Holdings Containing PHI	25
7. Statements of Purpose for Data Holdings Containing PHI.....	26
8. Policy and Procedures for Limiting Agent Access To and Use of PHI.....	26
9. Log of Agents Granted Approval to Access and Use PHI.....	33
10. Policy and Procedures for the Use of PHI for Research	34
11. Log of Approved Uses of PHI for Research.....	34
12. Policy and Procedures for Disclosure of PHI for Purposes other than Research	34
13. Policy and Procedures for Disclosure of PHI for Research Purposes and the Execution of Research Agreements	36
14. Template Research Agreement	42
15. Log of Research Agreements.....	43
16. Policy and Procedures for the Execution of DSAs	43
17. Template Data Sharing Agreement.....	44
18. Log of Data Sharing Agreements	45
19. Policy and Procedures for Executing Agreements with Third Party Service Providers in Respect of PHI.....	45
20. Template Agreement for All Third Party Service Providers	46
21. Log of Agreements with Third Party Service Providers.....	47
22. Policy and Procedures for the Linkage of Records of PHI.....	47
23. Log of Approved Linkages of Records of PHI.....	50
24. Policy and Procedures with Respect to De-identification and Aggregation.....	51
25. Privacy Impact Assessment Policy and Procedures.....	54
26. Log of Privacy Impact Assessments.....	57
27. Policy and Procedures in Respect of Privacy Audits.....	57
28. Log of Privacy Audits.....	59
29. Policy and Procedures for Information (Privacy/Security/Policy) Breach Management	59
30. Log of Privacy Breaches	63
31. Policy and Procedures for Privacy Complaints and Privacy Inquiries	64
32. Log of Privacy Complaints & Privacy Inquiries.....	67
33. Policy and Procedures for Privacy Inquiries.....	68
Part 2 - Security Documentation	69
1. Information Security Policy	69
2. Policy and Procedures for Ongoing Review of Security Policies, Procedures and Practices.....	72
3. Policy and Procedures for Ensuring Physical Security of PHI.....	73
4. Log of Agents with Access to ICES Premises.....	77
5. Policy and Procedures for Secure Retention of Records of PHI and de-identified Information	77
6. Policy and Procedures for Secure Retention of Records of PHI on Mobile Devices	79
7. Policy and Procedures for Secure Transfer of Records of PHI	81
8. Policy and Procedures for Secure Disposal of Records of PHI.....	83

Table of Contents

9.	Policy and Procedures Relating to Passwords	86
10.	Policy and Procedures for Maintaining and Reviewing System Control and Audit Logs	87
11.	Policy and Procedures for Patch Management	87
12.	Policy and Procedures Related to Change Management	89
13.	Policy and Procedures for Back-Up and Recovery of Records of De-identified Information and PHI ...	94
14.	Policy and Procedures on the Acceptable Use of Technology	95
15.	Policy and Procedures in Respect of Security Audits.....	97
16.	Log of Security Audits.....	99
17.	Policy and Procedures for Information Security Breach Management	104
18.	Log of Information Security Breaches.....	109
Part 3 - Human Resources Documentation.....		113
1.	Policy and Procedures for Privacy/Security Training and Awareness	113
2.	Log of Attendance at Initial Privacy/Security Orientation and Ongoing Privacy/ Security Training	119
3.	Policy and Procedures for the Execution of Confidentiality Agreements by Agents.....	119
4.	Template Confidentiality Agreement with Agents	121
5.	Logs of Executed Confidentiality Agreements with Agents	121
6.	Job Description for the CPO	122
7.	Job Description for the CISO.....	122
8.	Policy and Procedures for Termination or Cessation of the Employment or Contractual Relationship ..	123
Part 4 - Organizational and Other Documentation		125
1.	Privacy and Security Governance and Accountability Frameworks	125
2.	Security Governance and Accountability Framework.....	130
3.	Terms of Reference for Committees with Roles with Respect to the Privacy Program and/or Security Program.....	130
4.	Corporate Risk Management Framework.....	130
5.	Corporate Risk Register.....	133
6.	Policy and Procedures for Maintaining a Consolidated Log of Recommendations	133
7.	Consolidated Log of Recommendations.....	134
8.	Business Continuity and Disaster Recovery Plan.....	135
Appendix One: Privacy Indicators		138
Security Indicators.....		156
Human Resources Indicators		164
Organizational Indicators		169
Appendix Two: List of ICES Data Holdings Containing PHI		171
Appendix Three: Recommendation Table.....		178
Appendix Four: Deficiencies to be Addressed/Timelines.....		188
Appendix Five: Registry of the Canadian Stroke Network.....		195
Appendix Six: Affidavit.....		201

INSTITUTE FOR CLINICAL EVALUATIVE SCIENCES (ICES) IPC Report

Introduction

The Institute for Clinical Evaluative Sciences (ICES) is an independent, not-for-profit, charitable organization that collects personal health information (PHI) in order to analyze and evaluate the effectiveness, quality, equity and efficiency of health care and health-related services in the Province of Ontario. The goal of these analyses and evaluations is to inform and assist decision- and policy-makers, clinicians and other service providers in managing, evaluating, monitoring and planning the delivery of health services and in improving outcomes of care¹.

Background

Since its inception in 1992, ICES has played a key role in providing unique scientific insights to help policymakers, managers, planners, practitioners and researchers shape the future direction of the Ontario health care system. Unbiased, evidence-based knowledge and recommendations, profiled in atlases, investigative reports, and peer-reviewed journals, are used to guide decision-making and inform changes in health care delivery.

Initially included in the Regulation to the *Health Cards and Numbers Act* 1991, ICES has had the privilege of access to individual health card numbers to potentiate linkage of data across the large administrative databases of the Ontario Ministry of Health and Long Term Care (MOHLTC). Using these data, generated by the day-to-day workings of the health care system, ICES' multi-disciplinary expertise facilitates the assessment of care delivery, patterns of service utilization, health technologies, drug therapies and treatment modalities. Linked data allows scientists to obtain a more comprehensive view of specific health care issues that could not be achieved with unlinked data. The ability to link individual-level health information **anonymously** using unique identifiers (ICES-encrypted health card numbers, called IKNs) to create cohorts of thousands of patients, potentiates the statistical power of massed data while ensuring the privacy and confidentiality of health information. ICES statistical and evaluative studies contribute to research excellence, policy debate and effective, sustainable changes in Ontario's health care system. Since ICES first began collecting PHI through its foundational agreement with the MOHLTC, ICES has had in place privacy/security policies, practices and procedures to protect the privacy interests of Ontarians whose data we have the privilege to use.

Over a decade later, on November 1, 2004, the *Personal Health Information Protection Act* (PHIPA) came into effect. The Office of the Information and Privacy Commissioner of Ontario

¹ THE INFORMATION AND PRIVACY COMMISSIONER/ONTARIO. *REPORT OF THE INFORMATION AND PRIVACY COMMISSIONER/ONTARIO. Three-Year Review of the Institute for Clinical Evaluative Sciences, a Prescribed Entity under the Personal Health Information Protection Act*; p3

Introduction

(IPC) was designated as the oversight body responsible for ensuring compliance with PHIPA. PHIPA establishes rules for the collection, use and disclosure of PHI by health information custodians (HICs)² that protect the confidentiality of, and the privacy of individuals with respect to, PHI. In particular, PHIPA provides that HICs may only collect, use and disclose PHI with the consent of the individual to whom the PHI relates or as permitted or required by the Act.

However, section 45(1) of PHIPA permits HICs to disclose PHI without consent to certain prescribed entities for the purpose of analysis or compiling statistical information with respect to the management of, evaluation or monitoring of, the allocation of resources to or planning for all or part of the health system, including the delivery of services, provided the prescribed entities meet the requirements of section 45(3).

Section 45(3) of PHIPA requires each prescribed entity 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. Section 45(3) further requires each prescribed entity to ensure that these practices and procedures are reviewed and approved by the IPC in order for HICs to be able to evaluate the acceptability of disclosure of PHI to the prescribed entity without consent. Section 45 (4) of PHIPA requires this review and approval be conducted tri-annually by the IPC.

ICES, was named as a prescribed entity on November 1, 2004, and underwent review/approval of its policies, practices and procedures for the first time on October 31, 2005. Following a second statute-mandated review by the IPC, ICES had its status renewed on October 31, 2008. While the IPC was satisfied that ICES had practices and procedures in place that sufficiently protected the privacy of individuals whose PHI it received and sufficiently protected the confidentiality of that information in both instances, the IPC did make certain recommendations to further enhance these practices and procedures. The recommendations made during the 2005 and 2008 reviews to improve and bolster ICES' privacy and security program have been included in this document.

Section 18(2) of Regulation 329/04 to PHIPA further requires each prescribed entity to make publicly available a plain language description of its functions³. This includes a summary of the, practices and procedures described above to protect the privacy of individuals whose PHI it receives and to maintain the confidentiality of that information.

Review Process

PHIPA requires that, as a prescribed entity, ICES have in place practices and procedures to protect the privacy of individuals whose PHI has been collected. These practices and procedures must be reviewed by the IPC every three years from the date of their initial approval in order for HICs to be able to continue to disclose PHI to ICES without consent and in order for ICES to be

² See http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_04p03_e.htm#BK4 for definition.

³ See http://www.ices.on.ca/webpage.cfm?site_id=1&org_id=119 for public information brochure.

Introduction

able to continue to collect, use and disclose PHI without consent as permitted by PHIPA and the regulation to PHIPA.

The IPC has prepared the *Manual For The Review and Approval of Prescribed Persons and Prescribed Entities* (the Manual) to outline the new review process that will be followed, commencing January 31, 2010. The Manual sets out in detail the obligations imposed on such entities arising from the new review process.

Throughout the Manual, prescribed entities are asked to comment on overall compliance and audit processes across a span of corporate-wide activities.

Pursuant to the Manual, ICES must submit a detailed written report and sworn affidavit to the IPC, one year prior to the date that the continued approval is required pursuant to PHIPA and its Regulation.

The Manual has four appendices with which ICES must demonstrate compliance in a written report. Within the Manual, Appendix A lists all of the categories of documentation that prescribed entities like ICES are required to have in place and submit for review; Appendix B lists the minimum required content for each category of required documentation; Appendix C lists Privacy and Security Indicators, additional factors that must be reported on, in order to assess the performance of the entity's privacy and security programs, including their policies, procedures, practices, standard operating procedures, tools and guidelines; and Appendix D includes the affidavit sworn by ICES' President & Chief Executive Officer (CEO).

Upon receipt, the IPC will review the written report and accompanying sworn affidavit and decide, in its sole and absolute discretion, whether further action is required on the part of the prescribed entity prior to the continued approval of its practices and procedures.

Provided any further required actions are taken in a timely manner and to the satisfaction of the IPC, or in the event that no further action is warranted, the IPC will advise ICES, in writing that it continues to meet the requirements of PHIPA and its Regulation. This is subject to any further actions that the IPC may require ICES to take prior to the next scheduled review of its practices and procedures.

About this Report

The following document is ICES' revised submission to the IPC in response to the requirements for the review and approval of Prescribed Persons and Prescribed Entities for review year 2011. ICES was previously approved by the IPC as per the requirements of section 45 (3) and section 45 (4) on 31 October 2005 and 31 October 2008.

It is important to document at the outset that at the time of the initial review of its practices and procedures in 2005, ICES was geographically located at one site. Since that time, ICES has

Introduction

maintained its posture as a single organization, but it is now geographically located at three sites⁴. These sites are now referred to as “ICES Expansion Sites.”

The IPC, with each of these sites, has assisted ICES by allowing the presentation of and reviewing documentation related to the plans for each ‘build’, and made a site visit after the build was completed. Additionally, the IPC has been provided with reports and presentations on all Security Testing, Threat-Risk Assessments and Penetration Testing prior to the opening of all sites. As is ICES’ usual practice, these reviews are performed at all sites in an ongoing fashion.

All sites are committed in Memoranda of Understanding (MOUs) to the same culture of diligence related to the security of the data and protection of the privacy rights of individuals. Each expansion site, under the guidance of a Local Privacy Officer and Site Director, is required to adhere to all privacy and security policies, practices, standard operating procedures (SOPs) and other procedures, standards, tools and guidelines implemented by ICES, as reviewed and approved by the IPC. All sites routinely undergo third party security reviews, penetration testing and threat-risk assessment and associated policy review annually by independent third –party reviewers.

The first expansion site, known as ICES@Queen’s, was opened at Queen’s University in October 2007 (<http://ices.queensu.ca/index.html>). ICES@Queen’s was part of ICES’ 2008 review by the IPC.

A second expansion site, located on the Civic Campus of The Ottawa Hospital and known as ICES@uOttawa, opened in June 2010 (<http://www.ohri.ca/icesuottawa>).

Two other expansion sites have been approved by the ICES Board of Directors and are preparing formal proposals for presentation to the IPC. These are located in the Health Promotion, Measurement and Evaluation (HPME) Department at the University of Toronto (known as ICES@uToronto), and at the University of Western Ontario, known as ICES@Western. Construction is anticipated in 2011. Other sites are currently being contemplated for the future (McMaster University, the Northern Medical School and University of Waterloo). More information related to the expansion sites is located throughout the document: however, it is important to note that ICES regards the construct of ICES-Central and the expansion sites as one entity, with mutual goals and interests, all of which are governed by the same policies, SOPs, other types of procedures, standards, tools, practices and guidelines. All sites undergo privacy audits and security reviews which are conducted concomitantly across the network.

This report tries to map closely to the Manual itself. It follows the table of contents in Appendix A and covers the required content in Appendix B. All ICES documents referenced in the report have been named in appropriate footnotes. The requirements of the Manual are included in tables labelled as Parts 1-4 and are attached as the Indicators’ Appendix at the back of the report (see Appendix ONE). An up-to date list and brief description of ICES’ data holdings of PHI and Statements of Purpose will be found in Appendix TWO. Appendix THREE presents a

⁴ THE INFORMATION AND PRIVACY COMMISSIONER/ONTARIO. *REPORT OF THE INFORMATION AND PRIVACY COMMISSIONER/ONTARIO. Three-Year Review of the Institute for Clinical Evaluative Sciences: a Prescribed Entity under the Personal Health Information Protection Act*; p3

Introduction

spreadsheet of Recommendations from the IPC's tri-annual review of ICES and the changes executed as requested. Appendix FOUR lays out a table of deficiencies and timelines, to complete tasks related to types of documents and logs that the Manual requires that ICES does not currently have in place or has not yet completed. Appendix FIVE contains up-to-date information related to activities around the migration of the Registry of the Canadian Stroke Network (RCSN), which is being brought into ICES as one of its clinical registries under section 45. Finally, Appendix SIX provides the affidavit that is to be sworn by ICES' CEO.

To help inform readers of this document, some important general points related to ICES as an organization are listed below. ICES' commitment to transparency, accountability and accessibility, like its commitment to securing all health data assets and protecting the privacy interests of Ontarians, is infused throughout most, if not all, of its policy instruments.

1. At ICES, the term "Agents" includes all scientists, adjunct and collaborating scientists, staff of all types, students, contractors and external consultants.

It is mandatory for ALL Agents to sign confidentiality agreements annually. The Confidentiality Agreement expressly obligates the signator to comply with **all** ICES policies, SOPS, other types of procedures, standards, tools, practices and guidelines.

The only Agents who have access to PHI at ICES are (1) **named, authorized data covenantors and (2) abstractors (usually clinically-trained individuals)**, who de-identify PHI as a "first use" of PHI at ICES, prior to its use for statistical and evaluative purposes. Access to data for all other Agents – for approved statistical and evaluative purposes – is only provided once the process of de-identification has occurred.

As part of its privacy and security posture, ICES segregates roles and duties based on access to PHI. In this report, we will identify roles by name when necessary for purposes of clarification.

2. ICES has a corporate policy related to annual review, and new policies specifically related to privacy and security policy review have been drafted. Because technology evolves and privacy best practices change rapidly, we consider many of our policies, practices, SOPS and other procedures, tools, guidelines and standards as *living* rather than static documents. Documents may be reviewed informally more frequently as a consequence.

Importantly, it should be noted that resources, both human and financial, have constrained these review activities. As reported to the IPC in other correspondence, the extended period of time committed to drafting this Report and ICES internal reorganization and expansion has stretched availability of human resources for these formal functions. This is clearly noted in Appendix Four: Table of Deficiencies for remediation.

3. ICES, uses ***a variety of policy instruments***, rather than simply policies, including SOPS, other types of procedures, standards, tools, practices and guidelines. We believe that in

Introduction

some chosen situations, these various instruments may be more practical, because they provide the opportunity for *nimbleness* in an environment where e-pressures are forcing change in best practices for privacy and security. We believe that guidelines and standards provide sources of expert opinion, which inform decision-making suitable to some of our circumstances. They are experiential documents from which we learn. Ultimately, however, all of these ‘types’ of instruments are intended to provide pathways to effective security/privacy best practices and we believe provide equivalence. ICES requires ALL Agents to comply with its’ policies, SOPS and other types of procedures, standards, tools, practices and guidelines. Where ICES does not have a specified policy instrument, but the intent is captured in other documents which are *at par*, those documents will be listed with specifics of how it meets required standards. Where we believe we are deficient, and agree that we should develop the specific policy or procedure suggested, we will state this explicitly, include it in Appendix Four: Table of Deficiencies, define an action plan to address the deficiency – and a time frame in which we anticipate completing the plan. In this Report, we will use the word “policies” to include this suite of instruments.

4. Audit programs are conducted internally by various ICES Agents and by external third-party Agents, including security audits, threat-risk assessments, penetration testing – and social engineering experiments (among others), to measure compliance with policies. We encourage a “respectful” privacy and security culture among our Agents, mindful of the privilege of the use of Ontarians’ health data. Information privacy and security programs at ICES are risk-based and also serve to inform our executive and Board.
5. ICES acknowledges the differences between section 44 (disclosure for research) and section 45 (disclosure for planning and management of the health system) of PHIPA. ICES collects PHI from the MOHLTC as per its’ long-standing agreement for the purposes articulated in ICES’ Mandate, Mission and Goals, which are concordant with section 45 purposes of evaluating, analyzing and compiling statistical information in relation to “*the management of, evaluation or monitoring of, allocation for resources to or planning for all or part of the health system, including the delivery of services*”⁵.

Agents are always asked to categorize planned projects as to the applicable section of PHIPA on the first page of ICES project-specific Privacy Impact Assessment (PIA) form to be absolutely sure of the purpose of the science planned; this document was previously reviewed by the IPC. A Briefing Note and Schematic, also previously sent to the IPC, were prepared to assist ICES scientists in this decision. Use of the data is always in a de-identified format, not as PHI. For purposes of this document and for greater clarity, we will endeavour to use the word “scientist” or “analyst” instead of researcher and the words “project” or “statistical and evaluative research” or “study” in lieu of “research” to reduce misperceptions of planned uses.

6. ICES has a policy of ***non-disclosure*** of PHI as per its’ agreement with the MOHLTC, which retains the rights to the data; disclosure would only occur *when instructed*

⁵ *Personal Health Information Protection Act, 2004; Section 45*

Introduction

explicitly / in writing by the MOHLTC (as to another prescribed entity under O. Reg 329/04 section 18(3)), or when compelled by a court order.

Part 1 - Privacy Documentation

General Privacy Policies, Procedures and Practices

1. Privacy Policy in Respect of ICES' Status as Prescribed Entity

ICES has developed an overarching approach in its *Privacy Code: Protecting Personal Health Information at ICES* (privacy policy) that sets out its commitment to protect the privacy rights of individuals whose PHI it receives. This commitment to protection of the privacy interests of Ontarians is at the core of all of ICES' policies, and informs ICES' actions and decisions at all levels of the organization. The *Privacy Code* is the backbone of ICES' overall privacy program.

Status under PHIPA

Section 45 of PHIPA permits HICs to disclose PHI to prescribed entities and authorizes prescribed entities to collect PHI for the purposes of analysis or the compiling of statistical information for the planning and management of a health system. In order to be a 'prescribed entity,' ICES must have 'practices and procedures' to protect the privacy of individuals whose information it receives and to maintain the confidentiality of the information. These in turn must be approved by the IPC. The 'practices and procedures' are subject to review by IPC every three years.⁶This report forms part of that review process.

ICES *Privacy Code: Protecting Personal Health Information at ICES* sets out ICES' status as a prescribed entity under section 45(1) of PHIPA. The *Privacy Code* describes how, consequently, ICES has implemented 'policies, procedures and practices' to protect privacy and the confidentiality of the information it receives and for ongoing review of these by the IPC. Further, the *Privacy Code* articulates ICES' commitment to comply with the provisions of PHIPA and its Regulation.

The *Privacy Code* builds on the Ten Guiding Principles (*CSA Model Code*) which are also foundational to PHIPA. The *Privacy Code* describes its status as a prescribed entity under PHIPA and the obligations that arise from this status. It further sets out the accountability framework for ensuring compliance with PHIPA and for ensuring adherence to the privacy and security policies implemented by ICES. ICES has also implemented numerous privacy and security policies that support the *Privacy Code*, including documents related to:

- Receiving, documenting, tracking, investigating and remediating privacy complaints;
- Protecting the confidentiality and security of PHI;
- Access to PHI and de-identified information;
- Research Ethics Board (REB) approval;

⁶ *Personal Health Information Protection Act, 2004; Section 45(3)*

Part 1 – Privacy Documentation

- Protecting PHI on mobile devices;
- Retention and destruction of records of PHI; and
- Identifying, containing, investigating, remediating and notifying of privacy breaches.

More recently, ICES has created a multi-pronged approach to privacy and security, and actively works to promote and nurture an organizational culture that emphasizes ICES' commitment to protect the privacy interests of Ontarians. This approach includes:

- Revision of ICES *Privacy Code: Protecting Personal Health Information at ICES*;
- Creation of a *Privacy Framework* and companion *Security Framework*;
- Website presentation of information related to privacy and security, including a clear public articulation of what ICES is and does (its *Mission, Mandate and Goals*), as well as copies of all statistical and evaluative studies conducted back to 1998 or earlier for the public to scrutinize;
- Information related to all ICES expansion sites;
- Information related to all ICES administrative data holdings and registries;
- Focussed, comprehensive policy instruments in effect in all parts of the organization;
- Focussed, privacy & security orientation, training/retraining and confidentiality agreements for all Agents.

Collectively, these components set out ICES' commitment to protect the privacy of individuals whose PHI it receives. This commitment to creating a culture where privacy and security protections is *mission critical* is at the core of all of ICES practices, and informs ICES' actions and decisions at all levels of the organization.

The CEO of ICES, who reports directly to the Board of Directors, is ultimately accountable for ensuring that ICES complies with *PHIPA* and its regulation and with the privacy and security policies implemented by ICES.

The Chief Privacy Officer (CPO), who reports directly to the CEO of ICES, has been delegated the day-to-day authority to manage the privacy program. The CPO is responsible for the development, implementation, review, maintenance and adherence to the suite of privacy policy instruments implemented by ICES and for ensuring compliance with *PHIPA* and its regulation. Some of the CPO's specific responsibilities are:

- Providing consultation and opinion to the CEO and ICES' Agents to ensure privacy best practices are operating in all projects;
- Developing, implementing and ensuring compliance with *Data Sharing Agreements(DSAs)*;
- Overseeing, directing or delivering privacy and security training;
- Facilitating and promoting activities to foster information privacy awareness; and
- Documenting, investigating and remediating privacy complaints and privacy breaches.

Additionally, each satellite site is also required to have a Local Privacy Officer (LPO) who reports to the CPO of ICES and to their Expansion Site Director. This on-site LPO is responsible

Part 1 – Privacy Documentation

for assisting in the development, implementation, review, maintenance and adherence of that expansion site to the suite of privacy and security policies implemented by ICES – and for assisting the CPO in ensuring that the expansion site complies with these policies.

ICES has in place a Chief Information Security Officer (CISO) who reports to the Senior Director, Research Operations but also reports directly to ICES' CEO on security concerns or problems. The CISO is responsible for the development of and oversight of the comprehensive security program at ICES and all ICES expansion sites. The CISO is supported by a senior security staff leader in the role of 'Security Lead'.

The CISO and Security Lead work closely with the CPO and LPOs.

ICES established a Privacy & Security Committee in 2009, replacing its original Confidentiality Committee (2000), with representation from each role group at ICES and each of the expansion sites. The Committee meets monthly or more frequently as needed. Its mandate is to provide role group-specific expertise, assist in the design, implementation, and evaluation of privacy and security at ICES, and help communicate issues of importance and change to Agents of the differing role groups.

ICES recognizes the vital importance of a clear accountability framework to ensure compliance with its own privacy and security policy instruments, as with PHIPA and its Regulation. Accountability must start at the top of the organization; therefore, ICES' *Privacy Code* clearly indicates that the CEO is ultimately accountable for such compliance. It also clearly indicates that day-to-day authority to manage the privacy program and security program has been delegated to the CPO and CISO respectively. The duties and functions of the key privacy and security roles and structures are clearly outlined in ICES' *Privacy and Security Frameworks*.

“ICES recognizes the vital importance of a clear accountability framework to ensure compliance with its own privacy and security policies, practices and procedures, as with PHIPA and its Regulation.

ICES' CEO is ultimately responsible for ICES' overall compliance with the suite of policy instruments. The CPO has day-to-day authority to manage the privacy program, and is responsible for the comprehensive privacy framework and ensuring that all studies are implemented/executed in accordance with current legal requirements and standards. The CISO is responsible for the day-to-day management of ICES' security program, and is responsible for the comprehensive security framework for the secure protection of the information. The duties and functions of these roles are further outlined in schematic fashion in ICES' Privacy and Security Frameworks (See Part 4, Section 1 for schematics). These individuals are directly accountable to the CEO, the Board of Directors, and, indirectly, the MOHLTC, and other stakeholders.”

Finally, ICES' *Privacy Code* clearly states that ICES remains responsible for the PHI used by its **Data Covenantors**. It identifies the policies implemented to ensure that its Data Covenantors

Part 1 – Privacy Documentation

only collect, use, retain and dispose of PHI in compliance with PHIPA and its regulation and in compliance with ICES’ privacy and security programs.

*"ICES is responsible for the PHI used by its Data Covenantors. Specifically, ICES’ policies ensure that its Data Covenantors only collect, use, retain and dispose of PHI in compliance with PHIPA and its regulation and in compliance with ICES’ privacy and security policies."*⁷

*"Designated ICES Data Covenantors are responsible for the day-to-day collection and processing of PHI. As a first use, all PHI will be de-identified and health card number encrypted prior to use for statistical and evaluative study purposes".*⁸

ICES’ mandatory *Confidentiality Agreement* requires all Agents to comply with *ICES Privacy Code* and all ICES’ policies at all times and in all situations. Furthermore, the *Confidentiality Agreement*, which must be signed annually, obligates the signatory not only to

*"...familiarize him/herself to and comply with all policies, practices and procedures of ICES relating to privacy and security, but also includes any policies, practices and procedures implemented from time to time after the date of signing the Agreement".*⁹

ICES Confidentiality Agreement is foundational to ICES’ privacy and security programs and to ICES’ culture. Noting that requirements related to policy instrument compliance are found in many sections of the Manual for this report, we would like to underscore for future requirements in this document that ICES clearly states in the *Confidentiality Agreement* that breach of the agreement may result in discipline, up to and including termination.

"You agree to notify ICES’ CPO in writing immediately upon becoming aware of any breach or any possible breach of this Agreement."

*"Any breach of this Agreement may result in disciplinary action being taken by ICES, up to and including a termination of any relationship you have with ICES, including without limitation any employment or other contractual relationship with ICES."*¹⁰

Collection of PHI

Entities prescribed under s.45 of PHIPA and its Regulation are permitted to collect PHI that is disclosed to them for purposes of analysis or compiling statistical information with respect to the management of, evaluation or monitoring of, the allocation of resources to or planning for all or part of the health system, including the delivery of services.

⁷ ICES Privacy Code: Protecting Personal Health Information at ICES Principle 1.3

⁸ ICES Covenantor Confidentiality Agreement

⁹ ICES Covenantor Confidentiality Agreement Clause 6

¹⁰ ICES Covenantor Confidentiality Agreement Clause 8 and 9

ICES' *Privacy Code* identifies at a high level the purposes for which PHI is collected, the types of PHI collected and the persons or organizations from which PHI is typically collected.

"ICES uses and/or collects PHI to conduct statistical analyses that contribute to the effectiveness, quality, equity, and efficiency of health care in the province of Ontario, as part of its unique mandate and partnership with the Ontario MOHLTC and multiple other stakeholders".¹¹

"PHI is transferred from one responsible custodian (such as the MOHLTC) to ICES with a chain of accountability for data protection. The legal authority to transfer (disclose) PHI to ICES for statistical and evaluative purposes is found in Section 45 of PHIPA. The disclosure of PHI to ICES by HICs as permitted in PHIPA is articulated in ICES' data-sharing agreements with HICs."¹²

These identified purposes are all consistent with PHIPA. Further, the *Privacy Code* articulates ICES' commitment not to collect PHI if other information will serve the purpose and not to collect more PHI than is reasonably necessary to meet the purpose.

"Identifying the purposes for which ICES uses and/or collects PHI before use/or collection allows careful determination of the information needed to fulfill the intended purpose. ICES uses and/or collects only the information necessary to meet the pre-identified written and ethically-approved purposes."¹³

In a separate document, a list of data holdings¹⁴ is available on the ICES website. Finally, the *Privacy and Security Frameworks*, together with postings on the ICES intranet, also outline the policies implemented to ensure these commitments are met.

Use of PHI

s.45 (6) of PHIPA provides that ICES may only use the use the PHI it receives for the purposes for which it is received. **ICES' consistent approach to PHI at the point of collection varies from other entities; the PHI is de-identified immediately.** Use of the de-identified information is targeted for PHIPA section 45 purposes.

ICES' first use of PHI collected is its management through the de-identification process by its named, authorized and designated *Data Covenantors*. The use of PHI for statistical and evaluative studies and other projects contravenes ICES core principles; de-identified and/or aggregate information is used.

"Designated ICES Data Covenantors are responsible for the day-to-day collection and processing of PHI. As a first use, all PHI will be de-identified"

¹¹ ICES *Privacy Code: Protecting Personal Health Information at ICES. Principle 2.1*

¹² ICES *Privacy Code: Protecting Personal Health Information at ICES. Principle 2.2*

¹³ ICES *Privacy Code: Protecting Personal Health Information at ICES Principle 2.2*

¹⁴ See this url: http://www.ices.on.ca/webpage.cfm?site_id=1&org_id=26&morg_id=0&gsec_id=5314&item_id=5322.

*and health card number encrypted prior to use for all analyses, statistical and evaluative studies, and other purposes.*¹⁵

All of ICES' uses listed above are consistent with the uses of PHI permitted by PHIPA and its regulation. Further, the *Privacy Code* articulates ICES' commitment not to use PHI if other information will serve the purpose and not to use more PHI than is reasonably necessary to meet the purpose.

*“Identifying the purposes for which ICES uses and/or collects PHI before use/or collection allows careful determination of the information needed to fulfill the intended purpose. ICES uses and/or collects only the information necessary to meet the pre-identified written and ethically-approved purposes.”*¹⁶

The ICES *Privacy Code* outlines the procedures and practices implemented, to ensure these commitments are met and identifies how limits are placed on the use of PHI by agents.

Disclosure of PHI

Although ICES has a policy of non-disclosure of PHI, ICES understands that PHIPA permits a prescribed entity to disclose PHI for research purposes in compliance with section 44 of PHIPA and to another prescribed entity for planning and management of the health system in compliance with section 45 of PHIPA. Additionally, PHIPA permits disclosures to prescribed registries for purposes of facilitating or improving the provision of health care pursuant to section 39(1)(c) and subsection 18(4) of the Regulation to PHIPA.

ICES' *Privacy Code* clearly distinguishes the circumstances in which and the purposes for which de-identified and/or aggregate information is disclosed. It documents that ICES reviews 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 utilized, alone or with other information, to identify an individual.

*“ICES does not disclose individual-level PHI that it uses or collects, as this would contravene its core agreements and approved policies, with one exception. ICES will only disclose unaugmented PHI to the organization from which it was collected upon request, as this disclosure is tolerated in its core agreements”.*¹⁷

Secure Retention, Transfer and Disposal of Records of PHI

Multiple documents support the secure retention, transfer and disposal of PHI.

¹⁵ ICES *Privacy Code: Protecting Personal Health Information at ICES. Principle 1.1*

¹⁶ ICES *Privacy Code: Protecting Personal Health Information at ICES. Principle 2.2*

¹⁷ ICES *Privacy Code: Protecting Personal Health Information at ICES. Principle 5.1 and 5.2*

Part 1 – Privacy Documentation

ICES' *Privacy Code* addresses, at a high level in Principles 5.1 and 5.2, the secure retention of records in both paper and electronic form. As a basic principle, ICES projects are managed in electronic format and are securely retained on ICES servers. All-paper records for collection are discouraged; however, if this modality is the only format available, records are de-identified at the site of collection and a unique number assigned to them. All paper documents are irreversibly shredded once they are coded into secured, in-house databases and validated (ICES *Data Destruction Policy* and ICES' *Shredding Policy*).

SOPs for both electronic erasure (ICES SOP DM003 *Destruction of Third Party Health Data, Original Medium, Backups and Project-created Datasets 2010*) and for physical destruction (ICES SOP *Destroying Hardware – DVDs, CDs, Floppies, Hard Drives, Memory Sticks/USB Keys 2008*) are in place.

Administrative datasets and all other datasets collected through *Data-Sharing Agreements* (DSAs) which contained PHI are de-identified as the first use, as previously mentioned. This is clearly articulated in the DSA.

Decisions on retention periods and destruction dates are also clearly stated in the pertinent DSA and on the *Project-Specific Privacy Impact Assessment* (PIA) form. Original cartridges and tapes of administrative data are documented and archived in a fire-proof bank safe behind four layers of secured doors with highest access restriction as part of ICES *Disaster Recovery Plan*.

Three documents – ICES' core agreement with the MOHLTC, the *Data Privacy Agreement for a Prescribed Entity Agreement, Guidelines for Importing External Data to ICES* and *ICES SSL-VPN User's Guide v1.0 2010* all address components of secure transfer of PHI.

Implementation of Administrative, Technical and Physical Safeguards

ICES's *Privacy Code* clearly states that ICES has in place administrative, technical and physical safeguards implemented to protect the privacy of individuals whose PHI, ICES receives and to maintain the confidentiality of that PHI.¹⁸

Additionally, *ICES Data Privacy Agreement for a Prescribed Entity Agreement 2006* with the MOHLTC requires the secure maintenance of the relevant PHI using administrative, technical and physical safeguards.

These safeguards, or controls, include steps taken to protect PHI against theft, loss and unauthorized use or disclosure and to protect records of PHI against unauthorized copying, modification or disposal.

“ICES has practices and procedures for ensuring confidentiality and security of data, which are strictly enforced in order to respect the privacy of users and providers of the health care system, and to protect data against loss, destruction or unauthorized use. ICES, as a section 45 prescribed entity, is responsible for

¹⁸ ICES *Privacy Code: Protecting Personal Health Information at ICES Principle 7*

Part 1 – Privacy Documentation

all data held in its possession or custody and has designated individuals who are accountable for ICES' compliance with PHIPA.

ICES recognizes the vital importance of a clear accountability framework to ensure compliance with its own privacy and security policy instruments, as with PHIPA and its Regulation”¹⁹.

Inquiries, Concerns or Complaints Related to Information Practices

ICES' Privacy Code, General Public Inquiry related to the Management and Protection of PHI Policy, ICES' Challenging Compliance Policy, ICES' website Privacy Statement and ICES website Public Information Brochure identify the CPO as the individual to whom individuals may direct inquiries, concerns or complaints relating to ICES' privacy procedures and practices, as well as ICES' compliance with PHIPA and its regulation. It also states that individuals may direct complaints regarding compliance with PHIPA and its regulation to the IPC and provides the contact information for the same.

“Information about ICES' policies and practices, as related to the management and protection of PHI, is available on ICES website – www.ices.on.ca Descriptions of studies in progress and publications from completed projects are also available on the ICES website, including:

- a) The name or title and address of the Agent accountable for ICES' policies and practices and to whom inquiries or complaints can be forwarded;*
- b) A description of the type of information held by ICES, including a general account of its use; and,*
- c) A copy of any public information brochures or other general information that explains ICES policies, standards or codes of practice”²⁰.*

“An individual can challenge compliance with the principles via the designated persons accountable for ICES' compliance. These individuals will generally include the CPO and the LPO at an expansion site, or their designate(s). Individuals may also make a complaint to the Office of the Information and Privacy Commissioner of Ontario (IPC) at www.ipc.on.ca or by calling 416-326-3333 (Toronto area) or 1-800-387-0073 (within Ontario).

- ICES has put simple and accessible procedures in place to receive and respond to complaints or inquiries about its policies and practices relating to the handling of PHI and all health information held at ICES.

- Individuals with inquiries or complaints will be informed in a timely fashion by ICES about relevant procedures.

- ICES will investigate all complaints in a timely fashion. If a complaint is found to be justified, ICES will take appropriate

¹⁹ ICES Privacy Code: Protecting Personal Health Information at ICES Principle 1, Principle 7

²⁰ ICES Privacy Code: Protecting Personal Health Information at ICES Principle 8

measure, including amending its policies, practices and procedures if necessary.”²¹

Transparency of Practices in Respect of PHI

ICES' *Privacy Code* and *Questions & Answers about Information Privacy Protection at ICES (FAQ)* identifies that individuals may obtain further information in relation to ICES' privacy procedures and practices from the CPO (address, email and phone number provided) or through privacy@ices.on.ca. Similar information is available on the ICES@Queen's website (<http://ices.queensu.ca/index.html>) and the ICES@uOttawa website at <http://www.ohri.ca/icesuottawa>

2. Policy and Procedures for Ongoing Review of Privacy Policies, Procedures and Practices

ICES is committed to the ongoing review of its privacy policies in order to determine whether any amendments are needed or whether new privacy policies are required. Specifically, ICES has developed a specific new policy for the annual *Review of Privacy and Security Policies, Practices and Procedures*. In undertaking formal review and determining whether amendments and/or new privacy and security policies are necessary, the review framework indicates that updates or changes to ICES' privacy and security policies will take into consideration:

- Any orders, guidelines, fact sheets and best practices issued by the IPC under *PHIPA* and its regulation;
- Evolving industry privacy and security standards and best practices;
- Amendments to *PHIPA* and its regulation relevant to the prescribed entity;
- Recommendations arising from privacy and security audits, privacy impact assessments and investigations into privacy complaints, privacy breaches and information security breaches;
- Whether the privacy and security policies, procedures and practices of ICES continue to be consistent with its actual practices; and
- Whether there is consistency between and among the privacy and security policies, procedures and practices implemented.

The policy requires review and revision/approval annually under the direction of ICES' CPO, CISO and their staff.

ICES communicates all updates or changes by ensuring that all documents available on ICES intranet are current and continue to be made available to all Agents at all ICES sites. Further, the CPO and CISO and their designates are responsible for working with the Director, Communications and staff to communicate the changes or additions by intranet posting, notification of Role Group leads and the corporate email system (listserve). As well, the CPO and CISO/Security Lead are responsible for determining the content of privacy and security re-training in collaboration with ICES' Human Resources (HR) Department.

²¹ ICES *Privacy Code: Protecting Personal Health Information at ICES. Principle 10*

ICES has been engaged in activities related to restructuring and expansion over the past three years in a resource-constrained environment. The CPO and CISO have prioritized certain activities such as comprehensive security reviews across the ICES' network, developing privacy and security frameworks, drafting new policies and SOPs to meet the evolving needs of the organization and careful scrutiny of findings to improve ICES' privacy and security posture. Formal review of all policies has yet to be undertaken: informal review is ongoing and in place. It is our intent to create opportunities for formal review and documentation, and plan to have these in place within the 2012 fiscal year, under the aegis of the Agents/CPO and CISO, once the press of restructuring and significant resource constraints allow (see Appendix Four: Deficiencies).

Transparency

Regulation 329/04, s.18 (2) of PHIPA provides that an entity that is a prescribed entity for the purposes of subsection 45 (1) of PHIPA shall make publicly available, a plain language description of the functions of the entity (see http://www.ices.on.ca/webpage.cfm?site_id=1&org_id=119), including a summary of the practices and procedures described in subsection 45 (3) of PHIPA. This document, *ICES Review of the Practices and Procedures of ICES* and ICES' *Approval* by the IPC, are provided on ICES website at www.ices.on.ca under the Privacy tab.

3. Policy on the Transparency of Privacy Policies, Procedures and Practices

ICES' commitment to transparency and accessibility is infused throughout most, if not all, of its policy instruments. For example, *ICES Privacy Code* describes ICES' commitment to the principle of openness and transparency, and describes generally the information made available to the public and other stakeholders relating to ICES' privacy policies, and identifies the means or media by which this information is made available. As such, ICES makes the *Privacy Code* accessible to the public through its external website (www.ices.on.ca). Other documentation is also available on the website, such as ICES' *Public Information* brochure and a *Frequently Asked Questions* document (FAQ), which together identify 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 the steps taken to protect the PHI against theft, loss, unauthorized use or disclosure and unauthorized copying, modification or disposal; documentation related to the review by the IPC of the policies implemented by ICES to protect the privacy of individuals whose PHI is collected and to maintain the confidentiality of that information; and, a list of the data holdings maintained by ICES. ICES lists important administrative and registry database holdings for the public as well. Additionally, in the spirit of accountability and transparency of purpose, the website identifies statistical and evaluative projects currently underway, and includes a comprehensive library of all reports and articles developed using Ontario's data over the last 19 years for the review of all interested parties.

Listings of all ongoing projects may be found at (http://www.ices.on.ca/webpage.cfm?site_id=1&org_id=2) and completed projects

(http://www.ices.on.ca/webpage.cfm?site_id=1&org_id=31) are viewable on the internet site. There is a comprehensive listing of ICES faculty, their scientific interests and contact information

(http://www.ices.on.ca/webpage.cfm?site_id=1&org_id=26&morg_id=0&gsec_id=6402&item_id=6402). Also included on the website is the name, title, and contact information for the CPO to whom inquiries, concerns or complaints regarding compliance with the privacy policies, procedures and practices implemented and regarding compliance with PHIPA and its Regulation may be directed.

This comprehensive approach ensures that ICES' status as a prescribed entity under PHIPA, the duties and responsibilities arising from this status and the privacy policies, procedures and practices implemented in respect of PHI are well known and understood.

ICES does not have a specific, stand alone policy on the content of public brochures or *Frequently Asked Questions* (FAQ) documents, as these documents have been previously approved twice by the IPC. ICES believes this objective and level of transparency have been met.

Collection of PHI

Entities prescribed under s.45 of PHIPA are permitted to collect PHI that is disclosed to them by HICs for the purpose of analysis or compiling statistical information with respect to the management of, evaluation or monitoring of, the allocation of resources to or planning for or part of the health system, including the delivery of services.

4. Policy and Procedures for the Collection of PHI

The Introduction and Sections 1 and 2 of ICES' *Privacy Code* identifies the purposes for which ICES collects PHI, the nature of the PHI that is collected, and from whom the PHI is typically collected. *ICES collects PHI under its DSAs but de-identifies the PHI as a first use; only de-identified information is used for statistical and evaluative studies.* The *Privacy Code* requires the ICES Privacy Officer to ensure that data-sharing agreements (DSAs) are always executed prior to collection of PHI to fulfill the identified and approved purposes²². This information has been presented previously in this report and has been previously approved by the IPC.

Sections 2 and 3 of ICES' *Privacy Code* and ICES' *Security Governance Framework* articulates ICES' commitment to the secure collection of PHI, which is supported by a comprehensive suite of policies and procedures. More specifically, ICES has developed several documents for its data providers: *Importing External Datasets to ICES Guidelines*; *ICES SSL VPN User's Guide*; and *ICES Off-line Chart Abstraction (OCA2)* and *SOP DM001 Receiving project-specific data sets from external sources* that offer options for the secure transmittal to ICES of PHI, based on best practices.

²² ICES Privacy Code. Principle 4.

*“ICES... collects PHI to conduct statistical analyses and evaluative studies that contribute to the effectiveness, quality, equity, and efficiency of health care in the province of Ontario, as part of its unique mandate and partnership with the Ontario MOHLTC and multiple other stakeholders”.*²³

*“Identifying the purposes for which ICES uses and/or collects PHI before... collection allows careful determination of the information needed to fulfill the intended purpose. ICES collects only the information necessary to meet the pre-identified written and/or ethically-approved purposes. PHI is transferred from one responsible organization (such as the MOHLTC, Cancer Care Ontario, among others) to ICES with a chain of accountability for data protection. The legal authority to transfer (disclose) PHI to ICES for statistical and evaluative studies is found in Section 45 of PHIPA and sections 13 and 18 of the PHIPA regulation. The disclosure of PHI to ICES by HICs and prescribed entities and prescribed persons as permitted in PHIPA and its regulation is articulated in ICES’ data-sharing agreements.”*²⁴

The ICES *Privacy Code*, *ICES Confidentiality Agreement* and all ICES policies require Agents to comply with the terms of these various instruments.

Review and Approval Process for Collection

DSAs are negotiated and executed by the Health Information Officer and CPO, generally in discussions with the agents of the HIC or other organization; they are approved by the CEO and an individual who has signing authority for the HIC or other organization disclosing the PHI.

ICES’ Health Information Officer and CPO, in collaboration with counterparts at data-providing organizations, establish data requirements. These requirements are related to the broad scope of projects with their relevant stakeholders, such as the MOHLTC. The data requirements are often part of routine annual feeds planned over several years, and are not reviewed until such time as amendment is required or the agreement is expiring. Occasionally, amendments to the minimum data sets are made at the same time. In many cases, external Advisory Committees comprised of representatives from the data-providing organizations and other key stakeholders provide advice and guidance on the variables optimal for collection. ICES is committed at all times, as stated in Sections 1 and 2 of ICES’ *Privacy Code*, to minimal data collection.

The CEO, Health Information Officer, Program Leaders, CPO and Investigator(s), in collaboration with leaders from various stakeholder agencies such as the MOHLTC, are responsible for reviewing and determining whether to approve ICES collection of PHI under structured DSAs with stakeholders such as the MOHLTC. However, the MOHLTC controls the frequency of review of data elements provided in the administrative data.

²³ ICES Privacy Code Section 2.1

²⁴ ICES Privacy Code Section 2.2

Part 1 – Privacy Documentation

Secure Retention of PHI Collected

Section 7 of ICES' *Privacy Code* articulates ICES' commitment to the secure retention of PHI, which is supported by a comprehensive suite of policies and procedures (i.e., *Note on the Secure Retention of Administrative Data at ICES*). ICES requires that all records of PHI be retained in a secure manner in accordance with ICES' *Policy and Procedures for Secure Retention of PHI*.

Secure Transfer of Collected PHI

As stated above, ICES has developed several documents for its data providers related to the secure transfer of PHI: *Importing External Datasets to ICES Guidelines*; *ICES SSL VPN User's Guide*; and *ICES Off-line Chart Abstraction (OCA2)* and *SOP DM001: Receiving project-specific data sets from external sources* all offer options for the secure transmittal to ICES of PHI, based on best practices.

ICES requires that any transfer or collection of PHI be conducted in a secure manner under the supervision of the Director, Information Management and/or designate and in accordance with ICES's *Policy and Procedures for Secure Transfer of Records of PHI*.

Secure Return and Disposal of Collected PHI

ICES' *Data Privacy Agreement for a Prescribed Entity* with the MOHLTC states that, consistent with its mandate and core functions, ICES may retain PHI for as long as necessary to meet the identified purposes. At such time as PHI is no longer required for ICES' purposes, it is disposed of in compliance with ICES' *Data Destruction Policy* and the related *SOP DM003: Destruction of 3rd Party Health Data*.

In other DSAs, dates of destruction are sought at the time of collection; the dates are tracked in a log and the data destroyed with notification as per ICES' *Data Destruction Policy* and the related *SOP DM003: Destruction of 3rd Party Health Data. Notification* in this context means that the Scientist of record for a project is notified of pending data destruction so that he/she is aware that this final step is being executed. A specified date for this notification is sought in the Project-specific Privacy Impact Assessment form (PIA), at the time the project begins.

Under the *Data Destruction Policy*, the Director, Information Management is responsible for ensuring that all records of PHI that have been collected are, at the end of their retention period or at the date of termination set out in any documentation or agreements executed prior to the collection, securely disposed of. Data is destroyed as that is the safest process. Records are to be disposed of in compliance with the *Policy and Procedures for Secure Disposal of Records of Personal Health Information*. The *Data Destruction Policy* stipulates that the Director, Information Management is responsible for ensuring that a *Data Destruction Certificate* is issued to the organization that provided the data that the data has been destroyed.

5. List of Data Holdings Containing PHI

ICES maintains an up-to date list of its data holdings of PHI which are archived in its vault. A list of Data Holdings and Statements of their Purposes, current as of the date of this report, can be found in Appendix TWO. Only de-identified information is used for statistical and evaluative purposes; original media is stored for disaster recovery purposes.

6. Policy and Procedures for Statements of Purpose for Data Holdings Containing PHI

ICES' general statements of the overall intended purpose of its data holdings are articulated in the *ICES Privacy Code*.²⁵ General statements of purpose set out:

- The purpose of the data holding;
- The source(s) of the PHI;
- The need for the PHI in relation to the identified general purposes

These general statements are consistent with ICES' articulated mandate, mission and goals. Furthermore, data holding-specific purpose statements are clearly articulated in every project-specific proposal and Privacy Impact Assessment (PIA) form. Finally, a synopsis of all projects is developed and posted on the ICES' website to give the general public a quick view and understanding of the data holding purpose, scope and usefulness, as previously mentioned in this report.

“ICES uses and/or collects PHI to conduct statistical analyses and evaluative studies that contribute to the effectiveness, quality, equity, and efficiency of health care in the province of Ontario, as part of its unique mandate and partnership with the Ontario MOHLTC and multiple other stakeholders.”

“Identifying the purposes for which ICES uses and/or collects PHI before use/or collection allows careful determination of the information needed to fulfill the intended purpose. ICES uses and/or collects only the information necessary to meet the pre-identified written and ethically-approved purposes. PHI is transferred from one responsible organization (such as the MOHLTC, Cancer Care Ontario, among others) to ICES with a chain of accountability for data protection. The legal authority to transfer (disclose) PHI to ICES for statistical and evaluative purposes is found in Section 45 of PHIPA. The disclosure of PHI to ICES by HICs as permitted in PHIPA and sections 13 and 18 of the PHIPA regulation. The disclosure of PHI to ICES by HICs, prescribed entities and prescribed persons as permitted in PHIPA and its regulation, is articulated in ICES' DSAs.”²⁶

ICES' policies require the de-identification of PHI and encryption of health card numbers immediately upon collection by designated **Data Covenantors**. PHI is **not** made available for

²⁵ ICES Privacy Code. Principle 2

²⁶ ICES Privacy Code. Principle 2.2

statistical and evaluative purposes and projects; only de-identified data is accessed by Agents at ICES and expansion sites on a common, highly-secured server.

ICES does not currently have a policy and procedures with respect to the creation, review, amendment and approval of statements of purpose for data holdings containing PHI that meets the requirements of the *Manual*. ICES' Privacy Officer will work with the IPC to develop an acceptable policy and procedures prior to the next scheduled IPC review in 2014 (see Appendix FOUR: Table of Deficiencies).

7. Statements of Purpose for Data Holdings Containing PHI

ICES' DSAs with the MOHLTC and other key stakeholders are explicitly directed at an overarching but fundamental purpose: statistical and evaluative studies that contribute to the effectiveness, quality, equity and efficiency of health care and health services in Ontario. A List of Data Holdings containing PHI and a discussion of general statements of purpose for these data holdings can be found in Appendix TWO. These purposes are seminal components of section 45 (1) of PHIPA, which guides ICES in its work, and is the source of its designation as a prescribed entity. Key objectives are to: (1) carry out population-based health services research that is relevant to clinical practice and health policy development; (2) document province-wide patterns and trends in health care delivery; and, (3) develop and share evidence to inform decision-making by policy makers, managers, clinicians, planners and consumers. A copy of the Data Privacy Agreement with the MOHLTC has been provided to the IPC previously.

These general purposes are posted on ICES website, and are integral to the Umbrella Agreement between ICES and the MOHLTC.

“...a viable and effective business relationship has evolved between the MOHLTC and ICES, and whereas ICES has contributed, and continues to contribute essential research [statistical and evaluative studies] to address health research priorities...”²⁷

As previously described, all statistical and evaluative projects conducted by ICES' Agents must clearly state the purpose of the use of the de-identified data in the documentation or the project, required as part of the approvals process. It is a scientific requirement that all projects align with ICES' mission and goals.

8. Policy and Procedures for Limiting Agent Access To and Use of PHI

ICES takes reasonable steps in relation to all accesses to and uses of the PHI in its data holdings. This includes limiting Agent access to and use of PHI. ICES has two types of Agents who access and use PHI: data covenantors and chart abstractors.

²⁷ *Umbrella Agreement between Her Majesty the Queen in Right of Ontario as represented by the MOHLTC and ICES 1 April 2008 p1*

Data Covenantors

ICES' *Access to Health Data Policy* clearly sets out the limited and narrow circumstances under which ICES' data covenantors may access and use PHI. A foundational principle of its privacy and security framework, ICES has segregated the roles and responsibilities of Agents, where feasible and possible, based on a need-to-know requirement related to job performance, to avoid a concentration of privileges. This policy describes the levels of access that may be granted and also describes how ICES ensures that the duties of data covenantors with access to PHI are segregated, in order to avoid a concentration of privileges that would enable a single Agent to compromise PHI. These Agents are responsible for the collection and first use de-identification of PHI.

*“As a Prescribed Entity under PHIPA, ICES is authorized to collect and use PHI for the purposes of section 45 of PHIPA, including statistical and evaluative studies of the health system. One of the principles of Fair Information Practices is to limit use, disclosure and retention of PHI. ICES' intention with respect to the access to Health Information (HI) is to limit it on an 'as needed' basis to appropriate Agents. Access to PHI is further limited to brief periods of use by a small number of designated staff for the purposes of collection and de-identification”.*²⁸

“Any PHI (or HI) collected or received by ICES will be considered to have entered the ICES domain once it is: a) contained within an ICES portable electronic device such as a lap-top computer; b) transmitted to an ICES server (SSL-VPN); or c) delivered to an ICES physical site on a portable storage device such as a CD, USB key or tape cartridge or on a non-electronic medium such as paper or micro-fiche. This policy defines the circumstances under which ICES' Data Covenantors may access PHI (or HI) within the ICES domain regardless of the data-sharing agreement governing the possession of the PHI”.

*“Any PHI within the ICES domain may only be accessed by Primary Data Covenantors or Administrative Data Covenantors”.*²⁹

ICES' data Covenantors are authorized to “use” PHI for the purpose of de-identification.

An *Administrative Data Covenantor* is defined as:

*“An ICES employee named in data-sharing agreements and identified to the IPC, who can access PHI at ICES in any allowable setting for the purposes of receiving, transferring or destroying PHI or for the encryption of personal identifiers or for data linkage using personal identifiers.”*³⁰

²⁸ ICES *Access to Health Data Policy*. pp1-2

²⁹ ICES *Access to Health Data Policy*. pp1-2

³⁰ ICES *Access to Health Data Policy* p4

Part 1 – Privacy Documentation

A *Primary Data Covenantor* is defined as:

*“An individual named in our data sharing agreements and identified to the IPC, who can access PHI at ICES in any allowable setting other than the UNIX system for the purposes of receiving, transferring or destroying PHI”.*³¹

Abstractors

A second type of ICES Agent who is permitted access to PHI – **chart abstractors** – review and abstract project-specific medical records within the confines of hospital/office medical records departments. These Agents are generally clinicians (experienced nurses and physicians, usually) who abstract clearly-chosen and -defined clinical variables required to meet an articulated purpose. In this circumstance, the health information is always collected from the source in a de-identified fashion, under a unique identifier related to a medical record number mapped in a “key” that is kept separately and securely from the health information. These Agents are engaged for the duration of the project only; ICES makes project-specific arrangements with hospital Medical Records Departments related to the required records, the named Agents and the specific day/s of the work assignment. Access to charts is terminated for each site at the time the abstraction is completed.

The PHI is further de-identified by the data covenantors when abstraction is complete/ information has been rendered linkable with encrypted health card number.

These individuals are additionally bound by the oaths of their professions. All of these Agents undergo small group session training related to the project, which includes: using project-specific templates for variable collection with abstraction manuals (clear definitions); participating in inter- and intra-abstractor reliability checks; privacy and security training; signing of confidentiality agreements and training on the SSL-VPN transmission modalities or web-based data collection. All mobile devices are encrypted in accordance with ICES policy on *Protecting Personal Health Information on Mobile Devices*³², although the data collected is de-identified at the time of collection. Abstractors are restricted further in the *Access to Health Data Policy*:

“Any ICES Agent who has access to PHI in a capacity external to the ICES domain must not have access to the same health information (identified or not) within the ICES domain unless that person is an ICES data covenantor or that Abstractor who obtained PHI collected in a clinical setting”.

All ICES projects are explicitly directed at a fundamental purposes of section 45 of PHIPA: statistical and evaluative studies related to Ontario’s health care system. All projects conducted by ICES’ Agents must clearly state the purpose of the use of the de-identified data in the documentation required for all projects as part of the approvals process. ICES’ Agents are only allowed to use de-identified information either alone or linked to other information using encrypted health card numbers for these purposes. All ICES’ Agents are prohibited from re-identifying an individual. This prohibition extends to attempting to decrypt encrypted information.

³¹ ICES *Access to Health Data Policy* p4

³² ICES *Protecting Personal Health Information on Mobile Devices*. pp1-2

Part 1 – Privacy Documentation

“ICES’ Agents are prohibited from re-identifying any individual. This prohibition extends to attempting to decrypt encrypted information.”³³

Review and Approval Process

Analysis at ICES is conducted with the use of record-level data, where the health card number has been encrypted and all nominal data stripped. Data covenants require access to unencrypted health card numbers and PHI in order to execute the de-identification and health card number encryption process prior to the use of the data for approved statistical and evaluative projects. Projects must be consistent with ICES’ mandate and core functions, and in compliance with all applicable legislation, including privacy legislation. Principle 1 of ICES’ *Privacy Code*³⁴ and *Access to Health Data* policy³⁵ clearly sets out that access to PHI by ICES’ Agents is limited to a “need to know” basis, related to performance of specific duties and/or services, and only after these Agents have met the mandatory education requirements in the areas of privacy and security and signed specialized confidentiality agreements for data covenants. Additionally, data covenants are named to both the IPC and the MOHLTC.

Mandatory privacy education requirements and signing of confidentiality agreements are required of all ICES’ Agents, as set out in ICES’ *Confidentiality Agreement Policy*.

Consultants and other Third Party Service Providers do not require access to ICES de-identified data or information systems. ICES *Collaborating Scientist Non-disclosure confidentiality agreements* are signed by external scientists who collaborate only on manuscript development and have no access to data or ICES/analytic systems. These agreements require that: collaborators treat the aggregated information contained in tables and the manuscript as confidential; all documents, reports and statistical outputs are to be shredded as per ICES policy, using approved and provided ICES tools and receptacles; no attempt will be made to identify individuals from any aggregate information to which he/she has access; that he/she will follow any collaboration principles or documentation put in place related to the project, including legal contracts and DSAs; and that by signing this, he/she agrees to have read, understood and comply with the agreement.

For all PHIPA section 45 statistical and evaluative projects done at ICES, scientific Agents are required to develop a scientific proposal, complete a project-specific Privacy Impact Assessment Form (PIA) and a Project Activation worksheet (PAW) articulating financial and staffing requirements. Dataset creation plans (DCPs) are constructed to limit databases and variables used to those necessary to answer the scientific question of interest, and document the statistical pathway to obtain results. ICES’ PIA form is built on the requirements of PHIPA and has been previously approved by the IPC in 2005 and 2008.

Once completed, these documents are signed by the Principal Investigator (Scientist), and submitted to the Program Leader, who reviews and approves projects to be done with and within

³³ ICES *Privacy Code. Principle 7.3*

³⁴ ICES *Privacy Code. Principle 1*

³⁵ ICES *Access to Health Data Policy. pp1-2*

Part 1 – Privacy Documentation

the theme group. ICES has five main statistical and evaluative Programs: Cancer; Cardiovascular & Diagnostic Imaging; Chronic Disease & Pharmacotherapy (formerly Drug, Diabetes & Kidney); Health System Planning and Evaluation; and Primary Care & Population Health. Additionally, three new “theme programs” are being developed under the umbrella of the Primary Care program and the Chronic Disease & Pharmacotherapy program – Mental Health and Addictions, Respiratory, and Musculoskeletal. The documents then flow to the Privacy Office for logging, review and approval, and to the CEO for final sign-off.

Once this multi-step approval process is completed and the project is approved, the scientific Agent notified of the approval by email and provided with a copy of the fully-executed approval. The completed document package is sent to the Project Database Coordinator who creates a project file, assigns a working project number for tracking purposes, and archives the original signed hardcopies of all documents for ease of future reference.

Access to the de-identified data is decided on the “need-to-know” principle as well, with defined access to ICES’ UNIX systems laid down in ICES’ *Access to Health Data Policy*.

ICES defines 4 levels of user access to these data on the UNIX system:

“Level 0 –Data Covenantors access to all administrative data and all un-encrypted identifiers.

Level 1 –Analysts/Programmers and Biostatisticians: access to all de-identified administrative data.

Level 2 – Epidemiologists and scientists with statistical expertise: access to all de-identified administrative data excluding postal code and birth date.

*Level 3 – Students access limited to only project-specific, pre-linked sets of administrative data and to “pilot” data”.*³⁶

Conditions or Restrictions on the Approval

Once access to and use of PHI is granted to an individual who is a Data Covenantor, the Covenantor must re-sign annually the ICES *The Covenantor’s Confidentiality Agreement*.³⁷ The agreement identifies conditions and restrictions with which Data Covenantors must comply in accessing and using PHI.

Access to de-identified data for ICES’ other Agents – Scientists, Programmer/Analysts, Biostatisticians and Epidemiologists – are reviewed twice yearly as part of ICES’ internal data access audit by the CPO, CISO, Manager Administration and Manager Information Systems. For students, whose access term has been predefined when commencing studies at ICES, their academic supervisors must clearly demonstrate continued need for access when students have not completed planned analyses within the designated timeframe.

³⁶ ICES *Access to Health Data Policy*. p1

³⁷ ICES *The Covenantor’s Confidentiality Agreement*. pp1-3

Notification and Termination of Access and Use

ICES has implemented an off-boarding process executed by the Manager Administration to ensuring prompt and timely revocation of access privileges to ICES' premises and networks, including de-identified data holdings.

In the event that a data covenantor granted access to and use of PHI resigns, or is no longer employed or retained by ICES, ICES notifies the MOHLTC and the IPC in writing. As per ICES usual exit procedure, all Agents return coded keys and identification badges on their last day. All email and internal accounts, including UNIX accounts, are terminated by the IT Department on the last day of employment. These processes are consistent with ICES' *Termination of Employment/Resignation and Discharge*³⁸ policy instruments.

“The Role Group Director/Manager must send a copy of the letter of resignation to the Senior Director, Corporate Services to initiate processing the final documentation. Immediately thereafter, the Senior Director Corporate Services will complete an Employee Change Form and send it to Human Resources so that compensation and benefit transactions may proceed promptly. It is the responsibility of the Role Group Director/Manager to make arrangements to obtain all ICES property on the last day of work, i.e. identification badges, all keys, cell phones, laptop computers, passwords, etc.”

“The Information Systems Department must be given at least one (1) week's notice so that they may work with the agent to secure computer files, passwords and terminate computer and building access on the last day worked.”

“The determination to discharge an Agent from employment at ICES must be made in consultation with the Senior Director, Corporate Services. ICES must ensure that, all relevant policies and legislative requirements are adhered to and the discharge is completed in a humane and caring manner. The Information Systems Department must be notified in advance to ensure that computer, voice mail and building access is terminated at the time of discharge”.³⁹

These policy instruments also require any agents granted approval to access and use PHI, as well as his or her supervisor, to notify ICES when the agent is no longer employed or retained by ICES or no longer requires access to or use of the PHI. *Termination of Employment/Resignation and Discharge* policies set out the procedure to be followed in providing the notification and identify which ICES agent must be notified, the time frame within which this notification must be provided, the format of the notification, the documentation that must be completed, the agent who must complete it, the agent to whom the documentation must be provided and the required content thereof.

³⁸ ICES *Termination of Employment/Resignation and Discharge*. p2

³⁹ ICES *Termination of Employment/Resignation and Discharge*.p1-2

Secure Retention and Destruction of Accessed/Used Records

ICES' Agents in the Information Management and Privacy/Security team recognize that information is only secure if it is secured throughout its entire lifecycle: creation and collection, access, retention and storage, use, disclosure and disposition. Accordingly, ICES has a comprehensive suite of practices and procedures that specifies the necessary controls for the protection of information in both physical and electronic formats, up to and including robust encryption and secure destruction. This suite of policies and procedures reflect best practices in privacy, information security and records management.

Some of the routine Information Management procedures in place include: daily back-up of analytic work executed on the secure data network in relation to all projects; original media are catalogued stored in a vault behind four layers of secured doors with highly limited access; the date for secure destruction is set at the time a project is submitted to ensure files are managed to the end of their lifecycle in a manner that is consistent with ICES practices; holdings and destruction dates are logged in information management databases to facilitate tracking; and, data destruction policies and destruction certificates are in place.

Tracking Approved Access to and Use of PHI

ICES' Agents, with the exception of data covenantors and Abstractors, do not have access to PHI – only de-identified data. Data covenantors have access to and use of PHI for the previously identified purposes. Approved projects requiring chart access are facilitated through collaboration with the organizations holding the records; Abstractors hired, records used, dates of use, training of Abstractors and their signing of Confidentiality Agreements by these Agents involved in the project for the site are logged by Project Managers routinely. ICES does not have a policy outlining this type of record keeping, which is added to Appendix FOUR: Table of Deficiencies.

Compliance, Audit and Enforcement of the Policies and Procedures for Limiting Agent Access to and Use of PHI

For ICES' Data Covenantors, the *Covenantor Confidentiality Agreement* states:

*“The Data Covenantor shall keep all Confidential Information confidential in accordance with this Agreement and applicable law;
The Data Covenantor will not use any Confidential Information for any purpose other than that for which it was provided to the Agent/Data Covenantor;
The Data Covenantor agrees only to disclose or to provide access to Personal Health Information in a form in which the individual to whom it relates cannot be identified;
The Data Covenantor shall handle all Personal Health Information in a manner consistent with the ICES' Privacy Policy “Confidentiality and Security of Data”;*⁴⁰

⁴⁰ ICES *Covenantor Confidentiality Agreement pp1-3*

For ICES Abstractors: the ICES *Confidentiality Agreement* requires all Agents to comply with all policies and practices. Compliance is enforced by a team approach by Project Managers/Role Group Leaders/CISO and CPO. It specifies that breach of the terms of the agreement may result in discipline, up to and including termination.

*“You have an obligation to familiarize yourself and to comply with all practices and procedures of ICES relating to privacy and security, including any practices and procedures implemented from time to time after the date of this Agreement”.*⁴¹

*“Any breach of this Agreement may result in disciplinary action being taken by ICES, up to and including a termination of any relationship you have with ICES, including without limitation any employment or other contractual relationship with ICES”.*⁴²

ICES *Confidentiality Agreement* and ICES *Information Breach Policy* also includes instructions on what to do in the event of a breach of the policy:

*“You agree to notify ICES’ CPO... immediately upon becoming aware of any breach or any possible breach of this Agreement”.*⁴³

*“Documentation of an information breach is critically important for both managing information breaches and for preventing similar breaches in future. You are obligated to report all suspected breaches of either PHI, de-identified health information (HI) or ICES’ policies, procedures, practices, SOPs and guidelines. Documentation is to be initiated as soon as discovered. Containment and notification should occur simultaneously, where possible. The CEO/Deputy CEO, CPO, CISO— will make decisions on the notification cascade”.*⁴⁴

Logs of users of de-identified information (individual user accounts) are audited twice per year.

9. Log of Agents Granted Approval to Access and Use PHI

ICES’ CPO and CISO maintain a log of all Administrative data covenantors and Primary data covenantors. The logs are reviewed twice annually as previously described.

ICES’ Project Managers maintain a log of all Agents who act as Abstractors – individuals who have been granted approval to access and collect PHI for approved purposes – and provide these to the Privacy Office for inclusion in the logs. The log includes the following fields of information:

⁴¹ ICES *Confidentiality Agreement*. Clause 6

⁴² ICES *Confidentiality Agreement*. Clause 9

⁴³ ICES *Confidentiality Agreement*. Clause 8 and *Covenantor Confidentiality Agreement*, Clause 11

⁴⁴ ICES *Breach Policy*. pp1-2

Part 1 – Privacy Documentation

- Name of Agents;
- Data holdings (databases or charts) to which access and use was granted;
- Level or type of access and use (Abstractor);
- Date permission to access and use PHI was granted (signature of Confidentiality Agreement date);
- Date of expiry of Abstractor’s permission to access and use the PHI.

10. Policy and Procedures for the Use of PHI for Research

This section is not applicable.

ICES does **not** permit the use of PHI (previously reported to the IPC in both 2005 and 2008) and expressly prohibits the use of PHI by its Agents. Please see ICES’ *Privacy Code*.

*“As a first use, all personal health information will be de-identified and health card numbers will be encrypted prior to use for all statistical and evaluative purposes”.*⁴⁵

11. Log of Approved Uses of PHI for Research

This section is not applicable as ICES does not use PHI for PHIPA section 44 research purposes.

Disclosure of Personal Health Information

12. Policy and Procedures for Disclosure of PHI for Purposes other than Research

This section is not applicable. Please see ICES’ *Privacy Code, section 1.1*.

Where the Disclosure of PHI is Permitted for Purposes other than Research

This section is not applicable. ICES does not disclose PHI. Please see ICES’ *Privacy Code, section 1.1*.

Where the Disclosure of PHI for Purposes other than Research is not Permitted

This section is not applicable. ICES does not disclose PHI. Please see ICES’ *Privacy Code, section 1.1*.

⁴⁵ ICES *Privacy Code*. Principle 1.1

Review and Approval Process for the use of De-identified or Aggregate Information for Purposes other than Research

For PHIPA section 45 statistical and evaluative projects done at ICES, Agents are required to develop a scientific proposal, complete a project-specific Privacy Impact Assessment Form (PIA) and a Project Activation worksheet (PAW) articulating financial and staffing requirements. Dataset creation plans (DCPs) are constructed to limit variables and databases to be used to those necessary to specifically answer the scientific question of interest, and document the statistical pathway to obtain results. ICES' PIA form is built on the requirements of PHIPA and has been previously approved by the IPC in 2005 and 2008. ICES *Policy for the Review and Approval of Project Submissions: PIA, PAW, Proposal Process* clearly lays out the requirements:

“All Agents (scientists and staff) requesting access to the de-identified datasets for purposes of statistical and evaluative studies under section 45 of PHIPA at ICES must be clearly described using three documents:

1. a scientific proposal identifies the study objectives with the background and rationale for undertaking the project. The study design and project participants are identified and the outcome measures noted. The proposal also includes the methods of measurement, potential limitations and a brief statistical data analysis plan for the study, the use of databases planned to answer the study question(s), and the anticipated results and public benefit of the study. In some circumstances, a carefully-constructed dataset creation plan which includes these elements may also be acceptable.

2. a completed project-specific Privacy Impact Assessment (PIA) form. The PIA form is a baseline “living” document that characterizes the project that will be undertaken and which can be updated as needed. The PIA form also provides a way to “do the diligence” by recording the privacy and security issues related to the project.

The PIA provides a comprehensive way to:

- a. document the purpose and uses planned for the data;*
- b. demonstrate compliance with requirements of PHIPA and ICES policies, practices and procedures;*
- c. identify areas of the project which may need special attention (ie, security consultation);*
- d. evaluate the privacy, confidentiality and security risks associated with the use of de-identified information found in ICES' databases as well as for primary data collection projects; and,*
- e. articulate some of the measures used to mitigate and, wherever possible, eliminate the identified risks.*

3. a Project Activation Worksheet (PAW) which identifies the funding for the project.

4. a dataset creation plan (DCP) is occasionally provided by some research teams concomitantly, but may still need to be further developed after the project has been approved. Some scientists prefer to consolidate their thinking on how to execute the project by creating a DCP rather than writing a prose proposal, which can be acceptable in some cases. All projects ultimately need DCPs

created, as they are integral to the process of defining the cohort and collecting the variables of interest that will help answer the study question.”⁴⁶

Once completed, these documents are signed by the Principal Investigator (Scientist), and submitted to the Program Leader, who reviews with and approves projects to be done within the program group. The program groups are constituted of Scientists who are experts in the various theme areas. [Additionally, projects often undergo intensive scrutiny by independent scientists reviewing projects on behalf of granting agencies, such as the Canadian Institutes for Health Research (CIHR), among many others].

ICES has five main statistical and evaluative Programs: Cancer; Cardiovascular & Diagnostic Imaging; Chronic Disease & Pharmacotherapy (formerly Drug, Diabetes & Kidney); Health System Planning and Evaluation; and Primary Care & Population Health. Additionally, three new “theme programs” are being developed under the umbrella of the Primary Care program and the Chronic Disease & Pharmacotherapy program – Mental Health and Addictions, Respiratory, and Musculoskeletal.

The documents then flow to the Privacy Office for signature and logging, review and inclusion in Research Ethics Board (REB) logs, and then to the CEO for final approval and sign-off. At each point along this pathway, sign-off must be obtained.

Once this multi-step approval process is completed and the project is approved, the Principal Investigator (Scientist) is notified of the approval by email and provided with a copy of the fully-executed approval. The completed document package is sent to the Project Database Coordinator who creates a project file, assigns a working project number for tracking purposes, and archives the original signed hardcopies of all documents for ease of future reference.

Results of all statistical and evaluative studies are assembled in tables for presentation and interpretation in reports and scientific manuscripts. As per privacy best practices and its agreement with the MOHLTC, ICES suppresses cells of 5 or less (≤ 5) to protect the privacy interests of individuals and reduce the chance of re-identification.⁴⁷ ICES’ *Confidentiality Agreement* and ICES’ *Privacy Code* prohibits Agents who are permitted to use de-identified or aggregate information from using the information alone or with other information to identify an individual.

13. Policy and Procedures for Disclosure of PHI for Research Purposes and the Execution of Research Agreements

Where Disclosure of PHI is Permitted for Research

This section is not applicable. ICES does not permit PHI to be disclosed. Please see ICES’ *Privacy Code, section 1.1.*

⁴⁶ ICES *Policy for the Review and Approval of Project Submissions: PIA, PAW, Proposal Process.pl*

⁴⁷ Standard. *Privacy Considerations at ICES: Working with Small Cells.* p1

Part 1 – Privacy Documentation

Review and Approval Process for Disclosures of PHI for Research Purposes

This section is not applicable. ICES does not permit PHI to be disclosed. Please see ICES' *Privacy Code, section 1.1.*

Conditions or Restrictions on the Approval of Access or Use for Research Purposes

This section is not applicable.

Secure Transfer

This section is not applicable.

Secure Return or Disposal

This section is not applicable.

Documentation Related to Approved Disclosures of PHI for Research

This section is not applicable. ICES does not permit PHI to be disclosed. Please see ICES' *Privacy Code, section 1.1.*

Where the Disclosure of PHI is Permitted for Research

ICES policies do not permit the disclosure of PHI.

Where the Disclosure of PHI is Not Permitted for Research

ICES' MOHLTC Agreements clearly articulate that ICES has no property right or title to the PHI disclosed to the Institute; it remains the property of Ontario. Additionally, the agreement stipulates that PHI may only be provided to ICES' Agents/analysts and data covenantors to carry out permitted purposes. ICES' focus is PHIPA section 45 statistical and evaluative studies.

Because ICES has adopted a uniform approach to the protection of PHI by de-identifying it as a first use, PHI is not disclosed for research.

Any request for access to de-identified information at ICES for a research purpose is also required to follow ICES standard submission, review and approval processes (described previously under Review and Approval Process for the use of De-identified or Aggregate Information for Purposes other than Research.) Use of de-identified information for this purpose must similarly follow the requirements of ICES' *Policy for the Review and Approval of Project Submissions: PIA, PAW, Proposal Process*. Agents are required when completing ICES' *Project-specific Privacy Impact Assessment* form to indicate in section B1 whether the planned

Part 1 – Privacy Documentation

purpose is for section 45 or section 44 work. A *Briefing Note* and *Schematic* are provided to Agents to facilitate that decision.^{48 49}

The single initiative currently for this type of disclosure is for the *cd-link project*, described below.

A heightened standard of de-identification has been developed by ICES' Agents/analysts and scientists Dr. Craig Earle and Dr. Khaled El-Emam for the new collaborative project ***cd-link*** described below. This project was built on ICES' and Cancer Care Ontario's (CCO) usual frameworks and suites of policies, practices, procedures, standards, tools, practices and guidelines. Collectively, we accelerated a common good by increasing capacity for cancer research by modelling analytic approaches found in the SEER-Medicare data in the United States, and by finding a new method to provide data, not PHI, to scientists in a format that is essentially impossible to re-identify. In the future, this might provide a method for providing data for other research purposes in other medical disciplines with which ICES is comfortable.

As per ICES' long-standing policies, the documentation related to such a request must include a fully-developed proposal, project-specific Privacy Impact Assessment (PIA) form, dataset creation plan, Project Activation Worksheet (PAW) (financial/funding information) and a copy of REB approval for the project. Additionally, support for the project must be provided by various ICES' Agents, including the CEO, Scientific Program Leader, CPO and any other stakeholder approvals required contractually. [Additionally, projects often undergo intensive scrutiny by independent scientists reviewing projects on behalf of granting agencies, such as the Canadian Institutes for Health Research (CIHR), among many others. A letter of support from ICES accompanies this type of grant application]. The scientist of record is responsible for application for REB approval and must provide a copy of the approval document.

The decision to permit the disclosure is ultimately that of the CEO of ICES, based on input from the persons described previously. Approved project documents are returned to the Privacy Office, where they are scanned, original documents archived, and email notification sent to the scientist of record by the Privacy Office.

EXAMPLE: The cd-link Project. ICES, OICR and CCO Collaboration

As presented to both the IPC and the Ministry of Health in 2009, the purpose of the ***cd-link project*** is to enhance Ontario's capacity to study how the organization and delivery of its cancer services affects the quality and outcomes of care by making existing data about the workings of our health system more directly available to scientists. The vision is to use such studies to drive improvements in the cancer system and reduce the burden of cancer in Ontario. Large, truly population-based cohorts can be constructed including patients of all ages, and including rich data on treatments such as radiation therapy or outpatient medications, not usually available from other sources. Furthermore, studies of dissemination, quality of care, and disparities from other jurisdictions are often confounded by issues of access and insurance, which are largely mitigated

⁴⁸ A Privacy Briefing Note: Section 44 and 45 of the Personal Health Information Protection Act, 2004 (PHIPA). pp1-2

⁴⁹ Schematic. Section 45 or Section 44? Which Section of PHIPA Applies to Your Project? p1

Part 1 – Privacy Documentation

in Ontario. Moreover, when considering economic evaluation and policy questions such as regionalization of services, the perspective of a decision-maker concerned with optimizing not only all health care resource utilization, but also the use of all societal resources, is more real than in almost any other setting. Capitalizing on these features can allow scientists to be uniquely situated to answer important questions related to cancer service delivery.

To this end, the Ontario Institute for Cancer Research (OICR), ICES and Cancer Care Ontario (CCO) collaboratively proposed creating a complementary data usage model in which ICES would centrally create standing linkages of relevant data sets, such as the Ontario Cancer Registry and OHIP claims, de-identify them by removing all personal identifiers, and then through policies and procedures that ensure appropriate use of the data (data use agreements (DUA) with non-disclosure pledges, pre-publication review of manuscripts, data destruction requirements and certification) provide the resultant comprehensively anonymized datasets directly to non-ICES investigators, creating a new infrastructure resource for health services research in the province. Analytic support is being provided in the form of data users workshops, a website providing common programming procedures and FAQs, and limited interactive technical assistance (see www.ices.on.ca/about-us/cd-link for more information). De-identified data that has also been subject to generally accepted statistical and scientific principles and methods for ensuring that the risk of re-identification is below a pre-determined threshold, is then manipulated further using software that assesses the re-identification risk of a particular data set. Through semi-automated procedures, the program manipulates variables to reduce the risk of re-identification (Privacy Analytics Risk Assessment Tool: ‘PARAT’). If risk is perceived as too high, the data can be further manipulated to further reduce risk to acceptable levels, resulting in Risk-Reduced De-identified Data (‘R2D2’).

The *cd-link project* and its Data Use Agreement (DUA), project-specific PIA, required a dataset creation plan (DCP), Confidentiality Agreement and SOPS specifically mandating that the person or organization to which the de-identified and/or aggregate encrypted information will be disclosed is required, to agree in writing that they will not use de-identified or aggregated information either alone or with other information, including prior knowledge, to identify an individual prior to receipt of the information. This prohibition includes attempting to decrypt encrypted information. Scientists are required to seek REB approval for the use of data for specified purposes. Additionally, the *Data-Use Agreement* (DUA) also identifies the scientist(s) responsible for ensuring that any conditions or restrictions that must be satisfied prior to the disclosure of the de-identified or aggregated information have, in fact, been satisfied, including the execution of the written acknowledgment.

“The Principal Investigator agrees that the data will be used only for the research purposes as outlined in, and in accordance with, the Proposal. The Principal Investigator represents and warrants that the statements and methods indicated in the Proposal are complete and accurate”.

“The Principal Investigator agrees that he/she shall be fully responsible for his/her breach of this DUA or by any Researcher, and that each Researcher shall be bound by a written agreement to protect the

Part 1 – Privacy Documentation

confidentiality and regarding the ownership of the data as provided for in this DUA”.

“The Principal Investigator agrees that he/she will not permit any other person to use the Data except for Researchers. Within the Principal Investigator’s institution, access to the Data shall be limited to the minimum number of Researchers necessary to achieve the purposes stated in the Proposal”.

“The Principal Investigator will ensure that no attempt is made to learn the identity of any individual to whom the data relates.”

“The Principal Investigator will ensure that no attempts are made to link data to any other data files other than in accordance with this DUA and the Proposal”.

“The Principal Investigator will ensure that no findings or information derived from the Data will be released if such findings or information contain any combination of data elements that might reasonably be foreseen to allow the deduction of the identify of an individual to whom data relates, a patient, a health care provider, a family or a household. The Principal Investigator agrees that ICES shall (in the sole discretion of ICES) be entitled to determine whether any findings or information derived from the data might reasonably be foreseen to allow the deduction of the identify of any such individual to whom data relates, a patient, a health care provider, a family or a household.”

“The Principal Investigator will ensure that, in tables, cell sizes equal to or less than five (≤ 5) are suppressed.”

“The Principal Investigator agrees to provide ICES with a copy of all documents (manuscripts, reports and other written material in any way based on any material produced under or in relation to the data or this agreement) which it is anticipated may be published ("Material") at least 45 days in advance of potential publication.”⁵⁰

The Confidentiality Agreement which must be signed by investigators seeking data using this method requires compliance through the following clauses⁵¹:

“You agree not to use Confidential Information for any purpose other than that for which it was provided to you unless you obtain ICES’ written pre-authorization to do so.”

⁵⁰ cd-link Data Use Agreement. pp1-2

⁵¹ cd-link Confidentiality Agreement p1

Part 1 – Privacy Documentation

“You agree not to disclose any Confidential Information to any person who has not entered into a confidentiality agreement with ICES and who requires access to the Confidential Information for purposes of carrying out such person's function.”

“You agree to keep any Confidential Information in your control or possession in a physically secure location, and you agree that access to all or a relevant portion of such Confidential Information shall be limited only to you and any other person who has signed a confidentiality agreement with ICES and who requires access to a relevant portion of such Confidential Information for purposes of carrying out such person's function.”

“You agree to take all necessary steps to keep such Confidential Information secure and to protect such Confidential Information from unauthorized use, reproduction or disclosure.”

“You agree to notify ICES’ CPO in writing immediately upon becoming aware of any breach or any possible breach of this Agreement.”

“Any breach of this Agreement may result in disciplinary action being taken by ICES, up to and including a termination of any relationship you have with ICES, including without limitation any other contractual relationship with ICES.”

“The provisions of this Agreement shall be governed by and construed in accordance with the laws of Ontario and the laws of Canada applicable therein and the parties hereby agree that the courts of Ontario will have non-exclusive jurisdiction with respect to this Agreement.”

“This Agreement is in addition to, and not in substitution for, all other obligations owed by you to ICES.”

“Upon and in accordance with ICES’ written request, you agree to securely return to ICES or to securely destroy any Confidential Information”.

“Upon and in accordance with ICES’ written request, you agree to cooperate in all respects with ICES regarding any request of the Ontario Ministry of Health and Long-Term Care regarding any Confidential Information; any investigation or review by the Information and Privacy Commissioner/Ontario regarding any Confidential Information. You also agree to permit ICES and its authorized representatives with access to all Confidential Information forthwith following request by ICES.”

Document tracking and document management is provided by ICES’ cd-link Project Manager, in collaboration with the Privacy Office.

14. Template Research Agreement

ICES does not collect or disclose PHI for research purposes.

A description of the contents of the *Data Use Agreement*⁵² and *Confidentiality Agreement*⁵³ that must be executed by researchers using comprehensively de-identified data in the context of the *cd-link project* has been provided in section 13 above.

However, ICES is initiating a new corporate process which tracks, among others, formal requests for ICES to provide **analytic functions** related to ICES' de-identified, linkable data holdings. These agreements are often called "Research Agreements" by stakeholders requesting assistance – such as the Ontario Agency for Health Protection and Promotion (OAHPP), Ontario's Health Quality Council (HQC, now part of Health Quality Ontario [HQO] under the *Excellent Health Care For All Act* [Bill 46, 2010]) but they **do not use the word "research"** in accordance with the PHIPA section 3 definition of "research" (PHIPA section 44) as required by the IPC. In these agreements, the statistical results are aggregated and included in reports for the stakeholder.

ICES finds that the 'new' rules of accountability are changing the landscape of documentation required for the types of work and partnership relations in which its' Scientists and staff engage. We feel that this distinction between sections 15 and 16 of this document is important to make as this is where the most significant changes seem to be manifesting themselves.

1. Previously, and currently, the secure movement of PHI from HICs to ICES for declared purposes approved in proposals and project-specific PIAs was documented in mutually-negotiated and executed data-sharing agreements.

2. Increasingly,

- (a) ICES is being asked to enter into "research agreements" with partners and stakeholders that, in reality, categorize or list specific linkages and analyses that will be undertaken on the partners'/stakeholders' behalf – they are essentially a type of 'statement of work' or work 'contract'. The evaluation project or analyses is undertaken entirely by ICES' Analysts under the supervision of the ICES' Scientist of record and the final output of aggregated data is incorporated into a report (if that is part of the requirements) OR is provided to the partner to create their own product of interest;
- (b) as ICES is not permitted to hold large grants itself, another variation of this type relates to grant funds, successfully procured by ICES-appointed scientists and adjuncts for projects using ICES administrative datasets, held at another organization (usually the primary appointment organization of the scientist). The organization holding the grant requires a research agreement which is a 'statement of work' for the analyses that are conducted by ICES Analytic staff to document and facilitate cost recovery for analytic time from the grant.

⁵² *cd-link Data Use Agreement. pp1-2*

⁵³ *cd-link Confidentiality Agreement p1*

3. At the intersection of these two types of documents is one in which, at the request of the partner or stakeholder, the explicitly requested work is incorporated into the data-sharing agreement as a schedule.

These requested changes have forced ICES to evaluate these evolving requirements and identify gaps, so appropriate policies and practices can be developed and implemented. It is our intention to develop policies and procedures for the disclosure of de-identified information for research purposes because of the increased interest of the scientific community and the restructuring underway internally. Please see Appendix FOUR: Table of Deficiencies for timeline. ICES will likely follow a similar path as taken for the *cd-link project* in relation to policies, procedures, data-use agreements and confidentiality agreements. ICES will keep the IPC updated on progress in this changing area.

15. Log of Research Agreements

ICES does maintain a log of all *Data Use Agreements*, *Confidentiality Agreements* and *written acknowledgements* executed by researchers to whom de-identified information is disclosed for research purposes in the context of the *cd-link project*. We have also started a log for Research Agreements to track the changes we are anticipating (described in section 14 above). We have modelled this log on the requirements found within the Manual.

The log includes:

- The title of the research study;
- The name of the Principal Investigator to whom the information was disclosed and the names of all members of the project team;
- Tracking by document of all required documents: PIA, proposal, DCP, PAW;
- Number and date of DUA;
- Approval date by CCO and ICES;
- ICES' Analyst responsible for execution;
- Anticipated date of commencement and completion;
- The date of disclosure of the information (shipping date);
- Expiry date for DUA;
- Receipt of Documentation of Destruction or return of data.

16. Policy and Procedures for the Execution of DSAs

ICES' *Policy and Procedures for Executing a DSA* states that DSAs must be executed prior to the collection of PHI for "purposes related to s.45".⁵⁴

As described in section 4 of Part I Privacy Documentation, ICES executes a DSA with all stakeholders prior to the collection of PHI for purposes related to PHIPA section 45 activities.

⁵⁴ ICES' *Policy and Procedures for Executing a DSA*. p1

Part 1 – Privacy Documentation

ICES' *Policy and Procedures for Executing a DSA* document identifies the circumstances requiring the execution of a DSA and the requirements that must be satisfied prior to its execution. It includes the process that must be followed including the documentation which must be completed, provided or executed, who is responsible for same, the content of the documentation and to whom it must be provided.

The Health Information Officer, Director Information Management and CPO share the responsibility for ensuring that the process articulated in the *Policy and Procedures for Executing a DSA* is followed and that a DSA is executed prior to the collection of any PHI. The CPO must be satisfied that the collection was approved in accordance with fundamental principles of ICES' *Privacy Code* and the internal document *Orientation Module 5: DSA Guidelines*.

The *Policy and Procedures for Executing a DSA* requires the Corporate and Privacy Offices staff to mutually maintain a log of DSAs and to retain all documentation relating to the execution of the DSAs in ICES' electronic library of DSAs. This log is a working file employed jointly by the Health Information Officer, Director Information Management, Manager Administration and CPO to track and manage DSAs against the background of approved section 45 studies.

The ICES policy for considering the development and execution of a DSA includes:

“Considerations: The information in consideration is not available at ICES, and is under the stewardship of another entity or health information custodian; the information is necessary for the statistical and evaluative purpose contemplated by scientists; identification of the intention to link information to ICES administrative and other datasets, and the need for PHI or de-identified health data (including MRN or health card number only) for the purposes of the study; and, willingness of the HIC... to share information for this purpose.”⁵⁵

“Once the requirement of a Data-sharing Agreement is noted in the intake procedure described above, the Health Information Officer, Director Information Management and CPO will liaise regularly in both formal meetings (HIPS – Health Information, Privacy and Security Committee) and informally by phone and email about the drafting and/or ultimate execution of the agreement to ensure compliance with the requirement for an agreements. The Privacy Office will...archive agreements as described and with the Director Information Management to log all agreements and their data destruction dates for future use.”

17. Template Data Sharing Agreement

ICES requires that, prior to collection of PHI, a DSA or other legally binding instrument that satisfies the requirements of the Manual be executed with the person or organization or HIC from whom the information will be collected for statistical and evaluative purposes.

⁵⁵ ICES *Policy and Procedures for Executing Data-Sharing Agreements* p1

The combination of ICES' *Policy and Procedures for Executing a Data Sharing Agreement*, ICES *Project-specific PIA* form, and ICES-MOHLTC *Data Privacy Agreement with a Prescribed Entity 2006* require that, prior to collection of PHI for health services, evaluative and statistical studies, a DSA be executed with the data-supplying organization from whom the information will be collected.

All elements listed in the IPC Manual, namely, all items in the General Provisions, Purposes of Collection, Use and Disclosure, Secure Transfer, Secure Retention, Secure Return or Disposal, Notification, and Consequences of a Breach and Monitoring Compliance are contained in ICES' *Template Data-sharing Agreement*, previously reviewed in 2005 and 2008, and amended as requested by the IPC in 2008.⁵⁶

18. Log of Data Sharing Agreements

ICES' CPO, Privacy Office Administrator and Manager Administration, mutually maintain an electronic library of all executed DSAs, as well as a spreadsheet logging ICES' Active DSAs.

The logs include:

- The name of the signatory and organization from whom the PHI was collected;
- The name of the ICES' Principal Investigator/Scientist or Adjunct Scientist for whom the PHI was requested/collected for purposes described in the agreement;
- The name of the ICES' Data Covenantor to whom the PHI was disclosed;
- The date the PHI was collected at ICES;
- The purpose of the collection and any amended purpose;
- The dates that the collection of PHI was approved and executed, and by whom;
- The nature of the PHI subject to the DSA (description of the data and years of data collected);
- The retention period for the records of PHI set out in the DSA and the date of Data Destruction;
- The presence of health card number and linkage method planned (deterministic/probabilistic);
- Location of information (server location);
- Names of ICES Agents with access;
- The date a certificate of destruction was provided.

19. Policy and Procedures for Executing Agreements with Third Party Service Providers in Respect of PHI

ICES does not permit third party service providers access to or use of the PHI held by ICES.

⁵⁶ ICES *Data Sharing Agreement Template*. April 2010

Part 1 – Privacy Documentation

ICES' *Sourcing and Procurement Policy* sets the guidelines that govern the acquisition of all goods and services by ICES and requires that all purchase orders or Third Party Supplier agreements/contracts must be drafted, reviewed, approved and duly signed prior to the official performance start date of work and be in place for the entire period of work. ICES may allow, in some circumstances, third party service providers to access specific data on a need-to know basis, that is, when required to perform their services. However, ICES requires that prior to permitting third party service providers to access any de-identified information or aggregate information held by ICES, they also must undergo Privacy and Security Orientation appropriate to the work contracted and sign *Confidentiality Agreements*. The signature of Confidentiality Agreements anticipates those individuals who are contracted to work with ICES' Security and IT staff on testing/reviewing and have, as a consequence, greater understanding of ICES' Security posture, which must be kept confidential.

All Third Party Supplier contracts reference a Non-Disclosure Agreement (NDA) that is required in advance of any work or communication with ICES. The NDA not only reflects confidentiality requirements but also commits the Supplier organization to Information Security requirements within their own organization and any of their subcontracted organizations. ICES requires the signature of an NDA from a 3rd party service provider in advance of any disclosure or discussion regarding ICES strategies or operations. In addition, any third party service provider is required to sign an NDA in advance of their interest/willingness to participate in Request for Proposal (RFPs) and Request for Quote (RPQs) calls.

The Sourcing and Procurement Officer is responsible for insuring agreements are executed; the Sourcing and Procurement Analyst in ICES' Procurement Office maintains a database of all fully executed Supplier Agreements for the purposes of managing the contract, for historical reference, and audit. Additionally, the Procurement Analyst also maintains a log of these project-specific NDAs, Confidentiality Agreements and service provider contracts.

20. Template Agreement for All Third Party Service Providers

ICES' Sourcing and Procurement Office has developed a suite of template agreements, collectively referred to as *Third Party Supplier Contracts*. These include: Consulting Agreements; Contracting Agreements; Chart Abstractors Agreements; Analytic [Research] Service Agreements; and, Corporate Goods and Services Agreements. The agreement which is appropriate to the type of third party service being sought/provided is used by the Sourcing and Procurement Office in each individual circumstance.

All elements listed in the IPC Manual, namely, all items in the General Provisions, Obligations with Respect to Access and Use, Obligations with Respect to Disclosure, Secure Transfer, Secure Retention, Secure Return or Disposal following Termination of the Agreement, Secure Disposal as a Contracted Service, Implementation Safeguards, Training of Employees of the Third Party Service Provider, Subcontracting of Services, Notification, Consequences of Breach and Monitoring Compliance are contained in ICES' Third Party Supplier Contracts. This has been confirmed by ICES' CISO and by the Sourcing and Procurement Office.

ICES' Confidentiality Agreement has been described elsewhere in this document (see Part 3, section 5 and 6); the NDA is described in the same section.

21. Log of Agreements with Third Party Service Providers

ICES' Sourcing & Procurement Officer maintains a functional, living log of all Third Party Supplier Agreements. The following data elements are contained in the log:

- The name of the third party service provider;
- The nature of the services provided by the third party service provider that require access to de-identified information or aggregate information;
- The date that the agreement with the third party service provider was executed;
- The date of termination of the agreement with the third party service provider;
- The date that the agreement was terminated.
- The contract type
- The contract category
- The contract owner
- The contract day-to-day manager
- The currency (eg, CAD, US)
- The funder
- The ICES organization/project being charged
- The pricing information
- How pricing is broken out (single, monthly etc)
- The annual amount
- The contract amount
- The risk level (low, medium, high)
- The number of renewals
- The length of the renewal
- The price/information change and date of that
- The possession of a signed copy

A separate page in the spreadsheet includes a record of all project-specific NDAs and Confidentiality Agreements executed by providers, as discussed in Part 1, section 19.

22. Policy and Procedures for the Linkage of Records of PHI

ICES requires the capability to link individual level information across Ontario's administrative databases, among others, in order to achieve its Mission.⁵⁷

It is most important to note that ICES does not link PHI (further explanation of "first use", de-identification and health card encryption below).

⁵⁷ ICES Website: *Who We Are, Our Mission & Goals*. URL www.ices.on.ca

Part 1 – Privacy Documentation

ICES has developed a number of policy instruments which govern linkage of records. Employing these instruments, ICES permits the linkage of de-identified health records under certain circumstances and for the limited purposes articulated in the proposal/project-specific Privacy Impact Assessment (PIA) required for all projects done at ICES and its expansion sites.

“As a Prescribed Entity in the Personal Health Information Protection Act (PHIPA). ICES is authorized to collect and use PHI for the purposes of section 45 of PHIPA.”⁵⁸

All PHI received/collected by ICES is only handled by three *authorized and named Data Covenantors* who sign special confidentiality agreements related to the processes of de-identification. As a first principle, the process related to linkage at ICES attempts to significantly reduce re-identification risk, as so much linkage work is conducted at ICES. Additional principles are in place to reduce risk: all de-identification activities are carried out in isolated secured work environments on stand-alone machines by Data Covenantors with clearly defined roles and responsibilities.

“WHEREAS the Data Covenantor agreed at the time he or she entered into employment with ICES, to enter into an agreement with respect to confidential information and that he or she has received good and valuable consideration for entering into such agreement;”

“The Data Covenantor shall keep all Confidential Information confidential in accordance with this Agreement and applicable law”

“The Data Covenantor will not use any Confidential Information for any purpose other than that for which it was provided to the Data Covenantor... the Data Covenantor agrees only to disclose or to provide access to PHI in a form in which the individual to whom it relates cannot be identified”

“The Data Covenantor shall handle all PHI in a manner consistent with the ICES’ policy “Confidentiality and Security of Data” unless and to the extent that the Policy is inconsistent with the provisions of this Agreement, in which case the provisions of this Agreement shall govern”.⁵⁹

All records are de-identified and assigned a unique anonymous identifier called the ICES Key Number (IKN), which has a one-to-one (un-disclosed) correspondence to the Ontario health card number. As the second step, any record linkage is then carried out deterministically by matching on the IKN. The method of **deterministic linkage** is the most commonly used in statistical and evaluative projects and studies conducted at ICES.

The only exception to this occurs when ICES has collected records with PHI for purposes of linkage (to other records) *where the Ontario health card number is not present or of poor*

⁵⁸ ICES Access to Health Data at ICES Policy. p1

⁵⁹ ICES Confidentiality Agreement for Data Covenantors.p1-2

quality. In these instances, **probabilistic matching** is carried out on records with PHI to determine the IKN by matching personal identifiers from the records, to personal identifiers in the Ontario Registered Persons Database (RPDB). This activity is only executed by Data Covenantors in isolated secured work environments on stand-alone machines.

“Probabilistic matching involves the formalization of intuitive concepts regarding outcomes of comparison of personal identifiers. “Agreement” between identifiers argues for linkage and “disagreement” between identifiers argues against linkage. Partial agreement is less strong than full agreement in supporting linkage. Agreement on more attributes and disagreement on few attributes would support linkage. These types of agreement can be examined and formalized through examination of a file of true links and a file of true non-links. Probabilistic linkage may also involve calculating the likelihood that two given records belong to the same individual, based on the characteristics of the linkage files and probability theory.”⁶⁰

The following practices are adhered to when probabilistic matching is planned:

- Only three designated Data Covenantors are granted access to PHI for this activity. The activity is carried out in isolated work environments on stand-alone machines.
- The working files for purposes of probabilistic matches contain personal identifiers **but are stripped of any health information**.
- The final product of the process is a file with the **health information restored but all identifiers removed and replaced with the IKN** to allow linkage to other ICES de-identified records.

Review and Approval Process for Data Linkage

The ICES standard *Linkage of Records of Personal Health Information* sets out the process, including what documentation must be completed, provided or executed, who is responsible for this, the content of the documentation and to whom it must be provided. ICES’ Scientists in consultation with the Director, Information Management and members of ICES’ Analytic Teams determine linkage requirements.

Although as the first use of PHI collected from all sources is its de-identification, ICES rigorously tracks all uses of its de-identified data through its’ approval process (see Part 1, sections 8 and 12). This includes comprehensive documentation of the planned project, including development of a written proposal, project-specific Privacy Impact Assessment (PIA) form, dataset creation plan (DCP) and Project Activation Worksheet (PAW). All these components of each project must be approved by the Program Group leader, CPO (or designate) and the CEO, as described earlier (Section 8, Review and Approval Process).

Process for the Linkage of Records of de-identified PHI

The Director, Information Management is responsible for ensuring that the linking of de-identified records is conducted in accordance with the processes described above, as outlined in

⁶⁰ *Linkage of Records of Personal Health Information standard. pp1-2*

Part 1 – Privacy Documentation

the *Linkage of Records of Personal Health Information* standard. Once the records are posted on the UNIX, authorized users can access the UNIX system to create cohorts for the approved purposes using the IKN. The uniqueness of the IKN allows linkage across multiple administrative databases within the UNIX environment, allowing the assembly of multiple variables to answer the questions posed in the approved project. Analysis plans are developed prior to linkage for efficiency purposes but also to minimize the number of variables used.

Retention of Unlinked Records

For purposes of information management and disaster recovery, original collection media containing unlinked PHI are backed up and stored in a vault in ICES' high security area with highly restricted access (Data Covenantors).

Linked, project-specific datasets of de-identified and/or aggregated data on ICES' servers are backed up daily as per ICES' information management and disaster recovery standards (see Part 2, section 13).

Compliance, Audit and Enforcement

Although ICES has a wider range of policies for dealing with different types of actions and activities, the ICES *Confidentiality Agreement* is the core document which, regardless of situation, requires all Agents to comply with its terms. Compliance is enforced by the CEO and the Deputy CEO. It clarifies that breach of the policy may result in discipline, up to and including termination, as previously described. Audit and Enforcement is a cross-discipline and across Role Group effort, lead by the CISO, CPO, and the Deputy CEO.

Tracking Approved Linkages of Records of Health Information

As explained above, ICES does not truly link records of PHI in either its deterministic or probabilistic processes. Linkage does not occur until after the first phase – de-identification – and the second phase – encryption of health cards numbers into IKNs – has been executed by the Data Covenantors. The processes are separate and reasonably ensure that “seeing” fully-identified PHI does not occur.

Regardless, ICES rigorously tracks all uses of its de-identified data through its approval process related to use of a project-specific Privacy Impact Assessment (PIA) form, proposal, dataset creation plan (DCP) and Project Activation Worksheet (PAW). All these components of each project must be approved by the Program Group leader, CPO (or designate) and the CEO, as described earlier (Section 8, Review and Approval Process).

23. Log of Approved Linkages of Records of PHI

This section is not applicable. ICES does not link PHI.⁶¹

⁶¹ *Note on Linkage of Records of PHI at ICES.* Statement from the Director, Information Management.

24. Policy and Procedures with Respect to De-identification and Aggregation

Prescribed entities are required to have a policy and procedures to ensure that PHI will not be used or disclosed if other information, namely de-identified and/or aggregate information, will serve the identified purpose(s). ICES de-identifies PHI using the appropriate methodologies to reduce the risks of re-identification and residual disclosure as part of its commitment to protecting the privacy interest of Ontarians.

ICES has a comprehensive policy instrument that governs de-identification entitled the *Linkage of Records of PHI* standard. ICES also has three core documents which address aggregation requirements: at a public (high) level, the *ICES Privacy Code*; the *ICES-MOHLTC Data Privacy Agreement for a Prescribed Entity*, and *ICES' Working with Small Cells Guideline*. As a starting point, these documents specifically state that PHI will not be used or disclosed if de-identified and/or aggregate information will serve the identified purpose.

The *Linkage of Records of Personal Health Information* standard specifically designates, ICES authorized and designated Data Covenantors as responsible for de-identifying information as previously described in section 22 of this report. De-identified information is reviewed by its Data Covenantors *prior* to its posting on ICES' servers for statistical and evaluative purposes. Preferentially, ICES de-identifies PHI and has done so since inception in 1992.

The *ICES-MOHLTC Data Privacy Agreement for a Prescribed Entity*, the *ICES Project-specific PIA form*, *ICES Template DSA* and the *Working with Small Cells Guideline* articulates ICES' position with respect to cell sizes equal to or less than five. Restrictions are imposed in DSAs and reinforced in the *Project-specific PIA form* and required written research plans to ensure that ICES' Agents perform cell suppression in their publications. These documents take into account the meaning of "identifying information" as laid out in subsection 4(2) of PHIPA.

*"The Prescribed Entity shall aggregate information in its reports in such a manner as to prevent any identification of individuals. When aggregate information is based on a small subset of five or less that could lead to the identification of an individual or individuals, that information shall be excluded from the report or aggregated at a higher level."*⁶²

All ICES' Agents are directed on aggregation requirements through the *Working with Small Cells Guideline*:

"The purpose of methodologies for dealing with small cells is to minimize the risk of re-identification of individuals (identity disclosure), as well as the risk of disclosing information about a potentially known person (attribute disclosure). We focus on small cells because small cells highly increase the risk of disclosure".⁶³

⁶² MOHLTC –ICES Data Privacy Agreement for a Prescribed Entity (2006). Section 4.7

⁶³ ICES Working with Small Cells Guideline. P1

“In selecting a methodology, we must consider whether it is reasonably foreseeable that the information presented could be used with other information to identify individuals. This applies whether the additional information is available within the publication, within other ICES publications, or from any other source.

In principle, we avoid stating the exact cell size of a small cell; replacing the number with some notation such as “<5”, “<6”, or “1-5”. In addition, we make sure that the number cannot be derived by a simple subtraction from the total. This can be done by suppressing the total, or by suppressing another component cell size. Lastly, we make sure that percentage information is coarse enough as to not reveal precise cell sizes. This approach is referred to as ‘small cell suppression’.”

A key control in the *ICES-MOHLTC Data Privacy Agreement for a Prescribed Entity*, and *ICES’ Working with Small Cells Guideline* is the requirement that ICES’ Agents follow an prescribed process to review all statistical results, consisting of aggregate information, including cell-sizes of <5 (five), prior to its disclosure, in order to ascertain that it is not reasonably foreseeable in the circumstances that the information could be utilized, either alone or with other information, to identify any individual. The process and the risk assessment criteria are set out below:

“All ICES publications need to be examined by the research team for presence of small cells prior to releasing results. If any un-suppressed small cells are present, the publication must be submitted to the Privacy Office for approval before it is released. The ultimate responsibility for the handling of small cells according to ICES standards lies with the Primary Investigator.”⁶⁴

The CPO has struck a review committee who can be called upon to consult regarding the appropriate way to deal with small cell issues. The preferred method remains to suppress all small cells. If an scientific Agent finds it clinically compelling to consider publishing a small cell, the process is as follows:

- *An Author of the publication will submit a copy to the CPO, outlining which small cells should remain unsuppressed and the case for doing so. This submission to the PO must occur prior to any submission for publication, unless of course a reviewer’s comments give rise to the potential for small cells.*
- *The CPO will share the publication with one member of the review committee (on a rotating basis) and both will review the document to determine if the situation has an unequivocal response based on ICES “Criteria for Deciding Appropriate Ways to Deal with Small Cells”*

⁶⁴ ICES Working with Small Cells Guideline. p1

- which are outlined in this document. If so, the CPO and the Committee Member will make their decision and notify the Author.*
- *If the CPO and committee member determine that more discussion is needed, or if the Author wishes to appeal the decision of the CPO and Committee Member, then a meeting of the full review committee will be convened. The Principal Investigator or other member of the project team will be invited to attend but attendance is not mandatory. The Author will immediately be notified of the decision either way.*
 - *If the full committee review concludes that the small cells will be permitted, the CPO will consider whether a letter to the IPC is warranted (as has been done historically as a notification).*
 - *The ICES CEO will be copied on all decisions regarding small cells.”*⁶⁵

Decision criteria are clearly articulated in the document as well, which is posted on the ICES intranet.

ICES believes it achieves this objective of protection with various policy instruments and that it is not reasonably foreseeable that the information could be utilized, either alone or with other information, to identify an individual. ICES additionally describes in Part 1, Section 13 the internally –developed processes created for the use of de-identified health information in relation to the *cd-link* project, demonstrating our commitment to preventing re-identification of individuals.

ICES’ health information use/management is entirely predicated on this principle and is comprehensively inculcated into our work culture. ICES has demonstrated leadership in the care taken by its Data Covenantors, and invokes its’ record of the past 19 years in protecting the privacy interests of Ontarians.⁶⁶

In an ongoing fashion, ICES is exploring and testing new tools to assist in assessment of the actual risk of re-identification. One of these tools is actively being used in the *cd-link* project (see part 1, section 13). De-identified data that has already been subject to generally accepted statistical and scientific principles and methods for ensuring that the risk of re-identification is below a pre-determined threshold is then manipulated further, using software that assesses the re-identification risk of a particular data set. Through semi-automated procedures, the program manipulates variables to reduce the risk of re-identification (*Privacy Analytics Risk Assessment Tool: ‘PARAT’*, developed by Dr. Khaled El-Emam, University of Ottawa and ICES Adjunct Scientist)⁶⁷. If risk is perceived as too high, the data can be further manipulated to further reduce risk to acceptable levels, resulting in what is referred to as Risk-Reduced De-identified Data (‘R2D2’).

When there is concern that re-identification risk is unacceptably high, specific techniques can be applied to reduce it. Such techniques include manipulations such as:

⁶⁵ ICES *Working with Small Cells Guideline*. pp2-3

⁶⁶ ICES is pleased to report our participation in the *Data De-Identification Working Group* of the Health System Use Technical Advisory Committee in preparing a report for Canada’s Health Ministries’ Assistant Deputy Ministers (ADMs) in 2010

⁶⁷ <http://www.privacyanalytics.ca>. *Privacy Analytics Risk Assessment Tool*. Currently being used in *cd-link* initiative

Part 1 – Privacy Documentation

- recoding variables into fewer categories to provide less precise detail (including rounding of continuous variables);
- setting top-codes and bottom-codes to limit details for extreme values;
- “disturbing” the data – adding “noise” by swapping certain variables between records, replacing some variables in random records with mathematically imputed values or averages across small random groups of records, or randomly deleting or duplicating a small sample of records;
- replacing, actual records with synthetic records that preserve certain statistical properties of the original data.
- use of quasi-identifiers for variables that can potentially be used for re-identification.⁶⁸

In *ICES Privacy Code and Confidentiality Agreement*, ICES’ Agents are strictly prohibited from using de-identified or aggregated information, including information in cell-sizes equal to or less than five, either alone or with other information, including prior knowledge, to identify an individual. This prohibition includes attempting to decrypt encrypted information.

*“ICES’ Agents are prohibited from re-identifying any individual. This prohibition extends to attempting to decrypt encrypted information”.*⁶⁹

The *ICES Confidentiality Agreement* is renewed/re-signed annually by all Agents at the start of each fiscal year (April) in which they agree to abide by all ICES’ policies, including those policies which explicitly prohibit attempting to decrypt encrypted information, using de-identified or aggregated information, either alone or with other information, to identify an individual.

25. Privacy Impact Assessment Policy and Procedures

ICES’ *Systematic Privacy Impact Assessment Guidelines and Checklist* is its governing document on privacy impact assessments. ICES requires that *systematic* privacy impact assessments (PIAs) be conducted on all proposed data holdings, as well as whenever a new or a change to an existing information system, technology or program involving PHI is contemplated. Additionally, ICES makes every effort to meet with the IPC and to keep the IPC informed about proposed and planned changes.

“A Privacy Impact Assessment (PIA) is a process to determine the impacts of a proposal on an individual's privacy and ways to mitigate or avoid any adverse effects. The PIA process is similar to a continuous risk management approach and includes planning, analysis and education activities. It has four core components: project initiation, data flow analysis, privacy analysis and privacy impact analysis report.”

⁶⁸ *Statistical Policy Working Paper22- Report on Statistical Disclosure Limitation Methodology prepared by the Subcommittee on Disclosure Limitation Methodology, Federal Committee on Statistical Methodology, U.S. Office of Management and Budget*
<http://www.fcsm.gov/working-papers/spwp22.html>

⁶⁹ *ICES Privacy Code Principle 7.6*

Part 1 – Privacy Documentation

“Conducting a PIA is a cooperative process that brings together a variety of skill sets to identify and assess privacy implications. The PIA process is meant to be adapted to fit a particular application, and is most effective when issues are clearly identified and a process of management constructed to enable the project.”

“A PIA is a process that helps determine whether new technologies, information systems and initiatives or proposed programs and policies meet basic privacy requirements. It also assists organizations to anticipate the public's reaction to any privacy implications of a proposal and as a result, could prevent costly program, service, or process redesign. A key goal of the PIA is to effectively communicate the privacy risks not addressed through other mechanisms. The PIA is intended to contribute to senior management's ability to make fully informed policy, system design and procurement decisions.”⁷⁰

As these requirements did not exist at the time, ICES did not conduct PIAs on the PHI received from the MOHLTC through routine feeds as established with ICES' inception in 1992 – and which it receives to this day through more sophisticated transfer mechanisms (SSL-VPN versus tape reels or cartridges). As described elsewhere in the document, the data holdings are de-identified as a first use and the transfer mechanisms (collection) are subject to MOHLTC preferences. Similarly, ICES has been collecting PHI from the Cardiac Care Network (CCN) since 1995, which it also receives through long-standing transfer mechanisms.

However to balance this, ICES does conduct **project-specific** PIAs on all projects utilizing these historically-obtained data as part of requirements for executing *any* project. These requirements that have been in place since 2001 and have been updated with the promulgation of *PHIPA*. In relation to PHI from other prescribed entities, prescribed persons (registries) and HICs, ICES conducts Systematic PIAs. For example, ICES and CCO did conduct a PIA, when routine feeds of Ontario Cancer Registry (OCR) and other datasets were planned in 2001.

ICES physically “houses” the Registry of the Canadian Stroke Network (RCSN); Appendix FIVE describes the “migration” of the information to ICES under section 45 of *PHIPA*.

The CPO is the “owner” of the policy and custodian of the documentation, maintaining a log of all PIAs, completed, undertaken but not complete, and not yet undertaken. The CPO has the authority and responsibility for requiring PIAs. ICES routinely retains independent third party experts to execute PIAs with ICES' content expertise assistance.

“The authority to conduct a systematic PIA lies with the CPO, who will review the project and the proposed need for PIA. Two paths are available: first, some types of PIA can be conducted internally using a template document. For large projects, the Sourcing and Procurement Office will be engaged to select an appropriate independent third party reviewer to execute the work.”

⁷⁰ ICES Systematic Privacy Impact Assessment Guidelines. pp1-2

Part 1 – Privacy Documentation

“Implementation of change management process and concomitant documentation related to recommendations and findings in the report document will be managed as directed by the CPO, CISO (or their designates), Directors and the Deputy CEO. The Director of the relevant program area is responsible for ensuring that a plan to implement the recommendations is drafted. The implementation plan shall include prioritized action items with responsibilities and time lines.”⁷¹

ICES’ *Systematic Privacy Impact Assessment Guidelines* requires that a PIA on a new information system or a change to an existing information system, technology or program involving PHI must be done at the conceptual design stage and then reviewed and amended, if necessary, during the detailed design and implementation stage. ICES preferentially treats PIAs as “living documents” which are amended using change management tables to track recommendations, changes made, and date/authorized person executing the change. Similarly, security assessments impacting privacy are the responsibility of the CISO/Security Lead.

ICES’ PIAs are required, pursuant to its policy, to contain at least the following elements:

- The data holding, information system, technology or program at issue;
- The nature and type of PHI collected, used or disclosed or that is proposed to be collected, used or disclosed;
- The sources of the PHI ;
- The purposes for which the PHI is collected, used or disclosed or is proposed to be collected, used or disclosed;
- The reason that the PHI is required for the purposes identified;
- The flows of the PHI;
- The statutory authority for each collection, use and disclosure of PHI identified;
- The limitations imposed on the collection, use and disclosure of the PHI;
- Whether or not the PHI is or will be linked to other information;
- The retention period for the records of PHI;
- The secure manner in which the records of PHI are or will be retained, transferred and disposed of;
- The functionality for logging access, use, modification and disclosure of the PHI and the functionality to audit logs for unauthorized use or disclosure;
- 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 the risks;
- Recommendations to address and eliminate or reduce the privacy risks identified; and
- The administrative, technical and physical safeguards implemented or proposed to be implemented to protect the PHI.

In order to close the risk management loop, ICES’ policy contains a process for managing the recommendations arising from PIAs. The CPO, Security Lead and CISO (or designates), collaboratively, are responsible for the associated response to recommendations and change management logging required, working with other ICES’ Directors as required.

⁷¹ ICES *Systematic Privacy Impact Assessment Guidelines*. p3

26. Log of Privacy Impact Assessments

ICES' CPO or designate maintains a log of PIAs that have been undertaken, whether completed or not. The following elements are contained in the log:

- the data holding, information system, technology or program involving PHI that is at issue;
- the date that the PIA was completed or is expected to be completed;
- the Agents responsible for completing or ensuring the completion of the PIA;
- the recommendations arising from the PIA;
- the Agents 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.

Privacy Audit Program

27. Policy and Procedures in Respect of Privacy Audits

ICES has a long-standing commitment to ongoing audit and improvement processes across the organization. Privacy and Security audits are conducted concomitantly at ICES, and are a long-standing part of ICES' overall privacy and security posture. In 2001, in consultation with the ICES Confidentiality Committee (now Privacy & Security Committee), a list of 105 potentially auditable activities was drafted in consultation with representatives of all ICES' role groups and scientist representatives. From these core documents, ICES has developed and implemented evolving processes for privacy and security audits. The goal of ICES' audit processes is always to ensure compliance with its privacy and security policies. These include, among others, these current examples:

- Audits to assess compliance with ICES' privacy and security policies, procedures, SOPs, standards, tools, guidelines and practices; through 'social engineering' experiments which are made part of overall annual security audits; e-logs of activities tied to privacy and security policies; and
- Audits of Agents' LAN-based (local area network) computers tri-annually, using automated technology or manual audit methods.

ICES' Agents developed a *Privacy and Security Audits Policy* to provide procedures related to this important activity.

“ICES will conduct regular audits to assess compliance with privacy and security policy instruments implemented by the Institute. Generally, auditing work will be undertaken between January and March of each three-year reporting cycle where possible. Notification of Agents of audit activities will be provided in advance during staff and/or role group meetings and internal email where possible.... When planning audits, the purposes of the audit and the nature and scope of the audit will be clearly articulated in the planning document or

Part 1 – Privacy Documentation

statement of work (SOW) for independent third party reviewers(i.e. document reviews, interviews, site visits, inspections).”⁷²

Against a background of limited resources, the Agents of the Privacy & Security teams endeavour to optimize audit opportunities by coupling annual high-priority areas (Secure Area Networks [SAN] threat-risk assessment, security audits, penetration testing, as examples) with alternate topic areas which may be less resource-intensive. One such example is coupling what are termed ‘social engineering’ experiments to security audits. These experiments test Agents’ compliance with policies.

The plans for these annual audits set out the purposes of both security audits and compliance-testing experiments, the nature and scope of the circumstances under which an audit is to be conducted, and the responsible party who will be conducting the work. These ‘social engineering’ audits are narrower in scope but chosen to focus on how a particular policy/ies, is/are complied with across the organization. Priority for these “topic” audits is given to sensitive, visible, or high risk activities. The CISO/Security Lead and CPO consult and plan these activities, in concert with the independent third party commissioned to audit and conduct these ‘social engineering’ evaluations. Examples of these include posing as an untagged, unescorted visitor rushing to a meeting within the restricted access areas, tailgating into secured areas, sending fictitious emails to provoke breach of policy, etc. Importantly, these audits also perform a remedial function by identifying gaps in ICES’ privacy and security policies, practices, standard operating procedures (SOPS) and other procedures, tools, guidelines and standards – and actual or potential vulnerabilities.

ICES’ Privacy and Security staff twice-annually review extensive logs related to coded keys, UNIX (SAN) access, local area network (LAN) accounts and ‘traffic’, and visitor security. Wherever possible, electronic start/stop dates are placed on accounts, and password changes are forced (both the LAN and the entirely separate and moated SAN [secure area network]) to provide auditable trails.

As per ICES policy *Confidentiality and Security of Data*, internal audits of Agents’ LAN-based personal computers are conducted tri-annually by the CPO and IT staff, as previously reported and provided to the IPC in 2005 and 2008. These audits serve several functions: policy adherence is the main driver of the work, but it also provides an intimate education/remediation opportunity for the privacy and IT staff in a non-confrontational setting. However, the downside to this type of review is that it is very labour-intensive and costly to do. Most recently (2010/11), ICES’ Security staff have been able to execute LAN audits using automated software, which is a replicable method for monitoring compliance over time and the success of remediation training. The automated audits revealed files which required manual checking by the CPO. As is the case usually, the findings of the 2010/11 LAN audit are benign; all files checked did not breach privacy policies. The results of this audit are found in the Recommendations related to security audit in Part 2, section 16. Finally, ICES’ Agents have been provided with a self-administered audit tool to facilitate “maintenance” of their LAN files on the background of ICES’ policies and SOPs.

⁷² ICES *Privacy and Security Audits Policy*. 1-2

Part 1 – Privacy Documentation

In order to close the loop on risk management, ICES' audits contain a process for managing the recommendations arising from privacy and security audits. The CPO, Security Lead and CISO (and/or designates), collaboratively, are responsible for the associated responses to recommendations and change management logging required, working with other ICES' Directors as required. Working with the content area Director and/or Communications staff, a plan for remediation, heightened instruction or policy change is planned and executed. Much of the communication strategy includes CISO/CPO-led discussion at staff meetings, keyed email messaging across the organization and topic management in ICES Privacy/Security newsletter. All material related to audits is retained by the CISO and CPO and logged.

The *Privacy and Security Audits Policy* sets out the nature of the documentation that 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.

28. Log of Privacy Audits

ICES' CPO and Privacy Office staff maintain a comprehensive log of audits. The log is comprised of five distinct spreadsheets, which include the following: log of historical reviews (1992 – 2000); log of PIAs; log of security reviews; log of penetration testing; and, a log of threat-risk assessments that have been completed. This log contains the following elements:

- The nature and type of audit conducted
- The name of the document, where it can be found, date the audit was completed
- The independent third party or employee responsible for completing the audit and document authors/version number
- The recommendations arising from the audit
- The staff members responsible for addressing each recommendation
- The manner in which each recommendation was or is expected to be addressed and the anticipated date of completion.

During the first six months of 2010, one-on-one meetings were held with each of the ICES' Project Managers to audit and discuss privacy and security needs for their projects. Each project was reviewed for the uniqueness and the manner that data was being collected, used and disclosed. This provided an important opportunity for the Project Managers to receive one-on-one privacy and security training. This also provided the Privacy Coordinator an opportunity to address or remediate any privacy and/or security issues.

Privacy Breaches, Inquiries and Complaints

29. Policy and Procedures for Information (Privacy/Security/Policy) Breach Management

ICES has an *Information Breach Policy* to address the identification, reporting, containment, notification, investigation and remediation of privacy breaches, which has been presented to the

Part 1 – Privacy Documentation

IPC in 2005 and 2008, with updates. This policy is built on the relationship within ICES of the Privacy and Security teams and their interconnectedness. Like other ICES' document formats, for ease of use the *Information Breach Policy* includes the *Information Breach Report* form. The *Information Breach Report* form is considered a “living” document until the investigation of breach is satisfactorily concluded and signed off.

The Policy defines a privacy breach in this fashion:

“ICES, as a s.45(1) prescribed entity, bases its privacy and security policies, practices, standard operating procedures (SOPS) and other procedures, tools, guidelines and standards for privacy and data security on requirements found in Ontario’s privacy law, PHIPA, and on good quality information found in privacy and security best practices documents. Sections 45(3) and 45(4) of PHIPA requires these policies, practices, standard operating procedures (SOPS) and other procedures, tools, guidelines and standards policies, must be reviewed and approved by the IPC tri-annually.”

“Because of the potential intertwining of these three components, all must be considered, investigated and reviewed whenever there is a breach concern. Collectively, they are referred to as “Information Security Breach” until such time as the type of breach is discerned.”

“A privacy breach occurs when PHI is collected, retained, used or disclosed in ways that are not in accordance with PHIPA and its regulation with ICES policy instruments or with ICES’ Data Sharing Agreements, Research Agreements, Confidentiality Agreements and Agreements with Third Party Service Providers or where PHI is stolen, lost or subject to unauthorized copying, modification or disposal.”

“Importantly, security breaches are potentially part of, or, lead to the breach of PHI or de-identified health information (HI). Security breaches may be policy breaches, attacks with malicious intent (internal or external), or unauthorized use or disclosure of information.”

“A policy breach occurs when an ICES policy, practice, standard operating procedure (SOP) or other procedure, tool, guideline or standard is not followed. This type of breach may not result in unauthorized disclosure of PHI or de-identified health information (HI), but must always be followed up for purposes of remediation or education of staff.”

“Examples of potential breach include:

- *storing unencrypted PHI on a USB key, laptop computer or CD is a ICES policy breach;*

Part 1 – Privacy Documentation

- *the unauthorized disclosure of PHI when PHI is stored on an unencrypted USB key, laptop computer or CD and is lost, stolen or misplaced is a privacy breach;*
- *inadvertent disclosure through human error (i.e. information meant for person A is actually sent to person B, or a cell size less than five is used in a study);*
- *transfer of identifiable data to or from the UNIX system or other ICES servers resulting in unauthorized disclosure.”*⁷³

ICES' *Information Breach Policy* requires the reporting of all privacy breaches or suspected privacy breaches, all security breaches or suspected security breaches, and all policy breaches or suspected policy breaches. Moreover, it has been designed to make it easy for Agents to do so. At the initial reporting stage of the breach response process, Agents are required to report a real or suspected breach immediately to the CPO, CISO/Security Lead and/or to their supervisor/manager (who will extend the notification) – and to initiate containment of the breach as quickly as possible, including changing passwords and/or identification numbers and/or temporarily shutting down a system (or server). Although all breaches are important by their very nature, of particular importance is the assessment of inadvertent public disclosure (outside ICES physical structure) of PHI and the threat to the privacy interests of citizens. The *Information Breach Policy* sets out the 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. The policy ensures that reasonable steps are taken in the circumstances to protect PHI from further theft, loss or unauthorized use or disclosure and to protect records PHI from further unauthorized copying, modification or disposal.

The *Information Breach Policy* and the companion *Information Breach Report form* instructs Agents that notification of a real or suspected breach should be done immediately in person or by telephone, with email only when the first two modalities do not result in contact. On the *Information Breach Report form*, Agents are asked to provide a description of the compromised data, when the privacy/security/policy breach or suspected privacy/security/policy breach was discovered, how it was discovered, the location, the cause of the breach or suspected breach (if known), the individuals involved, any other relevant information, and any immediate steps taken to contain the breach or suspected breach. The scope of investigation information expected includes document reviews, interviews, site visits, inspections, security tapes etc).

Upon being notified of a breach or suspected breach, the CPO, CISO or Agent's manager/supervisor initiate the cadence of activities articulated in a step-wise fashion in the *Information Breach Report form*. The Breach Response Team is notified and assembled and, working in collaboration with the areas affected by the breach or suspected privacy breach, implements the described process. The Breach Response Team is comprised of the CPO, CISO, the President & CEO, the Deputy CEO and the Director, Information Management. The composition of the Breach Response Team may differ from time to time depending on circumstances and availability.

⁷³ ICES *Information Breach Policy*. pp1-2

Part 1 – Privacy Documentation

“When a breach is discovered, a cadence of notification must be initiated. The person discovering or suspecting a breach begins the process by informing his/her immediate supervisor, the CPO or CISO of the finding or suspicion immediately and initiating containment of the breach as quickly as possible. Although all breaches are important by their very nature, of particular importance is the assessment of inadvertent public disclosure (outside ICES physical structure) of PHI.”

“The notification process will be expanded by the Agents/CPO and CISO to the President & CEO, Deputy CEO, and the Director, Information Management as the situation requires, up to and including the IPC. A notification chart is part of the Information Breach Report document to enable documentation of escalation of notification. Notification should be done in person or by telephone, with email only when the first two modalities do not result in contact and notification.”⁷⁴

The Breach Response Team determines consultatively whether and what type of breach has occurred. Additionally, the Breach Response Team identifies compromised data and the affected individuals and/or organizations and jurisdictions as needed.

The *Information Breach Report* form and *Policy* clearly defines ICES’ notification requirements, up to and including the MOHLTC, the IPC, ICES Board of Director, legal counsel and/or Police. The form is purposefully laid out in chart format so it is easy to use; Agents/staff can be upset. The notification process (i.e., when to notify, how to notify, who should notify, and what should be included in the notification) is determined, with consideration of guidelines or other material published by the IPC or other regulators, and in keeping with any specific requirements for notification that may be found in Agreements with data providers.

“The notification process will be expanded by the CPO to the CEO and Deputy CEO and CISO of ICES and, as the situation requires, up to and including the IPC. A notification chart is part of the breach reporting document to enable documentation of escalation of notification. Notification should be done in person or by telephone, with email only when the first two modalities do not result in contact and notification.

- (a) In the case of a breach of PHI related to information collected under ICES’ data-sharing agreement with the Ministry of Health, immediate notification of the Ministry and the IPC is required (see notification chart).*
- (b) In case of a breach of PHI or HI related to a data-sharing agreement (DSA) with one or various HICs, ICES is required by statute to notify the HIC(s) who provided the PHI of the information breach, in order that the HIC may notify the individuals to whom the PHI relates when required pursuant to subsection 12(2) of PHIPA.”⁷⁵*

⁷⁴ ICES Privacy Breach Policy. pp1-2

⁷⁵ ICES Privacy Breach Policy. p3

Part 1 – Privacy Documentation

It is not ICES' role to notify the individual(s) to whom the breached PHI belongs, but it is ICES' responsibility to notify the HIC/Data Custodian of record of the breach.

The *Privacy Breach Report* (investigative report) is submitted to President & CEO after review and signature by the CPO and/or CISO and the Agent discovering the real or suspected breach as needs be. A log of all breaches, real or suspected, is maintained by the CPO and Privacy Office.

In order to close the loop on remediation and risk management, ICES *Privacy Breach Policy* contains a process for managing the recommendations arising from a privacy breach.

“According to the extent and the impact of the information breach, several actions may be taken:

- *Need for extent of notification, will be assessed by the Core Breach Team in consultation with the Privacy & Security Committee as required.*
- *In the case of any breach, review of existing policies and necessary changes to ICES policies and procedures must be made in order to avoid another breach of a similar nature.*
- *In the case of an internal breach, the Privacy & Security Committee may also recommend action for the core Breach Team to implement.*
- *An education campaign within ICES will be carried out by the CPO and the CISO (and members of the Privacy & Security Committee as needed) in order to educate ICES Agents on how to avoid similar breaches.*
- *A review of the ICES Breach Policy will also be done in order to improve the response to a breach and ensure that a clear, concise protocol is in place.*
- *Finally, should it be determined, the Agent(s) responsible for the breach will be disciplined or terminated according to the terms in the ICES Confidentiality Agreement, in consultation with ICES' HR Department and the CEO and Deputy CEO.*

The CPO, the CISO, Security Lead and members of the Privacy & Security Committee (as needed) are responsible for ensuring that a plan to implement the recommendations is drafted. The implementation plan includes Agents' responsible, action items with roles, responsibilities and timelines clearly stated.

30. Log of Privacy Breaches

ICES' CPO maintains a log of privacy breaches. The log contains the following elements:

- The date of the breach
- The date that the privacy breach was identified or suspected and by whom;
- Whether the privacy breach was internal to the Institute or external;
- Whether the breach involved de-identified information or was a breach of policy;
- The nature of the PHI that was the subject matter of the privacy breach and the nature and extent of the privacy breach;

Part 1 – Privacy Documentation

- 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 the prescribed person or prescribed entity 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; and
- The manner in which each recommendation was or is expected to be addressed.

31. Policy and Procedures for Privacy Complaints and Privacy Inquiries

ICES approach to privacy complaints and inquiries has been a “blended” set of documents, most clearly described in its *Privacy Code*. *ICES’ Privacy Code* sets out that a “privacy complaint” includes concerns or complaints relating to the privacy policies, procedures and practices implements by ICES, which relate to the compliance of ICES with PHIPA and its regulation.

Privacy Complaints

ICES has received no complaints since PHIPA came into being in November 2004.

ICES has a long-standing policy statement within its *Privacy Code* and public information brochure providing information to enable public privacy complaints and/or privacy inquiries related to projects and/or ICES’ compliance with PHIPA and privacy principles.

Within *ICES Privacy Code*, Principle 10 provides information about how an individual can challenge ICES’ compliance with PHIPA and with the ten guiding principles of good privacy practices:

“An individual can challenge ICES’ compliance with PHIPA and with the ten guiding principles via the designated persons accountable for ICES’ compliance. These individuals will generally include the Chief Privacy Officer (CPO) and the Local Privacy Officers (LPOs) at ICES’ expansion sites. ICES’ CPO may be contacted using privacy@ices.on.ca or by calling 416-480-4055 or mailing their concerns to ICES mail address. LPO addresses are available on the ICES or expansion site’s website as well.”

“Individuals are asked to provide pertinent, detailed information by letter, telephone or email related to the complaint to enable ICES’ CPO (or designate) to investigate and to respond reasonably. ICES’ Agents will acknowledge receipt and will communicate the decision to provide explanation, investigate or decline to investigate within 15 days of receipt. ICES’ designated Agents will notify other persons or organizations of the inquiry or complaint as needed.”

“In the event that the complaint will be investigated, the /CPO or designate will notify the complainant, using the communication modality of their choice,

Part 1 – Privacy Documentation

advising that an investigation will be undertaken, explaining the procedure, indicating next steps with a projected timeframe for completion, and identifying the nature of the documentation that will be provided to the individual following the investigation.”

“Individuals may also make a complaint about ICES’ practices by contacting the Office of the Information and Privacy Commissioner of Ontario at www.ipc.on.ca or by calling 416-326-3333 (Toronto area) or 1-800-387-0073 (within Ontario).

- 10.1 ICES has put simple and accessible procedures in place to receive and respond to complaints or inquiries about its policies and practices relating to the handling of PHI and all health information held at ICES.*
- 10.2 Individuals with inquiries or complaints will be informed in a timely fashion by ICES about relevant procedures.*
- 10.3 ICES will investigate all complaints in a timely fashion. If a complaint is found to be justified, ICES will take appropriate measure, including amending its policies, practices and procedures if necessary. These will be communicated to the complainant in a timely fashion by telephone, email or mail, as preferred”⁷⁶*

ICES’ website Privacy Section states clearly on the first page,

“For more detailed information on our privacy policies and practices, please refer to the following documents, or contact...the Chief Privacy Officer at privacy@ices.on.ca.”⁷⁷

In order to close the loop on remediation and risk management, ICES’s policy contains a process for managing the recommendations arising from the investigation of a privacy complaint.

“ICES will investigate all inquiries and complaints in a timely fashion. If a complaint is found to be justified, ICES’ CPO will notify the CEO, Deputy CEO and such Directors of the organization as is appropriate. ICES will also take appropriate measures, including amending its policies, practices and procedures as necessary. These will be communicated to the complainant in a timely fashion by telephone, email or mail, as preferred.”⁷⁸

ICES’ Public Information Brochure, *Our Business is Research, Our Priority... Privacy*⁷⁹, posted on ICES website, also provides three types of contact information (email, mail or telephone). This document is also available upon request in a printed format.

⁷⁶ ICES Privacy Code. Principle 10.

⁷⁷ See http://www.ices.on.ca/webpage.cfm?site_id=1&org_id=119

⁷⁸ ICES Privacy Code. Principle 10

⁷⁹ See <http://www.ices.on.ca/file/ACF209.pdf>

As required by the Regulation to PHIPA, ICES makes the following information available to the public:

- Name and/or title, mailing address and contact information of the CPO and LPOs at ICES satellites, to whom complaints may be directed
- The fact that privacy concerns or complaints may be made in writing, by email or by telephone
- The fact that individuals may also make complaints regarding compliance with PHIPA and its regulation to the IPC
- The contact information for the IPC

The CPO welcomes public inquiries related to privacy concerns in any activity in which ICES engages. ICES has received inquiries about projects and studies from the public and tracks these as well in what is now called the “*ICES Complaints & Inquiries Log*”, as required in the policy *General Public Inquiry Relating to Management & Protection of Personal Health Information*.

“Upon the receipt of the inquiry or request for more information, the Chief Privacy Officer (or designate) will log the inquiry or request; the Chief Privacy Officer will review the request and respond within 15 business days.”⁸⁰

ALL INQUIRIES are followed up; the log collects all pertinent information related to the inquiry (or complaint) to ensure that all recommendations arising from investigations are addressed. All inquiries received to date have been made by telephone or email, and have been resolved by direct contact between the CPO and the individual making the inquiry. Using a combination of the IPC website, the Government of Ontario website and the ICES website, the CPO reviews the various core components of any inquiry with the individual so that satisfaction with the answer and comfort with the issue has been achieved. All inquiries over the last six years have related to health card number disclosure and their management with encryption. Scientific Agents in charge of projects where inquiries and/or complaints are made are notified; they and their staff are engaged in various training activities to remediate any deficiencies. Training tools have been developed and more intensive orientation sessions provided in relation to these types of inquiries.

Privacy Inquiries

Second, ICES’ *General Public Inquiry Relating to Management & Protection of Personal Health Information Policy*⁸¹, provides basic instructions for inquiries related to obtaining information (or more information, if the case may be) about ICES’ practices. That *Policy* sets out that a “privacy inquiry” is an inquiry related to the privacy policies, procedures and practices implemented by ICES and related to the compliance of ICES with PHIPA and its regulation.

⁸⁰ ICES *General Public Inquiry Relating to Management & Protection of Personal Health Information Policy*. p1

⁸¹ *Ibid.* p1

Part 1 – Privacy Documentation

The ICES Privacy Code and the *General Public Inquiry Relating to Management & Protection of Personal Health Information Policy* establishes the process that ICES follows in receiving privacy inquiries setting out all requirements. The process includes the following elements:

- The CPO is responsible for receiving the privacy complaint or inquiry, which is logged
- Individuals are asked to provide pertinent, detailed information related to the complaint or inquiry to enable ICES Agents to investigate and to respond reasonably
- The CPO and/or designate must make a determination whether to investigate the complaint or inquiry within 15 days based on the circumstances related to each complaint. ICES always responds to public inquiries
- In the unlikely event that no investigation will be undertaken, the CPO and/or designated staff will email or send a letter to the complainant advising of such and advising that the complainant, may complain to the IPC, if there are reasonable grounds to believe that ICES has contravened or is about to contravene PHIPA and its regulation
- In the event that the complaint and inquiry will be investigated, the CPO and/or designate will send a letter to the complainant advising that an investigation will be undertaken, explaining the procedure, indicating next steps with a projected timeframe for completion, and identifying the nature of the documentation that will be provided to the individual following the investigation

ICES has received inquiries from the public, which are carefully logged. ICES' usual practice is to contact the individual making the inquiry as soon as possible and work through the questions of interest to the caller (see section 32).

In order to close the loop on remediation and risk management, ICES's policy contains a process for managing the recommendations arising from the investigation of a privacy complaint.

“ICES will investigate all inquiries and complaints in a timely fashion. If a complaint is found to be justified, ICES' CPO will notify the CEO, Deputy CEO and such Directors of the organization as is appropriate. ICES will also take appropriate measures, including amending its policies, practices and procedures as necessary. These will be communicated to the complainant in a timely fashion by telephone, email or mail, as preferred.”⁸²

32. Log of Privacy Complaints & Privacy Inquiries

ICES' CPO maintains a log of *Privacy Complaints and Inquiries* that have been received. The log dates back to fiscal 2004/5 and contains the following elements. The log is maintained on ICES' privacy shared drive and collects the following information:

- The date that the privacy complaint/inquiry was received, who the person making the complaint/inquiry with contact information provided and the nature of the complaint/inquiry;

⁸² ICES Privacy Code. Principle 10

Part 1 – Privacy Documentation

- The determination as to whether or not the privacy complaint/inquiry will be investigated further (as all are investigated by the CPO) and the date(s) of investigation;
- The date that the individual making the complaint/inquiry was provided a response to the complaint/inquiry;
- The CPO or designate responsible for conducting the investigation;
- The dates that the investigation was commenced and completed;
- The recommendations arising from the investigation;
- The Agent(s) responsible for addressing recommendations and the date each recommendation was addressed or timeline for completion;
- How the recommendation was/is expected to be addressed;
- Date the person initiating the privacy complaint/inquiry was advised of the findings/measures taken in response to the complaint/inquiry.

33. Policy and Procedures for Privacy Inquiries

Not applicable.

Part 2 - Security Documentation

General Security Policies and Procedures

1. Information Security Policy

ICES has developed an overarching *Information Security Governance Framework* that sets out its commitment to secure the PHI it receives, as well as a suite of security policies, practices, guidelines, standards, SOPs and other procedures and tools. The *Information Security Policy* is the backbone of ICES's security program and provides evidence of the commitment to security and privacy at ICES as "mission critical". Of particular importance is the commitment in the policy that ICES will take reasonable steps to ensure that the PHI it receives, is protected against unauthorized copying, modification, theft, loss, unauthorized use and disposal. PHI is de-identified as first use, and source data is stored in a highly secured vault behind many layers of diminishing accessibility.

The *Information Security Policy* requires ICES to undertake comprehensive threat and risk assessments of all information security assets, particularly de-identified information and PHI. Security reviews are to be done, at an organization-wide level, as well as for certain specific projects. ICES' Procurement Office develops RFPs (Request for Proposals) which include the scope of and statement of work for all third party assessments. These RFPs require documentation of a methodology for identifying and assessing risk. The remediation of risks and prioritizing all threats and risks identified for remedial action is also outlined in ICES *Information Security Policy*.

"Annual technical security audits will be performed by impartial third-party assessors. These assessors must be qualified to perform the work and report findings in a clear and practical, actionable manner. Remediation action on the findings must be evaluated and proposed to the CEO/Deputy CEO within 30 days of the final report. All findings of an elevated level, (eg. "Critical" or "High" Risk) must be addressed".

"All new projects will undergo an impact assessment to evaluate whether they require a Threat-Risk-Assessment (TRA), either internally or by an external party. New projects that are considered by the CISO or other senior management to pose new or elevated risk to ICES will require a TRA".⁸³

ICES' *Information Security Policy*, *Security Quality Assurance* and *Information Security Governance* documents mandate, a comprehensive information security program that consists of industry- standard administrative, technical and physical safeguards to protect PHI and that is amenable to independent verification.

⁸³ ICES *Information Security Policy*. p1-2

“In conjunction with the ICES Information Security Framework, this Information Security Policy is intended to provide the instruction and direction to the organization. The policy direction here is to assist in the implementation of appropriate security controls to support the privacy efforts and initiatives that protect the sensitive data that ICES has the privilege to hold.”⁸⁴

“The Security Quality Assurance (SQA) program is an ISO 27001 based assurance program that is composed of 10 modular assessment components. Each of these components addresses areas of compliance for information security such as technical scanning, legislative compliance, BCP/DR, etc. The SQA is a cost effective means to assess projects for the right criteria and in the right timeframe. The assessment components are selected based on the appropriateness for the project at hand rather than arbitrarily as is found in other assessment methodologies.”

“The fundamental principle of the SQA program is to engage all Security/IT Team Members in proactive monitoring of systems to prevent or reduce downtime, automation of tasks to reduce errors and detailed logging of events and tasks to ensure commitments are met. This is all done following a detailed set of industry best practice tools based on IT Infrastructure Library (ITIL) methodologies.”

“The SQA will help establish a baseline for ongoing compliance. It is repeatable and measureable and, thus, will ensure ongoing compliance.”

Objectives for the SQA program include:

“Ensure industry acceptable security controls are in place – Our stakeholders demand certain controls and design characteristics with regard to security being met prior to the launch of many services, the SQA will test and assist the business meet and exceed these client requirements...”⁸⁵

ICES’ comprehensive *Information Security Framework* requires that ICES’ security program consist of the following elements:

- A security governance framework for the implementation of the information security program, including security training and awareness;
- Policies and procedures for the ongoing review of the security policies, SOPS and other procedures, standards, guidelines, tools and practices are implemented;
- Policies and procedures for ensuring the physical security of the premises;
- 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, data in use and data in motion***;
- Policies and procedures to establish access control and authorization including business requirements, user access management, user responsibilities, network access

⁸⁴ ICES Information Security Policy. p1

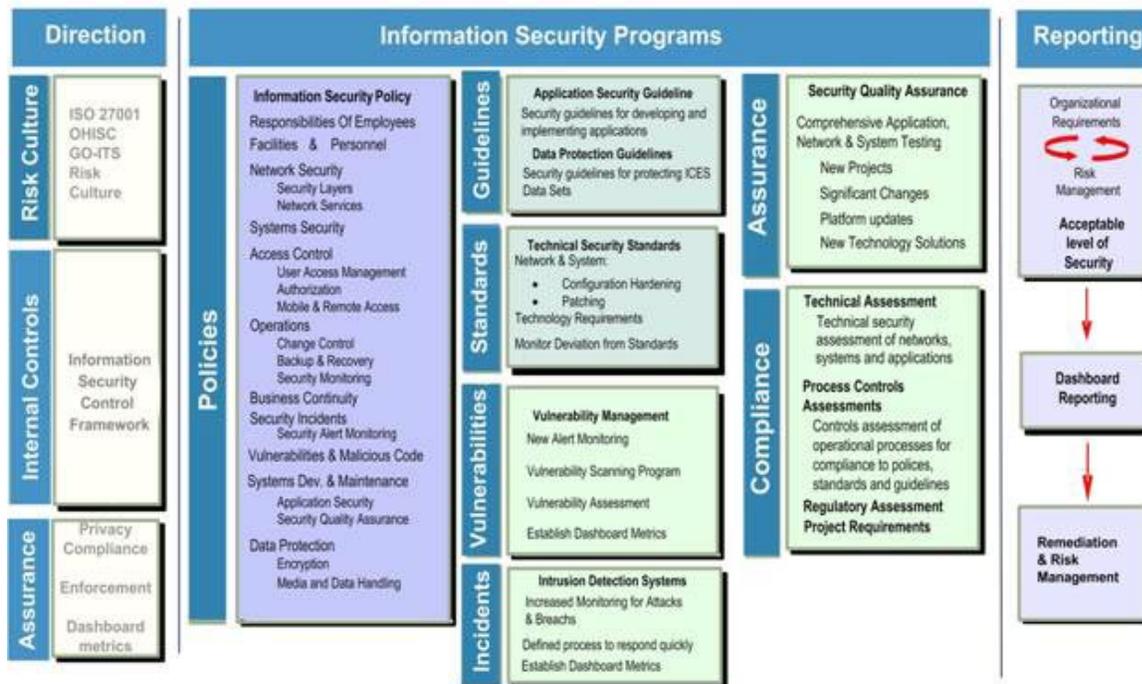
⁸⁵ ICES Security Quality Assurance. p1

Part 2 – Security Documentation

control, operating system access control and application and information access control;

- Policies and procedures for information systems acquisition, development and maintenance including the security requirements of information systems, correct processing in applications, cryptographic controls, security of system files, security in development and support procedures and technical vulnerability management;
- Policies and procedures for monitoring, including policies and procedures for maintaining and reviewing system control and audit logs and security audits;
- Policies and procedures for network security management, including patch management and change management;
- Policies and procedures related to the acceptable use of information technology;
- Policies and procedures for back-up and recovery;
- Policies and procedures for information security breach management; and
- Policies and procedures to establish protection against malicious and mobile code.
- A credible program for continuous assessment and verification of the effectiveness of the program

ICES Information Security Framework



The goal of the *Information Security Framework* is to define the supporting governance programs the CISO and Security Lead/team have developed and continue to develop.

The *ICES Information Security Framework* schematic shown above outlines the security infrastructure implemented by ICES, which is built on a suite of policy instruments, relating to the tactical controls that robust governance programs require:

- The transmission of PHI over authenticated, encrypted and secure connections;

Part 2 – Security Documentation

- The establishment of hardened servers, firewalls, demilitarized zones and other perimeter defences;
- Anti-virus, anti-spam and anti-spyware measures;
- Intrusion detection and prevention systems;
- Privacy and security enhancing technologies; and,
- Mandatory system-wide password-protected screen savers after a defined period of inactivity.

ICES' *Confidentiality Agreement*, as previously stated in Section One, requires all ICES' Agents to comply with all its policies.

2. Policy and Procedures for Ongoing Review of Security Policies, Procedures and Practices

ICES *Review of Privacy and Security Policies, Procedures and Practices* policy for the ongoing review of its privacy and security policies has been developed in order to determine whether any amendments are needed or whether new security policy instruments are required.

The *Review of Privacy and Security Policies, Procedures and Practices* policy states that a shared approach will be taken by the CPO, CISO and Security Lead, with the assistance of the ICES Privacy Office/ IT/security staff and the expansion sites' LPOs, to undertake the review annually. As previously stated in this report, ICES' usual approach to review is quite iterative – one of vigilance, assessment and response in an ongoing fashion. Every attempt is made to align these document reviews with final fiscal quarter security testing.

In undertaking the review and determining whether amendments and/or new security policies, procedures and SOPs, tools, guidelines, and practices are necessary, the *Review of Privacy and Security Policies, Procedures and Practices* policy indicates that the following will be considered:

- Any orders, guidelines, fact sheets and best practices issued by the IPC under PHIPA and its Regulation;
- Evolving industry security standards and best practices;
- Technological advancements;
- Amendments to PHIPA and its Regulation;
- Recommendations arising from privacy and security audits, privacy impact assessments, threat-risk assessments and investigations into privacy complaints, privacy breaches and information security breaches;
- Whether the privacy policies, procedures and practices of the prescribed entity continue to be consistent with its actual practices; and
- Whether there is consistency between and among the privacy and security policies, procedures and practices implemented.

The policy indicates that the CPO and CISO/Security Lead will be responsible for amending and or drafting of new policies if deemed necessary after the review. The CPO and CISO/Security Lead will be responsible for obtaining approval of any such amendments or additions to the

policy suite. Further, the CPO, CISO, Security Lead are responsible for working with the Director, Communications and staff to communicate the changes or additions by intranet posting, notification of Role Group leads and the corporate email system (listserve), and with the Human Resources team in relation to training. This team will work collaboratively to ensure communication materials available to the public and other stakeholders are reviewed and amended accordingly, the procedure for which is set out in the policy. All broadcast and presentation materials are reviewed and approved by the Director, Communications prior to dissemination.

Physical Security

3. Policy and Procedures for Ensuring Physical Security of PHI

A suite of policies and SOPS ensure physical security at ICES – technological, administrative and physical protections – have been previously presented to the IPC in the 2005 and 2008 reviews. These are augmented or modified as technology and privacy/security best practices change. ICES’ *Access to Health Data Policy*, *Confidentiality and Security of Data Policy*, *Building/Office Access/Security Policy*, *Privacy Code*, *Incident Management Policy*, *Visitor Policy* and the *ICES Confidentiality Agreement* are some of the core documents, supported by technology SOPS and ongoing audit/review requirements. ICES’ physical safeguards protect PHI against theft, loss and unauthorized use or disclosure and help to protect the same from unauthorized copying, modification or disposal.

Policy, Procedures and Practices with Respect to Access by Agents

No ICES Agent has access to PHI other than Abstractors and Authorized Data Covenantors; Administrative Data Covenantors, Primary Data Covenantors and Application Covenantors, as previously described. The *Access to Health Data*⁸⁶ policy requires implementation of controlled access to the premises and to locations within the premises where records of PHI are retained. The *Confidentiality and Security of Data Policy*⁸⁷ sets out ICES process for determining access levels, and communicates decisions related to access levels. The policy is posted internally on the ICES intranet.

“Principles and procedures for confidentiality and security of data are to be strictly enforced and adhered to in order to respect the privacy of users and providers of the health care system, and to protect data/databases against loss, destruction or unauthorized use.”

ICES’ premises are divided into a minimum of three levels of security with each successive level being more secure and restricted to fewer individual Agents. In order to gain physical access to PHI, individuals with unauthorized or malicious intent would be required to pass through more than three levels of security and have coded access instruments to do so.

⁸⁶ *Access to Health Data Policy*. pp1-2

⁸⁷ *Confidentiality and Security of Data Policy*. pp2-7

“Electronically controlled key access divides the building into levels of security, each successive level being more secure and restricted to fewer employees (full and part-time employees, contract workers/consultants, students and affiliates). The same system provides a detailed audit record every time a coded... key is used in a lock... Access to the room which contains the administrative data server (i.e., UNIX room) is highly restricted to designated persons... The building has continuous 24/7/365 video camera surveillance with central monitoring and responsive security staff services... Glass breakage detectors set off alarms if outside windows are broken... vibration detection sensors... Written approval for access to data housed at ICES (primary, secondary or administrative) must be obtained from the CEO ... Data tapes that contain identifiers are accessible only to designated persons (the Director, Information Management or the named, Authorized Data Covenantors) as outlined in the MOHLTC – ICES research agreement... Data tapes and cartridges are kept in fire-proof tape safes behind multiple levels of security doors.”^{88 89}

The process to be followed in providing identification cards and keys to the premises and locations within ICES premises, including required documentation, is defined in the ICES *Building / Office Access/Security Policy* and the Manager, Administration is designated as responsible for this process. Log books of Marlok keys and exterior keys are maintained by the Manager Administration. Requisitions for Agent identification cards are completed electronically by the Manager Administration and sent by email to Sunnybrook HSC Personnel Services to be made.

Theft, Loss and Misplacement of Identification Cards and Keys

ICES’ *Building / Office Access/Security Policy* defines the specific process to manage identification cards and keys in the event of loss, theft, or misplacement. Agents are required to advise the Manager, Administration OR the CPO as soon as reasonably possible of the loss, theft, or misplacement of identification cards and keys. A process is in place for requesting the replacement of identification cards and coding replacement access keys. The lost key is decoded immediately in the computer in accordance with internal processes before a new access key(s) is issued. The Sunnybrook Health Science Centre Security Office is also notified by the Manager, Administration of the loss of identification credentials prior to approving/issuing a new identification card.⁹⁰

Termination of the Employment, Contractual or Other Relationship

In accordance with ICES’ *Termination of Employment* policy, access to ICES premises terminates upon termination of the employment, contractual or other relationship.

All scientists and employee supervisors are required to advise ICES’ Human Resources Department and the Deputy CEO of a termination of their relationship with ICES. Human

⁸⁸ ICES *Confidentiality and Security of Data Policy*, pp2-7

⁸⁹ ICES’ *Information Asset Management Policy*

⁹⁰ ICES *Information Asset Management Policy*

Part 2 – Security Documentation

Resources staff notifies the IT department of resignations and terminations so that appropriate steps can be taken to close accounts in a timely fashion. All individual Agents leaving ICES must return their identification cards, keys, laptops and/or other technology on or before the termination date. Email, LAN (local area network) and UNIX access is terminated immediately at 5pm on the last day at ICES for all Agents of all levels. The process is set out in ICES' *Termination of Employment Policy* and is the responsibility of the Supervisor, or in the case of scientific faculty, the Deputy CEO. Please consult Part 3 *Human Resources Documentation* for more information.

Notification When Access is No Longer Required

The *Termination of Employment* policy requires similar reporting of the resignation of an Agent who has been granted access to a location where records of PHI are retained. Notification of Data Covenantor resignation (and replacement Covenantor) is communicated to the IPC and MOHLTC as soon as is reasonably possible. Access is terminated on the final day as described in the section above. When a Data Covenantor decides to leave that role, notification is provided by the Director, Information Management to the CPO, Security Lead, IT Manager and HR. Access level is reduced according to the new role (usually analyst) as per ICES' *Access to Health Data at ICES Policy*⁹¹.

Audits of Agents with Access to the Premises

It is ICES' practice to audit the following every six months: key logs, UNIX accounts, Transfer PC accounts, email accounts and studentship logs. This review is conducted collaboratively by the CPO, CISO, Security Lead, the IT Manager and the Manager Administration, to ensure that Agents with access to the physical premises and de-identified information continue to have an employment relationship with ICES and require the same level of access. Logs are reviewed up to one year out as a second, fail-safe mechanism related to resignation, termination, and change in access status.

Tracking and Retention of Documentation Related to Access to the Premises

The *Confidentiality and Security of Data Policy* requires that the CPO and the Manager, Administration and designates are responsible for maintaining a log of Agents granted access to ICES premises. **All Agents** are required to undergo privacy and security orientation and to sign ICES *Confidentiality Agreements* on their first day of access to ICES' premises. Individuals who function as Data Covenantors and have access to records of PHI must undergo privacy and security orientation and sign the *Confidentiality Agreement for Data Covenantors*. The CPO, Manager Administration, CISO and their designates are also responsible for ensuring that all documentation related to the receipt, review, approval and termination of such access and to LAN-based email is maintained in electronic logs in the secured server rooms.

“ICES administration will ensure that all Agents of ICES...and associates (collaborators not formally affiliated with ICES), receive an orientation to the principles of privacy, confidentiality and security”.

⁹¹ ICES *Access to Health Data at ICES Policy*. p1-2

Part 2 – Security Documentation

ICES is planning changes to physical access to the building by replacing Marlok key access with card access readers with an anti-passback feature. The contract has been awarded and anticipated completion is Fall 2011.

Policy, Procedures and Practices with Respect to Access by Visitors

ICES' *Visitor Policy* sets out its comprehensive process for screening and supervising visitors to ICES premises. ICES Agents/Reception staff are responsible for identifying, screening and supervising visitors.

“Visitors require special identification and escorts, and all visits must be tracked through a sign-in system... visitors should be informed in advance that they will have to sign in, wear a visitor’s badge, and sign out when the meeting is concluded, returning the visitor badge to Reception. Badges are in distinct, bright colours: one for visitors attending meetings (VISITOR - Blue)... one for those attending rounds (VISITOR - Yellow), and a third category (DAY PASS – Red) for those who will be on-site for several hours or an entire day.”⁹²

“On arrival in the lobby, visitors for meetings with ICES Agents must present themselves at ICES Reception. The Receptionist notifies the contact person, verifies that a meeting will take place, requests an escort, and issues a... numbered visitor’s badge. Badges are controlled in locked cabinets in the Reception Office. Visitors sign into the logbook at Reception. The logged entry must show date and time of arrival at ICES, visitor’s name, visitor badge number assigned, name of ICES Agent who escorts the visitor to a meeting.”

“All visitors are required to wear their badges while they are at ICES. If any Agent sees a individual within ICES who is not wearing an identification badge and whom they do not recognize, the Agent should approach the person offering assistance and provide guidance as required, or escort them to the lobby where they can be met by the ICES Contact.”

“All visitors must return to and exit via the lobby, recording their time of departure in the logbook and returning the visitor’s badge to the receptionist. When meetings run after business hours, ICES Agents are responsible for retrieving visitor ID and signing the visitor out.”

ICES' Reception staff must also ensure that all visitor requirements are met, as set out below. Logs are maintained for a period of seven years.

Visitors are required to:

- Record their name, date, time of arrival
- Record their time of departure
- The name of the Agent whom they are meeting

⁹² ICES Visitor Policy. pp1-2

Part 2 – Security Documentation

- Wear an ICES visitor identification badge at all times on the premises
- Be escorted by an ICES' Agent at all times while on ICES premises
- Return their identification upon their departure

4. Log of Agents with Access to ICES Premises

ICES' Manager HR, Manager Administration and Director Research Practice collectively contribute to a log of **all Agents** granted approval to access ICES premises and the level of access granted. The log includes the following elements:

- The name of the Agent granted approval to access the premises;
- The level and nature of the access granted;
- The locations within the premises to which access is granted;
- The date that the access was granted;
- The date(s) that identification cards and keys were provided to the Agent;
- The date that the identification cards and keys were returned to ICES' Manager Administration.

Audit of these logs is described earlier in this document, where access is cross-checked by senior staff.

Retention, Transfer and Disposal

5. Policy and Procedures for Secure Retention of Records of PHI and de-identified Information

The secure retention of electronic PHI is central to ICES' privacy and security programs and is governed by a suite of policies, practices, SOPs and other procedures, guidelines, tools and standards, including ICES' *Information Asset Management Program*; *Confidentiality and Security of Data Policy*; ICES' *Data Retention Policy*; ICES *Offline Chart Abstraction tool*; *DM001: Receiving project-specific data sets from external sources*; *DM002: Receiving and Processing Administrative Data*; *DM003: Destruction of 3rd Party Health Data*; ICES *Privacy Code*; *ICES Data-sharing Agreements*; *ICES Confidentiality Agreement* and ICES' *Confidentiality Agreement for Data Covenantors*; *Access to Health Data Policy*; ICES' *Protecting PHI on Mobile Devices Policy*; *ICES Project-Specific Privacy Impact Assessment form*; and, *Primary Data Collection Project Management Checklist*, among others.

ICES' approach with this comprehensive suite of policy-equivalent instruments defines the retention periods for all de-identified information, referring to retention periods set out in approved written study proposals, Data Sharing Agreements and other contractual arrangements, but mandating always that PHI shall be de-identified upon collection and not retained longer than is necessary to fulfill the purposes for which it was collected. The policy designates ICES' Director, Information Management and its' Data Covenantors as responsible for ensuring that both de-identified information and PHI are retained in a secure manner. This is accomplished by:

Part 2 – Security Documentation

“Data that has been collected by ICES and is considered PHI under PHIPA must be protected as per that legislation and ICES’ Information Asset Management program.”

“The first use of PHI at ICES is the de-identification of the data”.

“Access to the PHI must be restricted to those individuals that need to have access to perform their jobs, are named data covenantors or ICES’ Agents that have signed confidentiality agreements.”

“Data will only be held at ICES as long as is necessary for the fulfillment of the purpose for which it was collected. The DSA under which it is collected under must define the date of destruction.”⁹³

The Project-specific PIA must also stipulate the data destruction date. De-identified information is treated in the same careful fashion as identified data.

ICES does not contract a third party service provider to retain PHI on its behalf.

Note on Secure Retention of Administrative Data at ICES

At ICES, there is one important exception related to data retention and destruction.

ICES has had (dating back to 1995) and has currently a DSA with the MOHLTC which allows for regular feeds of PHI retained in administrative databases from numerous areas of the Ministry on an ongoing basis. These data support the vast majority of ICES projects carried out to fulfill its section 45 mandate.

Due to the retrospective/prospective nature of most ICES projects and the ongoing demand by ICES projects for these data, they are retained until such time as the data sharing agreement is declared void by either party. ICES will then be obligated to destroy all of the data.

ICES commits to taking all reasonable steps to ensure that source-level PHI is protected against theft, loss, unauthorized use or disclosure, unauthorized copying, modification or disposal using the suite of policy instruments listed above, among others.

“[sic] Source-level PHI that has been received at ICES will be handled by the Director Information Management and held behind, at least 4 layers of physical security when stored.”

“Source-level media containing PHI will be stored in the secure data safes located at ICES.”⁹⁴

⁹³ From ICES’ Data Retention Policy. p1

⁹⁴ From ICES’ Data Retention Policy. p1-2

Back-ups of the original PHI are made to external hard drives, which are then securely stored with the original media in a number of fire-proof safes located in highly restricted parts of the building. Records are maintained of the arrival and storage of these data. Similar agreements and practices are in place for PHI collected from other prescribed entities and prescribed persons.⁹⁵

A list of administrative databases and rationale for use can be found on ICES' website.

6. Policy and Procedures for Secure Retention of Records of PHI on Mobile Devices

ICES' policy *Protecting PHI on Mobile Devices Policy* governs the retention of PHI and de-identified information on mobile devices.

In the policy, mobile devices are defined as:

*“Portable electronic devices that can be used to collect and transport data such as laptops, personal data assistants (PDA), cell phones, and mobile storage media such as external hard drives, USB keys, jump drives, CDs, DVDs and diskettes”.*⁹⁶

The policy provides the following instructions:

*“As a Prescribed Entity authorized in section 45 of PHIPA and its Regulation, ICES may collect PHI from HICs for the purposes of analysis, evaluative studies and compiling statistical information with respect to the management, evaluation, monitoring, allocation of resource to or planning for the health system. However, appropriate safeguards need to be in place to ensure that the privacy and security of this information is protected at all times. The IPC recognizes that PHI may be most effectively transported and used in an electronic format, necessitating the use of Mobile Devices outside of the workplace. Notwithstanding the ease and portability of electronic devices, there are significant inherent risks such as potential loss or theft that must be carefully managed from a risk perspective. PHIPA and subsequent orders issued by the IPC, require that all reasonable steps are taken to ensure that PHI in ICES' custody or control is protected against theft, loss and unauthorized use, disclosure or modification.”*⁹⁷

The *Protecting PHI on Mobile Devices Policy* is consistent with orders issued under PHIPA and its Regulation, as well as with the various guidelines, facts sheets and best practices issued by the IPC.

“The use of mobile devices for the collection and/or transmission of individual level Data or PHI must be: a) authorized; b) in compliance with all applicable

⁹⁵ Note on Secure Retention of Administrative Data at ICES. D DeBoer, Director Information Management. Affirmed November 2010.

⁹⁶ ICES' *Protecting PHI on Mobile Devices Policy*. p1

⁹⁷ Ibid. p2

Part 2 – Security Documentation

ICES policies and procedures; and c) documented on the project-specific PIA form along with a description of the methods used to protect the data.”

*“Any files containing PHI on the mobile device **must** be encrypted. Both the mobile device and files must be protected with a minimum of two different complex passwords (see ICES password policy), or one complex password with biometric launch... Programming must be written that de-couples Health Information from PHI, which is stored in a separate file (a cross-walk table) away from the Health Information... Health Information, collected under a unique study number, should not be retained or stored on a mobile device. Transfer of the information to ICES secure systems and erasure from the device once the transfer is validated should be performed regularly with the shortest possible retention on the device with the assistance of IT and appropriate ICES data covenantor. All health information on mobile devices should be deleted when no longer required for the documented purpose as per IPC Mobile Devices directive.”*

ICES minimizes the retention period of PHI on a mobile device, and endeavours to collect at source and securely transfer the information as quickly as possible as per its data collection policies. Preferentially, ICES is moving to a model using only web-based collection or secured virtual private network (VPN).

Only variables needed to serve the purpose of the study are collected. Excerpts from ICES’ SOP *ISO-001 Preparing and Deploying Mobile Devices*, lays out the protection required on the mobile device by Agents of the IT/IS staff.

“For all ICES primary data collection (PDC) projects using mobile devices, the devices will be purchased, prepared, deployed and documented by ICES Agents/IT/IS staff; these Agents will also be responsible for ensuring the deletion of data from the hard drive of the mobile device... IS Agents will install all required software on the mobile devices (current ICES operating system, database application, anti-virus software and data encryption software). Appropriate documentation will be maintained by IS Agents... a minimum of two levels of password security will be installed, one for system security and one for data security. A third level of security to the database module itself is optional. Passwords must follow ICES “strong” password policy; the two passwords must be different”.⁹⁸

ICES permits PHI collected in the field to be “pushed” or “pulled” remotely through a secure connection or secure virtual private network (SSL-VPN), with approval and direction from the CISO and/or the Director, Information Management (Administrative Data Covenantor) and their designates on the IT/IS team. These data are collected and pushed/pulled directly onto secured ICES servers; the information **never resides** on the encrypted mobile device.

⁹⁸ ICES *Preparing and Deploying Mobile Devices*. pp1-3

Approval Process

This section is not applicable.

Conditions or Restrictions on the Remote Access to PHI

This section is not applicable.

7. Policy and Procedures for Secure Transfer of Records of PHI

ICES works during the DSA process with all stakeholders to enable its collection of PHI in a highly secured fashion.

ICES has developed a suite of policy instruments to ensure the secure transfer of PHI in electronic format. ICES took into account the applicable Orders, guidelines, fact sheets and best practices issued by the IPC under PHIPA and its regulation. Documents which make up the core of these policy instruments include, among others, ICES' *Information Asset Management Program*; ICES' *Confidentiality and Security of Data Policy*; ICES' *Data Retention Policy*; ICES *Offline Chart Abstraction tool*; *DM001: Receiving project-specific data sets from external sources*; *DM002: Receiving and Processing Administrative Data*; *DM003: Destruction of 3rd Party Health Data*; ICES *Privacy Code*; ICES *Data-sharing agreements*; ICES *Confidentiality Agreement* and ICES' *Confidentiality Agreement for Data Covenantors*; *Access to Health Data Policy*; ICES' *Protecting PHI on Mobile Devices Policy*; ICES *Project-Specific Privacy Impact Assessment form*; and, *Primary Data Collection Project Management Checklist*, among others.

ICES' *Confidentiality and Security of Data Policy* provides that the Director, Information Management and Data Covenantors ensure that records are transferred in the documented secure manner in compliance with *DM001: Receiving project-specific data sets from external sources*; *DM002: Receiving and Processing Administrative Data*; and ICES' *Data-sharing Agreements*. The process for secure transfer includes the requirement for the Director, Information Management and designates to document the following items:

- Date of transfer
- Mode of transfer
- Recipient;
- Written receipts of the records from the third party
- Nature of the records;
- Confirmation of receipt

These policies and SOPs require that the transfer of all PHI be conducted only via the approved secure methods set out below:

- Generally, ICES collects the large administrative databases from various departments of the MOHLTC which are “pushed” or “pulled” remotely through a secure connection or

Part 2 – Security Documentation

virtual private network (some pulled down using a SSHv2 server and Entrust PKI certificates), with approval and direction from the CISO and/or the Director, Information Management (administrative covenantor) and their designates **OR** in encrypted form on CDs. This information is collected onto secured ICES servers, managed by Data Covenantors, and de-identified with health cards encrypted as soon as reasonably possible.

- ICES permits PHI collected in the field in relation to chart abstraction studies to be “pushed” or “pulled” remotely through a secure connection or virtual private network (SSL-VPN), with approval and direction from the Director, Information Management (an administrative covenantor), the CISO and their designates. Generally, this information is collected under a unique study number, with PI stored separately in a cross-walk table or peel-away file. This information is collected onto secured ICES servers where it is de-identified with health cards encrypted as soon as possible by ICES’ Data Covenantors.
- Under DSAs, ICES collects PHI from HICs related to purposes declared in the agreements, using the same processes as outlined above: “pushed” or “pulled” through a secure connection or virtual private network (SSL-VPN) or encrypted CD under the supervision of the Director, Information Management (administrative data covenantor) and designates. SOPs delineating the transfer process are in place. The data is also collected onto secured ICES servers, where it is de-identified with health cards encrypted as soon as possible.
- Paper record transfer as part of a study process is extremely rare. ICES’ preferred approach has been to have documents professionally scanned in secure facilities under data agreements; facility staff sign confidentiality agreements and receive privacy orientation prior to this exercise. ICES Agents supervise the process from end-to-end. Paper records are scanned into a customized database using high-speed scanners. Scanners are “scrubbed” and paper shredded once capture and quality is confirmed and task of acquisition has been completed.
- ICES does not utilize faxing as a transfer mechanism for paper records.

ICES has **mandatory procedures** for each of these methods of transfer, including administrative, technological and physical safeguards that must be employed. These procedures assign responsibility for ensuring the secure transfer to the Director, Information Management, the CISO/Security Lead or their designates and set out the conditions under which such transfers are permitted, defining the nature and content of the required documentation.

As stated in SOPs *DM001: Receiving project-specific data sets from external sources*; and *DM002: Receiving and Processing Administrative Data*, the Agent responsible for transferring PHI is required to document the following elements:

- Date of transfer
- Mode of transfer
- Recipient
- Written receipts of the records from the third party
- Nature of the records
- Confirmation of receipt

8. Policy and Procedures for Secure Disposal of Records of PHI

ICES has focused closely on ensuring that the reconstruction of records of PHI that have been disposed of is not reasonably foreseeable.

To that end, it has developed and operationalized a number of policies and SOPs related to complete destruction of PHI and other confidential documents. These include: ICES' *Data Destruction Policy* (and concomitant *Data Destruction Certificate (Original Medium)/affidavit*); ICES' *Document Shredding Policy*; SOP DM003: *Destruction of 3rd Party Health Data*; SOP: *Offline Chart Abstraction Backup and Cleaning*; *Iron Mountain Shredding Contract Sunnybrook Health Sciences Centre - ICES subcontract*; SOP: *Destroying Hardware(DVDs, CDs, Floppies, USB Keys, Hard Drives)*

ICES believes these policies and SOPs are consistent with the requirements of PHIPA and its regulation, as well as with factsheets, guidelines and orders issued by the IPC, including HO-001, HO-006, Fact Sheet 1, and Section 13 of PHIPA.

The Director, Information Management (or designated covenantors), IT/IS staff, and the Manager, Administration have been designated by ICES to specifically ensure the secure retention of PHI pending their secure disposal.

ICES requires that linked records be securely disposed of in compliance with ICES' *Data Destruction Policy*. ICES requires that PHI records in electronic format be disposed of in the following manner:

“It is the responsibility of the scientist Agent to specify a destruction date for all data brought into a project as part of the project-specific PIA and to ensure that the destruction is carried out by that date. Destruction of data means that there will no longer exist any copy of the data either in its original form or any derived form in paper, electronic, or any other storage medium including back-up tapes or CDs. The only exception will be aggregated forms of the data in published manuscripts and reports. Computer programs that were designed to manipulate the data may be stored indefinitely provided that no vestiges of the data remain within the programs. The ICES project management support system (MSS) has been designed to track all datasets that come into ICES; for individual projects it will capture types of data used and monitor data destruction.”⁹⁹

A *Standard Operating Procedure (SOP DM003)* explicitly outlines the data destruction processes, roles, responsibilities, knowledge management and monitoring requirements for all data brought into ICES through data-sharing agreements and feeds, including original medium, derivative data, backups and project-created datasets. A *Data Destruction Certificate* related to the witnessed destruction of the above is issued by the Director, Information Management.

⁹⁹ ICES *Data Destruction Policy*. p1

Part 2 – Security Documentation

“Destruction of the data means that there will no longer exist any copy of the data either in its original form or any derived form in paper, electronic, or any other storage medium including back-up tapes or CDs... The destruction of data at ICES will occur at two levels, the source level and the project level. Agents of the IS staff will destroy all appropriate tapes with a magnetizing device. The Director, Information Management... will be called upon to ensure or verify that the data have been removed from ICES systems... and that Data Destruction Certificates are issued”¹⁰⁰

ICES requires that information -stored on devices or other hardware should be disposed of in the following manner:

“Destroying DVDs and CDs: To destroy DVDs and CDs, run them through the Data Destroyer twice, serrating both sides of the disk. Break the disks in quarters. Throw the pieces into separate secure bins; Floppies: To destroy floppies, manually remove the shutter, and open the protective outer plastic shell. Take the magnetic disk out and cut into pieces. Throw the pieces into separate secure bins; Hard Drives: Remove screws from hard drive case. Remove platters from the spindle. Destroy platters with compression or fracturing. Dispose of in separate secure bins; Memory Stick/USB Keys: Removable memory keys are physically fractured; chips are removed and securely disposed of. Malfunctioning keys are destroyed, rather than repaired”¹⁰¹

This destruction functions are performed by a designated Agent from the IT Department.

The ICES’ *Document Shredding Policy*, previously presented to the IPC, requires that any paper records containing PHI be disposed of using irreversible shredding procedures.

“1. All confidential information, such as computer printouts and any printed information containing personal identifiers, must be destroyed by irreversible shredding, using one of the two methods available at ICES.

- *Shredding machines: for confidential documents that DO NOT CONTAIN PERSONAL HEALTH INFORMATION. Small irreversible shredding machines are located on each floor throughout ICES.*

2. There are a number of smaller blue barrels marked “Not Confidential” located throughout ICES. These barrels are the property of Sunnybrook Health Sciences Centre (SHSC). The contents of these barrels are collected by Sunnybrook staff from time to time and removed from ICES premises. NO MATERIAL THAT IS REQUIRED TO BE SHREDDED ON-SITE IN A CONFIDENTIAL MANNER SHOULD BE PLACED INTO THESE BINS UNDER ANY CIRCUMSTANCES.”¹⁰² ¹⁰³

¹⁰⁰ ICES Data Destruction Policy. pp1-3

¹⁰¹ ICES SOP: Destroying Hardware. p1

¹⁰² ICES Document Shredding Policy. p1

Destruction by a Third Party Service Provider

The ICES' *Document Shredding Policy* describes shredding provided by a vendor-of-record for the MOHLTC, who acts as ICES' service provider for irreversible shredding. A contract with this vendor has been in place for many years; the contract is extensive and detailed as required by the MOHLTC and relative statutory requirements:

- *Confidential On-site Shredding for printed information CONTAINING PHI:* *ICES has an agreement with a bonded organization that provides special "Confidential" collection bins and performs on-site irreversible shredding of the material placed into these special large, locking, wheeled 65 gallon grey bins marked "Confidential", located throughout the key access protected areas. Material to be destroyed on-site by the third party shredding company **must** be put into these bins. The bins are collected and the contents shredded on site in a mobile shredder unit utilizing irreversible shredding techniques. An Agent is present each time the bins are collected and the contents are destroyed under ICES supervision. Upon completion of each on-site shred, the third party shredding company provides a certificate confirming the date, time and method of destruction and that the destruction process was carried out in a confidential manner by trusted employees. The certificate will also bear the signature of the Agent who witnessed the destruction and the personnel who executed the destruction.*¹⁰⁴

At ICES, all confidential paper records are securely disposed of by Iron Mountain® in accordance with timelines specified in the *Document Shredding Policy*. Iron Mountain® is also responsible for providing a certificate of destruction to the Manager, Administration (or designate, in case of absence), who witnesses the shredding:

- Identifying the records of that were to be securely disposed of;
- Confirming the secure disposal of the records;
- Setting out the date, time and method of secure disposal employed; and
- Bearing the name and signature of the agent of the third party service provider who performed the secure disposal

Records are always destroyed, on-site at ICES and are done in a secure manner, pursuant to the procedure set out in the policy.

The *Data Destruction Policy*, like all ICES policies, requires all Agents to comply with its terms; compliance is enforced by having signed an ICES *Confidentiality Agreement* which is tracked by

¹⁰³ NOTE: *Iron Mountain Shredding Contract Sunnybrook Health Sciences Centre - ICES subcontract. ICES is a tenant of Sunnybrook HSC and services are provided as per IRON Mountain's designation as MOHLTC vendor of record through Sunnybrook HSC. This contract is planned for review F2011/12*

¹⁰⁴ ICES *Document Shredding Policy*. p1-2

the CPO or designated staff in the Privacy Office. It clarifies that breach of the policy may result in discipline, up to and including termination.

9. Policy and Procedures Relating to Passwords

ICES recognizes that a rigorous approach to passwords is essential. ICES' *Password Policy* governs the passwords used for both authentication and access to information systems whether they are owned, leased or operated by ICES. The policy has been developed with regard to and is consistent with orders, fact sheets, guidelines and best practices issued by the IPC and also with regard to current best practices.

Pursuant to the policy, ICES sets the following conditions/restrictions on passwords:

- *“They must be a minimum of 8 characters and a maximum of 14 characters;*
- *They must contain a combination of upper and lower case letters, numbers and non-alphanumeric characters*
- *Passwords cannot be reused (history >5)*
- *Password change is forced on both the LAN and SAN (local area and secure area networks)”*

ICES systems will automatically reject passwords that do not comply with these standards. In addition, Agents are instructed that:

- *“Passwords must be changed frequently. Passwords automatically expire every 60 days (UNIX) and 90 days (LAN); passwords automatically expire after 60 days of password inactivity;*
- *Access is locked after 3 failed attempts to input the correct password;*
- *Password access is required to access the system after 10 minutes of inactivity because a system-wide locked screen-saver is automatically triggered.”*

ICES, also mandates the following administrative, technical and physical safeguards to be implemented by all ICES' Agents:

- *“Passwords must be kept private. Passwords must not be written down, displayed, hinted at, shared or otherwise made known to any other individual, including other Agents. No passwords are to be shared in order to “cover” for someone out of the office. Passwords are not to be shared with supervisors and personal assistants. Passwords are not to be displayed OR concealed in an Agent's workspace.*
- *Passwords cannot be Agent's name, address, DOB, username, nickname, license plate or a term that could be easily guessed by someone familiar with the Agent.*
- *Passwords must be changed immediately if they suspect it has become known to any other individual, including other Agents”¹⁰⁵*

¹⁰⁵ ICES *Password Policy*. p 1-2

The *Password Policy*, like all ICES policies, requires all Agents to comply with its terms as agreed in the ICES’ Confidentiality Agreement, and its compliance is enforced by the CPO/ IT Manager and through software that forces compliance. It clarifies that breach of the policy may result in discipline, up to and including termination.

10. Policy and Procedures for Maintaining and Reviewing System Control and Audit Logs

Authorized and named Data Covenantors de-identify PHI on stand-alone computers as first use after collection. In relation to managing these data, ICES has implemented an *Administrative Data Log*, which is maintained and regularly reviewed by the Director, Information Management and co-covenantors. It tracks the collection and de-identification / anonymization/management/ storage/destruction¹⁰⁶ of the large amounts of highly sensitive data that ICES holds. There is no opportunity for modification of the data or disclosure of PHI because of the careful separation of duties, and use of stand-alone machines with highly restricted access in the highest security area of the Institute. Original media are further secured in a vault; no PHI is available on its servers.

The *Administrative Data Log* ensures that the following information be collected, maintained and reviewed in an ongoing fashion: datasets by name; number of records; owner-covenantor; arrival date; reason for any production delay; date posted; PHI storage location¹⁰⁷; AHI (anonymized health information) location; DHI (de-identified health information) location; back-up location; production location; production personnel; date for destruction; original medium destruction date; and, total destruction date (all sources).¹⁰⁸ Additionally, the Director Information Management performs monthly reviews of access permissions.¹⁰⁹

“The Director Information Management will review the Administrative Data Log, the data holdings page, and the contents of the MOH directory on a monthly basis for completeness, consistency, and accuracy of information. At that time, the Director will also review access permissions to ensure they are properly set. The Director will keep a log of when each review is done.”

Given the criticality of the log records, ICES’ *Administrative Data Log* is a permanent record, backed-up daily to ensure that the logs are immutable and retained until such time as ICES closes.

11. Policy and Procedures for Patch Management

ICES has a *Security Patch Management Policy* implemented by the CISO, Security Team Lead and Technical Manager [IT/IS] which requires the monitoring of the availability of patches by

¹⁰⁶ Note on Secure Retention of Administrative Data at ICES. D DeBoer, Director Information Management. Affirmed November 2010

¹⁰⁷ Note on Secure Retention of Administrative Data at ICES. D DeBoer, Director Information Management. Affirmed November 2010

¹⁰⁸ ICES’ Information Asset Management System.

¹⁰⁹ SOP DM002: Receiving and Processing Administrative Data

Part 2 – Security Documentation

the security team on an ongoing basis. Notification generally comes by email from Microsoft, Cisco, Sun, UNIX, Oracle or on the websites of US-CERT National Cyber Alert System, US-CERT National Vulnerability Database, US-CERT Vulnerability Notes Database, Internet Storm Center, SecurityFocus Vulnerability Database, as examples.

“The Patch Management Procedure must be managed in a transparent manner with regular reviews. A four phased Patch Management Process is required:

- *Assessment and Inventory – accurately record what software components comprise the ICES operational environment, what security threats and vulnerabilities exist;*
- *Patch Identification – identify patches and software updates that are released, determine their criticality level;*
- *Evaluation, Planning, and Testing – develop, and test the implementation of all patches without compromising ICES’ critical systems and applications;*
- *Deployment – successfully roll-out the approved software update into the operational environment with minimum impact on system users.”¹¹⁰*

The Security Team Lead and Technical Manager [IT/IS] or designate is responsible for analyzing the patch and determining if it should be implemented through the consideration of comprehensive and documented criteria:

“The following Patch Priority Matrix represents all systems at ICES, their relative priority for vulnerability patching (high, moderate and low), and timeframes within which patches must be applied (i.e. 2-3 days, 7 days, 14 days, 30 days, 90 days).”

“Patches for non-critical vulnerabilities are deployed after they are tested and approved by application owners and business partners. The time for deployment for each patch will vary based on the complexity of the patch. Where the deployment time exceeds the time stated in the above chart notification will be made to the business owner and to the CISO/Security Lead.

“Critical vulnerabilities will be tested and approved only by the Agents/designated individual(s) from IT System Department, and the application owners and business partners will be only notified. The time for deployment will fall under the timelines indicated in the table above.”¹¹¹

“Vulnerability assessments will be performed routinely based on the Internal Scanning Programs schedule by qualified Agent/individuals. Reports of these assessments will be reviewed and approved by the Manager of IT Systems and these reports will become a primary resource for the individuals or groups responsible with Patch Management Process.”

¹¹⁰ ICES’ Security Patch Management Policy. p1

¹¹¹ Ibid. pp2-3

The following section describes the roles and responsibilities of Agents (individuals or groups) integral to the development, maintenance or execution of this Policy:

- *The Agent/CISO will be notified of the implementation of patches and service packs or changes to hardware operating systems and ratify those changes.*
- *The Agents/staff of IT Systems Department will be responsible for the execution of this Policy, including the implementation of security patches/changes for applications, services and hardware.*
- *Designated individual(s), Agent(s) from IT System Department will maintain appropriate documentation of changes made to each application, system and hardware device.*
- *The Agents of the IT Systems Department will also be responsible for ensuring that consistent, approved, licensed versions of software are maintained/ used on all workstations, servers and other information technology platforms. This will be accomplished through periodic inventories of application, system and hardware versions.¹¹²*

There is also a role for the Agent/Application Developer (internally, or externally [example: HOBIC]), where the developer shall agree that the patches do not break applications or systems.

12. Policy and Procedures Related to Change Management

ICES' Information Asset Management System

ICES, has implemented an *IT Change Management Program*, including a suite of SOPs (*IM001 Initiate – Request for Change; IM002 Approve – Request for Change; IM003 Implement – Request for Change; IM004 Evaluate – Request for Change; and the Request for Change Form v1.1*) which governs approval or denial of a request for a change to the operational environment at ICES¹¹³:

“The change management process encompasses any and all alterations to any and all IT based assets on which ICES depends. Assets subject to change management include:

- *Hardware (servers, workstations, routers, switches, mobile devices, etc)*
- *Software (operating systems, applications (built & bought)*
- *Information, data, and data structures (files and databases)*
- *Security controls (anti-virus software, firewalls, intrusion protection/detection systems, access, etc).”¹¹⁴*

“The Change Management Process is to ensure standardized methods, processes and procedures are used for all changes, facilitate efficient and prompt handling of all changes, and maintain the proper balance between the need for change and the potential detrimental impact of changes”.

¹¹² ICES' Security Patch Management policy. pp2-3

¹¹³ NOTE: ICES' Information Asset Management System

¹¹⁴ ICES' IT Change Management Program. pp 2-5

Part 2 – Security Documentation

For purposes of the *IT Change Management Program*, “change” is defined as:

“any production installation, alteration, or modification of hardware, system software, applications, documentation, network or environmental facilities related to the delivery of existing service(s) and/or new requests for service.”

In the document, the CISO (assisted by the IT Lead and the Security Lead) are designated as responsible for the Program, and responsibilities include: prioritizing investment in tools and resources; resolving escalation issues; and, communicating new and changed policies.

Definitions related to *Change Management Program’s* description below include:

Program Owner

The Director, Information Management will function as the program owner who sponsors the change management process, and has the responsibility and authority for the overall process results.

The Program Owner’s responsibilities include:

- Prioritizing investment in tools and resources
- Resolving escalation issues
- Communicating new and changed policies

Change Coordinator

The Manager of IT will function as the Change Coordinator. The Change Coordinator ensures that the process properly supports ICES IT operations, and the process works and meets the business’ needs. The Change Coordinator coordinates day to day activities and manages individual items or work within change management. The change coordinator has the additional responsibility to aid the Requestor for any large or complex change.

The Change Coordinator’s responsibilities include:

- Coordinating the process across all sites
- Ensuring that standards, policies, and procedures are followed
- Identifying the need for major improvements to the change management process including process enhancements and automation
- Chairing a weekly change review meeting with Change Advisory Board (CAB) and Change Owner(s)
- Receiving and reviewing all change requests for completeness and accuracy
- Producing a report of all submitted change requests to be circulated to the CAB in advance of the review meeting
- Resolving change scheduling conflicts through meetings with affected parties or escalation to management, as required
- Conducting post mortem reviews for all failed changes
- Maintains quality assurance for the change management process execution
- Preparing and analyzing all change management reports
- Ensuring currency of change data

Part 2 – Security Documentation

- Reviewing problems caused by changes
- Ensuring proper change categorization
- Verifying implemented changes before closing change records
- Producing regular and accurate management reports.

The Change Coordinator has the authority to update change records. In addition, the Change Coordinator will provide metrics for the purpose of improving the change management process.

Change Requestor

The Change Requestor is anyone who has a business requirement to request a change. This person will usually be a member of IT (ICES Agent), but could be any member of the ICES community or even an external person.

The change requestor's responsibilities include:

- Ensuring compliance with the change process, methods, and procedures when creating a request for change (RFC)
- Ensuring the submitted RFC has received proper departmental/client approval
- Submitting the completed RFC to the Change Coordinator
- Attending weekly change review meeting to answer any questions by CAB, if Change Owner is unable to attend meeting
- Completing all required change request documentation
- Providing required back-out plans for each of the implementation steps, where applicable
- Notifying the change coordinator to close change request based on customer verification of implemented change(s)

Change Owner

The Change Owner is responsible for the outcome of the change and must be an ICES IT Agent. Each Functional Area of Change will have a Change Owner to cover all change within that area.

The Change Owner has the responsibility for:

- Technical planning of the change
- Attend weekly change review meeting to answer any questions by Change Advisory Board
- Overseeing the implementation and the verification of success when finished
- Provides proof of testing and/or test results when requested for all scheduled changes and pre-authorized changes
- Evaluating and communicating the outcome of the change and validation

The Change Requestor and Change Owner can be the same person, different members of IT, or from different groups within ICES.

Change Advisory Board

The Change Advisory Board (CAB) is made up of Agent representatives of groups or areas directly involved or significantly impacted by the change. The Agents/members are responsible for approving or rejecting change requests based on risk assessment, past

experience, and knowledge. Approval is not based on the business case for change which has already been made. Each Functional Area of Change will have a CAB representative.

Change Implementer

The Change Implementer (usually an IT member) is responsible for executing the change activity. The responsibilities of a change implementer include:

- Ensuring compliance with the change process, methods, and procedures when implementing changes
- Executing the change back-out procedures in case of a failure during the implementation process
- Following the time guidelines to back-out changes per the procedures supplied by the requestor

Thus, the Director, Information Management is responsible for receiving and reviewing such requests and for determining whether to approve or deny them, following a detailed, documented process for arriving at a determination to approve or deny a request for a change. The Technical Manager [IT/IS] (or designate) will function as the Change Coordinator.

The documentation consists of a multipart *Request for Change* (RFC) Form and four accompanying SOPs. Requests for change can come from Agents at all ICES sites and areas. The RFC form must be completed, and contains the following information:

- *Clearly defined reason for the change, and the area it will impact*
- *Clearly identified resources required, and the change activities to be undertaken.*
- *Clear identification of the Agents who will validate the change*
- *Clearly defined implementation impact (how implemented) of the change to the ‘live’ environment*
- *Clear definition of how the change will be verified as successful, and the back out plan*
- *Clear definition of the amount of time required for the implementation of the change, including a possible back out in case of change failure*
- *Clear definition of any cost factors of the implementation plan. i.e. Assess the impact, cost, and benefits associated*
- *Clearly defined risks and impacts of the request for change, including regulatory impacts*
- *Clearly defined scheduled time for the change*
- *Identification of all affected parties (i.e. internal and external)¹¹⁵*

The final decision to approve or deny the request for a change is made by the Agents of the Change Advisory Board and will be documented in the Request for Change (RFC) Form, Section D and communicated.

¹¹⁵ ICES’ IT Change Management Program. p8

Part 2 – Security Documentation

“A change must not be implemented without full authorization from the proper departmental/client approval and by the appropriate CAB. The departmental/client approval of the RFC is communicated to the Change Owner via the Change Requestor.”

“The Change Owner will make an assessment by reviewing the Risk/Benefit assessment of the implementation versus the business reason. The Change Owner and Change Coordinator will confer on the assessment and decide if the RFC should go forward for approvals.”

Where a request for a change to the operational environment is denied, the Change Owner documents:

- The change requested;
- The name of the Agent requesting the change;
- The date of the request; and
- The rationale for denying the request.

Where a request for a change to the operational environment is approved, the Change Implementer(s) identified in the ICES’ *IT Change Management Program* is responsible for determining the timeframe for implementation and the priority assigned to the change, based on the information provided in the RFC, the Change Implementation Process, and makes the assessment using the following criteria:

- *Is the activity to be done by their group clearly documented?*
- *Are all the resources available for the time scheduled by the RFC?*
- *Is there any information known by the implementer that will affect the current outcome of the request?*
- *Resolves any same system change timing issues (pre-requisite, co-requisite, and conflicts)*

The Change Owner oversees the implementation and verification. The Change Implementer(s) communicate the outcome of their activity(s) to the Change Owner.

The Change Owner communicates the outcome of completing section D of the RFC. In the RFC record, the Change Owner must record:

- If testing was done prior to implementation;
- If there were any unexpected problems encountered;
- If the back-out plan was used;
- If the documentation was updated;
- Who validated the RFC

“Detailed change deviation information with approval can be sent to the Change Coordinator for RFC record update. It is the Change Owner’s responsibility to communicate with the Change Coordinator for the closure of the RFC activity records.”

“The Change Owner is also responsible to notify to all relevant parties the outcome of the RFC and to follow up with any cancelled, partial or failed attempts and with the outcome of the validation (if not successful). The Change Owner and Change Coordinator may conduct a post implementation review. This stage is especially important if a problem was encountered. Input from any of the other affected parties may be gathered.”

The IT Lead is responsible for the maintenance of the record of changes implemented. It includes the following data fields:

- A description of the change;
- The name of the Agent who requested the change;
- The date the change was implemented;
- The Agent responsible for implementing the change;
- The date, if any, the change was tested;
- The Agent who tested the change, if any; and
- Whether the testing was successful

13. Policy and Procedures for Back-Up and Recovery of Records of De-identified Information and PHI

ICES has policy instruments, mainly SOPs and tools, related to the back-up and recovery of all data, including PHI. These identify the nature of ICES’ s back-up devices and requires that back-ups be performed daily.

However, there are different methodologies in place for back-up, archiving and restoring information.

De-identified data on ICES’ UNIX systems are backed-up daily. A schedule of daily scheduling of backup responsibilities for Agents of the IT/IS department is included in the ICES’ *Project Server Backup, Archival and Restore SOP*. These Agents also perform weekly verifications of tapes on a rotational basis to ensure consistent recovery capability. The IT Lead (or designate) is responsible overall for the processes of back-up and recovery.

The ICES’ *Project Server Backup, Archival and Restore SOP* outlines the process for back-up and recovery.

PHI is treated differently from de-identified data. It can only be ‘handled’ by Data Covenantors. It is the responsibility of the Director, Information Management (a covenantor) to back-up PHI on two storage devices and secure the device in ICES’ vault. The SOPS for back-up, archiving and retrieval for the types of PHI collected by ICES are discussed in two IS/IT SOPS: *DM001: Receiving project-specific data sets from external sources; and DM002: Receiving and Processing Administrative Data*. Refer to Section 10 of part 2 for related information.

ICES recognizes that the security of the back-up storage devices is just as critical as the security of the active storage devices and consequently ensures via these SOPS that such back-up storage devices are logged and stored in the highest security area in the vault.

“The Data Covenantor will log the arrival date and storage location of the dataset in the Data Agreement... and... will write the arrival date, agreement number, project number on the disk and have it stored in the data safe. The original disk will be stored in the data safe, until the Data Covenantor performs a back up of the data onto BestCrypt™ containers in 2 identical external hard drives.”¹¹⁶

The Director, Information Management is responsible to ensure that they are retained in accordance with ICES’ *Confidentiality and Security of Data Policy*, previously discussed.¹¹⁷ In addition, ICES’ Director, Information Management or a designated covenantor maintains a detailed inventory of all backed-up records stored in the vault.

ICES recognizes the need for availability of backed-up records of PHI and de-identified information within a reasonable time-frame for operational purposes and further recognizes such backed-up records may sometimes be required by law.

ICES has previously described in this report (see part 2, section 5) that de-identified information and PHI on back-up devices stored in the highly secured vault are retained indefinitely, as per its Agreement with the MOHLTC.

“ICES has had (dating back to 1995) and has currently a DSA with the MOHLTC which allows for regular feeds of PHI retained in administrative databases from numerous areas of the MOHLTC on an ongoing basis. These data support the vast majority of ICES projects carried out to fulfill its section 45 mandate. Due to the retrospective/prospective nature of most ICES projects and the ongoing demand by ICES projects for these data, they are retained until such time as the data sharing agreement is declared void by either party. ICES will then be obligated to destroy all of the data.”¹¹⁸

14. Policy and Procedures on the Acceptable Use of Technology

A key underpinning of ICES’s privacy and security program(s) is ICES’ *Appropriate Use of Computer Equipment Policy*. It outlines for all Agents the acceptable use of information systems, technologies, equipment, resources, applications and programs, whether they are owned, leased or operated by ICES, and their required compliance. It sets out permitted uses, prohibited uses and the uses for which prior approval is required.

¹¹⁶ ICES’ *DM002: Receiving and Processing Administrative Data*. p4

¹¹⁷ See also ICES’ *Note on Secure Retention of Administrative Data at ICES*

¹¹⁸ *Note on Secure Retention of Administrative Data at ICES*. D DeBoer, Director Information Management. Affirmed November 2010

Part 2 – Security Documentation

“All computer usage must be reasonable and acceptable, and able to pass public scrutiny and disclosure. All network usage by employees is subject to monitoring. All ICES Agents need to be aware that the Internet is a public network... neither the files accessed nor the hardware and software used are the personal property of the employee although they are made available for individual use.”

“Agents must not access inappropriate internet resources such as websites containing offensive material which is illegal or which does not comply with the Ontario Human Rights Code.”

“The unauthorized installation, use, storage or distribution of copyrighted software or materials on institute computers is prohibited. All software on ICES computer systems must be approved by the ICES IT department and/or the CISO/CPO.”¹¹⁹

Occasionally projects require software (usually statistical or related to project management) which is not part of ICES’ usual suite of programs on institute computers. Agents/scientists/project managers may make requests for the addition of software using the *Request for Change* processes previously described in Part 2, section 12).

“ICES’ CISO/CPO/ Security Lead and/or Technical Manager [IT/IS] are responsible for receiving, reviewing and approving or denying requests for use that require approval[based on expertise] [sic] in accordance with the process defined in the Appropriate Use of Computer Equipment Policy and the Request for Change Process.”^{120, 121}

The final decision to approve or deny the request for a change related to project-specific requirements will be communicated to ICES’ scientists and staff via corporate email and/or personal discussion with ICES’ IT/IS Management, the Director Information Management and the CISO/CPO.

“All use of ICES’ systems must be in support of projects and research and be consistent with the mission of the institute. ICES, reserves the right to prioritize use and access to the system. Any use of ICES’ systems must conform to Provincial and Federal law, network provider policies, accepted software licenses and ICES policy.”¹²²

Agents who are granted approval for a use outside of the listed permitted uses are restricted to:

- The use only for the purposes specified in the request documentation
- The use only for the limited time specified in the request documentation, if any

¹¹⁹ ICES’ *Appropriate Use of Computer Equipment Policy*. pp1-2

¹²⁰ Ibid p2

¹²¹ ICES’ *IT Change Management Program*

¹²² ICES’ *Appropriate Use of Computer Equipment Policy*. p2

The *Appropriate Use of Computer Equipment Policy*, like all ICES policies, requires all agents to comply with its terms and its compliance is enforced by the ICES' Confidentiality Agreement. It clarifies that breach of the policy may result in discipline, up to and including termination.

15. Policy and Procedures in Respect of Security Audits

Security Audits are a key component of ICES's overall security program. The goal of ICES' audit processes is always to ensure compliance with its policies. ICES has developed and implemented the *Privacy and Security Audits Policy* and associated policy instruments that set out the types of security audits that are required at ICES. These include:

- Threat and Risk Assessments
- Security Reviews or Assessments
- Vulnerability Assessments
- Penetration Testing
- Physical Security Audits
- Ethical Hacks
- Log review audits
- Policies, procedures and practices compliance exercises

ICES, has implemented a Security Audit Schedule, led by the CISO/Security Lead with input from the CPO. The policy includes the frequency of each audit and the circumstances under which an audit is to be conducted.

“ICES will conduct annual audits to assess compliance with privacy and security policies, procedures, standards, guidelines and practices implemented by the Institute.”¹²³

In addition, every time a Request for Proposals (RFP) is promulgated for independent third party reviewer/vendor(s), a clear Statement of Work (SOW) is drafted with the assistance of ICES' Procurement Office, including the purpose of each audit, its nature and scope, and the responsible Agents/employee(s). The RFP and SOW details the process for conducting the audit, including criteria for selecting the subject matter, when and if notification occurs, the content and recipient of the notification, and all documentation required at the outset and conclusion of the audit and to whom it must be provided. The CISO/Security Lead and their designates provide oversight and consultation.

“...security-specific testing, including penetration testing and threat-risk assessment, as conducted under the authority of the CISO and Security Lead...will be done annually...automated LAN-based PC-specific audits with manual validation by the CPO will be conducted as resources permit by the CPO (at a minimum, tri-annually); additionally, Agents will be provided with

¹²³ ICES *Privacy and Security Audits Policy*. p1

Part 2 – Security Documentation

algorithms to self-audit to facilitate “maintenance” and good project management on the background of ICES policies and SOPs.”

In order to close the loop on risk management, ICES’ policy contains a process for managing the recommendations arising from a security audit. The CISO/Security Lead is responsible for reviewing the recommendations, setting timelines for mitigation and change, and monitoring to ensure implementation. The CISO/Security Lead and CPO maintain spreadsheet logs of findings and recommendations and the “hard points” related to execution as mentioned above.

ICES’ *Privacy and Security Audits Policy* includes a communication strategy that requires:

“Recommendations arising from audit reports are carefully reviewed by the CPO, CISO and Security Lead and are shared with Directors as needed. The CISO/Security Lead and CPO, individually and/or collaboratively depending on the audit process, are responsible for the associated responses to recommendations and change management logging required. They are responsible for reporting findings and recommendations to the President & CEO and Deputy CEO in a timely fashion.”

“Working with the content area Agents/Directors and/or Communications staff, a plan for remediation, heightened instruction or policy change is planned and executed. Much of the communication strategy includes Agents/CISO /CPO-led discussion at staff meetings, keyed email messaging across the organization and topic management in ICES Privacy/Security newsletter.”

“All material related to audits is retained by the Agents/CISO and CPO and logged.”¹²⁴

ICES’ policy requires that the Agents/CISO/Security Lead are responsible for maintaining a log of security audits and for tracking that recommendations are implemented within the identified timeframe. All material relating to the audit will be retained in the shared privacy/security directory.

Pursuant to ICES’ policy, auditors are instructed to notify ICES, at the first reasonable opportunity, of a privacy or security breach or suspected breach in accordance with ICES policy.

ICES has a routine pattern of the CISO and Security Lead reporting the findings of audits to the Senior Security Analyst at the IPC as they are executed and completed. The logs contain the following elements and may be inspected on-site by the IPC¹²⁵ as desired:

- The nature and type of audit conducted
- The date the audit was completed
- The Agents and vendor(s) responsible for completing the audit

¹²⁴ ICES *Privacy and Security Audits Policy*, p2

¹²⁵ ICES’ *Information Asset Management System*

Part 2 – Security Documentation

- The findings/ recommendations of the audit
- Impact of Finding
- Likelihood of Finding
- Risk Score
- Finding Remediated Y/N
- The Agents or vendor responsible for addressing each recommendation
- The date and manner in which each recommendation was or is expected to be addressed.¹²⁶

ICES has implemented *The Security Quality Assurance (SQA) program*¹²⁷, an ISO 27001 based assurance program composed of 10 modular assessment components. Each of these components addresses areas of compliance for information security such as technical scanning, legislative compliance, Business Continuity Planning/Disaster Recovery, etc. The SQA is a cost- effective means to assess projects for the right criteria and in the right timeframe. The assessment components are selected based on the appropriateness for the project at hand rather than arbitrarily as is found in other assessment methodologies.

The fundamental principle of the SQA program is to engage all team members in proactive monitoring of systems to prevent or reduce downtime, automation of tasks to reduce errors and detailed logging of events and tasks to ensure commitments are met. This is all done following a detailed set of industry best practices tools based on IT Infrastructure Library (ITIL) methodologies.

The SQA establishes a baseline for ongoing compliance, and as it is repeatable and measureable will ensure ongoing compliance.

To be effective, SQA has been designed with the following principles in mind:

1. Minimum impact on project development and deployment;
2. Provide appropriate levels of confidentiality, integrity, and availability; and
3. Protect ICES and its stakeholders' assets commensurate with the level of risk and magnitude of harm resulting from loss, misuse, unauthorized access, or modification.

ICES plans audits measuring against ISO standards; SQA helps articulate ICES' interest in best practices. See Part 4 of the Report for more related information.

16. Log of Security Audits

ICES' CISO/ Security Lead and CPO maintain an overall log of security and privacy audits that have been completed. Additionally, the CISO maintains a *fiscal-year specific* log which tracks findings from the reports and action items/execution/completion related to:

- Testing at all ICES' expansion sites (ICES@Queen's, ICES@uOttawa);
- Testing of all s.45 clinical registries (ICD, PDReg/DMAR, RCSN);

¹²⁶ ICES Security Audits Findings Final Report March 2010

¹²⁷ http://inside.ices.on.ca/webbuild/site/icesintranet/webpage.cfm?site_id=2&org_id=94&morg_id=0&gsec_id=5007&item_id=5197

Part 2 – Security Documentation

- Audit findings related to *ICES Policy Table, ICES Network Table* and *ICES Device Table*.

The most current security review was conducted across the ICES sites between January and March 2011. The review findings and recommendations have been presented to the IPC Senior Security Analyst by ICES’ CISO and Security Lead. We include the newly-automated internal LAN audit findings for which the validation was performed in July/August 2011 as well.

Since the last review by the IPC (2008), the following Recommendations have been made for F2009/10 and F2010/11:

YEAR		Risk/Severity of Finding				Purpose of the assessment	Conclusions / Recommendations from the final report	Corrections / Mitigation Plans
		Low	Medium	High	Critical			
Fiscal 2009/10								
ICES Central	External network testing	10	1	1	0	The external network testing was intended to assess the potential dangers to the ICES network from an external attacker.	The external network proved to be adequately protected from external attackers. While a number of vulnerabilities were identified, they were not serious enough to provide an attacker with easy access to the ICES network. The firewalls are well deployed and are correctly blocking access to the non public portion of the ICES network. The vulnerability scanning and patching program appears to be working correctly and the systems do not have any known critical security vulnerabilities exposed.	The High, Medium findings were fixed immediately after the report was issued.
ICES Central	Segmented network testing ("UNIX network")	n/a	n/a	n/a	n/a	To review the current security controls in place and make recommendations in areas that can be improved, intended to improve the security processes as well as identify any shortcomings in the security program.	The segmented UNIX network has several characteristics that are vital to its security. For instance, it is not attached to the main ICES LAN nor is it on the Internet. Additionally, the users are all trusted ICES Agents who cannot easily add or remove files from the network. In order to enhance the security of the network, it was strongly suggested to: (1) Enhance segregated network security. (2) Harden and patch the segregated network further.	The system was hardened and patched as recommended

Part 2 – Security Documentation

ICES Central	Social Engineering	n/a	n/a	n/a	n/a	The Phishing exercise was intended to test the awareness of the ICES Agents. An additional benefit of the testing is reminding Agents to question "out of the ordinary" emails they receive and to be very cautious about revealing their passwords.	Many users phoned or emailed the IT Agents and the Helpdesk asking if the email was legitimate. These are positive signs and show a positive awareness amongst many of the ICES Agents, 80% of whom resisted the simulated attack.	Remedial training provided at a staff meeting and listserve email. Multiple personal conversations with Agents.
ICES Central	Devices Review	10	3	0	0	A sample of the firewalls used by ICES was selected for a review. This review examined the configuration of these devices to uncover any security weaknesses. These devices were firewalls used in various roles through ICES infrastructure. The examination of the devices was primarily focused on the firewall rules and VPN configuration.	The firewalls and devices reviewed are providing reliable protection to the ICES networks. Each of the firewalls rule sets have a default deny policy and then allow specific connections based on business requirements. This shows that the firewall administrators are following best practices for managing the firewalls. The findings are mostly changes that can help harden the rule sets.	All obsolete rules identified during the assessment, that are no longer required, were removed from the firewalls' configuration.
ICES Central	Web Applications	13	13	5	1	The objectives for this assessment are aligned with ICES's security objectives: (1) Determine the overall security posture of the DMAR/HOBIC/ICD/ARM/RC SN applications; (2) Provide insight into the degree to which the recent changes in internal security assessment methodologies have increased the overall security posture at ICES (3) Leverage the assessments done by ICES' Agents over the year to reduce the level of effort required to conduct the audits requested by the RFP	In general, the findings were from access control , horizontal (accessing other user data within the same role) and vertical (gaining the privileges of a different role) privilege escalation categories of vulnerabilities.	Only 4 findings from Low category were deferred or partially tested during a re-testing session run by the external auditors.

Part 2 – Security Documentation

YEAR		Risk/Severity of Finding				Purpose of the assessment	Conclusions/ Recommendations from the final report	Corrections/Mitigation Plans
Fiscal 2010/11		Low	Medium	High	Critical			
ICES Central	External network vulnerability assessment	3	2	3	0	The objective was to identify vulnerabilities in the targets that might facilitate compromise of the external network, of the testing subjects themselves, or of the confidentiality of data processed, transmitted, or stored within the target hosts.	The external network proved to be adequately protected from external attackers. While a number of vulnerabilities were identified, they were not serious enough to provide an attacker with easy access to the ICES network. The firewalls are well deployed and are blocking access to the non-public portion of the ICES network correctly. The vulnerability scanning and patching program appears to be working correctly, and the systems do not have any known critical security vulnerabilities exposed.	One High finding was remediated already. Six out of the remaining seven findings, including the High rated vulnerabilities, refer to old versions of PHP and patch required by a <u>legacy</u> application. A review to identify the business needs for this application is scheduled and a remediation plan will be formulated when completed, not later than the end of August.
ICES Central	Internal network vulnerability assessment	6	9	8	3	The internal network testing was intended to assess the potential dangers to the ICES network from a strategically-placed internal threat agent. The internal vulnerability assessment stage consisted of onsite testing at ICES Central against 42 target hosts identified by ICES. The objective was to identify vulnerabilities in the targets that might facilitate compromise of the internal network, of the testing subjects themselves, or of the confidentiality of data processed, transmitted, or stored within the target hosts.	The vulnerability assessment of the internal network revealed that a patching gap exists. The Critical findings are: (1) one system running Windows 2000, no longer supported by Microsoft; (2) same system containing the Symantec Alert Management System 2 (AMS2), which is affected by multiple high-risk vulnerabilities; (3) a number of Windows-based hosts were missing critical security patches from Microsoft. The High rated vulnerabilities identified are also related with missing patches, or old versions for Adobe, PHP, Apache, Java installed on a number of hosts	An Enterprise Patch Management System will be installed this fall and effective quarterly patching cycles will be implemented to cover all systems and hosts from ICES Central network. It is scheduled that all systems will be fully patched by the end of December 2011. The next yearly Audit will validate the implementation of the Patch Management System.
ICES Central	Segmented network testing ("UNIX network")	2	1	0	2	To review the operating system configuration of a sampling of Solaris systems within the environment in order to evaluate the security posture of the UNIX environment, identify potential deficiencies in the security posture, and recommend remediation measures where applicable.	A number of configuration issues were identified on the Solaris systems. For an attacker to successfully exploit any of the identified configuration issues they would have to first gain access to the restricted network segment, which acts as a mitigating control.	The Technology Manager and the System Administrator did evaluate the current issues and it was decided and approved by the upper management to initiate a project for an entire review for ICES Segregated Network re-architecture and upgrade. This new project will be launched by the end of this fiscal year.

Part 2 – Security Documentation

ICES Central	Social Engineering	n/a	n/a	n/a	n/a	The phishing exercise was intended to test the security awareness of the ICES staff. An additional benefit of the testing is that it keeps staff mindful of suspicious emails that they receive and helps to foster a culture of security awareness.	The response from staff, both out-of-band and in-band indicated that generally, the security awareness training at ICES has fostered an understanding of what constitutes suspicious email activity. Many users engaged the security group either to report the incident or to enquire as to its purpose. Only one (1) system out of 245 were compromised during this exercise.	Remediation provided through a CISO listserve email, a staff meeting presentation, the ICES Privacy/Security Newsletter and personal discussions with concerned staff. The security awareness training will continue throughout the year.
ICES Central	Sharepoint configuration review	1	1	2	0	The SharePoint configuration review was intended to assess the potential weaknesses within the SharePoint environment that may be present as a result of insecure configuration. Security Compass also executed a cursory review of the runtime SharePoint environment to map configuration weaknesses to exploitable vulnerabilities.	Sharepoint Server was found not updated with the latest security fixes and service packs.	There is a project scheduled to assess the requirements for a CMS system and to identify if Sharepoint can fulfill this role. If yes, it will be upgraded to the latest version, and at that time all current findings will be addressed; if no, it will be replaced by a different system, more suitable to the business needs if ICES.
ICES Central	Devices Review	1	2	0	0	As part of their ongoing process of hardening their network, ICES wanted a third party to assess a sample of their network device configurations. These devices were firewalls used in various roles throughout ICES infrastructure. The examination of the devices was primarily focused on the firewall rules and VPN configuration.	The firewalls reviewed are providing reliable protection to the ICES networks. Each of the firewall rule sets has a default deny policy, and then allows specific connections based on business requirements. This shows that the firewall administrators are following best practices for managing the firewalls. The findings are mostly changes that can help harden the rule sets. The review did uncover obsolete rules that are no longer required.	All obsolete rules are to be eliminated from the firewalls' configurations.
ICES Central	Applications	4	8	8	1	The objectives for this assessment are aligned with ICES's security objectives: (1) Determine the overall security posture of the HOBIC/DMAR/RCSN/OCA1.3/OCA2.1 web/laptop applications and web services; (2) Identify particularly high-risk issues for immediate action; (3) Provide a list of key findings and recommendations for remediation	The Web App vulnerabilities are: primarily XSS, one missing logout function, 1 patch lacking (was Development site only).	Fixes prepared by the developers for all Critical and High findings were retested and validated by the external auditors during the Audit. Some of the issues identified in OCA 1.3 will not be addressed since this version has been retired already. The newest version of it, V2.1, is being finalized and included in the scope of this year's audit. The developer will focus on addressing the issues raised for <u>this version (the report was submitted first week of July 2011). A remediation plan will be prepared by the end of July 2011.</u>

Part 2 – Security Documentation

Internal network vulnerability assessment	4	6	0	0	The internal network testing was intended to assess the potential dangers to the ICES network from a strategically placed internal threat agent. The internal network testing was non-invasive.	The internal network proved to be adequately protected from internal attackers. While several minor vulnerabilities were identified, they were not serious enough to provide an attacker with easy access to the ICES network. The layer 2 controls as well as the firewalling behaviours that were observed serve to further increase the security posture of the internal network.	Corrections and mitigation plans are in place for all findings and their implementation is scheduled to end by mid-August.
Physical Security					Assess the integrity of all systems in place (access systems, camera systems, key systems, alarm systems) are functional and settings appropriate across the ICES network. After initial testing prior to 'go-live', performed site by site.	The most significant threats to the system are unauthorized data access/ physical theft and malicious employee or contractor. Increase security on reception room. All storage cabinets in the reception area should be locked at all times. Access to the building should only be permitted while a receptionist is on duty; Access to visitors should not be permitted after 5 pm. Visitors' contact should be held accountable for unreturned passes. Recommend clean desk policy.	The risk to the system is very low. There are no significant risks to this environment.
Internal LAN Audit	Automated internal LAN Audit				The automated internal audit revealed 13 accounts out of 150 which required review by IT Agents and the CPO	The audit usually reveals files with suspicious names which actually turn out to be benign	Review by IT Agents/CPO to validate/invalidate findings; completed August 2011. No files were found with PHI; naming conventions were the problem.

17. Policy and Procedures for Information Security Breach Management

ICES, has a blended approach to privacy, security and policy breaches. As discussed previously, ICES security and privacy Agents work very collaboratively, maximizing available resources. ICES *Information Breach* policy, and its *Information Breach Report* form focus on compromise of information from the privacy and security perspective.

First, ICES has an *Incident Management Policy* which provides for action and response related to “computer incidents” as part of first-line monitoring of machine function/malfunction. It outlines a process which facilitates ‘technological sorting’ of minor problems from potential breaches.

“Agents need to be vigilant for ‘unusual system behaviour’, which may indicate a security incident in progress. Users are responsible for reporting incidents (e.g., virus infection, a system compromise or denial of service incident detected by resident software on the user’s workstation to the ICES Helpdesk... The Computer Incident Response Leader is responsible for driving the incident

Part 2 – Security Documentation

process to completion, including Qualification of the incident, Containment, Eradication, Recovery and Reporting... [sic] following an investigative and documentation process. The Leader is to review details, determine the type of incident and update the Helpdesk ticket with the appropriate severity level within 15 minutes... if the Leader has not responded with 15 minutes, a page to the secondary on-call is required... within 15 more minutes, there is not response, an escalation to the ICES CISO/Security Lead or CPO is required.”¹²⁸

Most of these types of incidents are benign, but this process ensures that potential security misadventure is investigated at the earliest possible time to prevent unauthorized access or breach. Investigation leading to suspicion of breach moves immediately to operationalization of ICES’ *Information Breach Policy* and *Information Breach Report*.¹²⁹

ICES’ *Information Breach Policy* and *Information Breach Report* form have been revised as suggested in ICES’ 2008 IPC review; changes are found in Appendix THREE (Recommendations) of this document. The *Information Breach Policy* and its companion *Information Breach Report* Form are employed to address the identification, reporting, containment, notification, investigation and remediation of information security breaches. Additionally, ICES maintains a spreadsheet log of suspected and actual breaches.

The policy defines a privacy and/or information security breach as a contravention of ICES’ privacy and security policies, procedures or practices, and/or PHIPA requirements, as below:

“Because of the potential intertwining of these three components, all must be considered, investigated and reviewed whenever there is a breach concern.”

“A privacy breach occurs when personal health information (PHI) is collected, retained, used or disclosed in ways that are not in accordance with PHIPA and its regulation, ICES policy instruments or with ICES’ Data Sharing Agreements, Research Agreements, Confidentiality Agreements and Agreements with Third Party Service Providers or where PHI is stolen, lost or subject to unauthorized copying, modification or disposal. These policies are referenced in the ICES Privacy Handbook and can be found on ICES intranet site.

Importantly, security breaches are potentially part of, or, can lead to, the breach of PHI or de-identified HI. A Security Breach occurs when a person or entity gains access, either physically or electronically to an ICES domain (either physical space or electronic network) without authorization whether with malicious intent or no, and includes contravention of security policies;

A policy breach occurs when an ICES policy, practice, standard operating procedure (SOP) or other procedure, tool, guideline or standard is not followed. This type of

¹²⁸ ICES’ *Incident Management Policy*. pp1-2

¹²⁹ ICES’ *Information Breach Policy*

Part 2 – Security Documentation

breach may not result in unauthorized disclosure of PHI or de-identified HI, but must always be followed up for purposes of remediation or education of staff.”

ICES’ policy makes it mandatory to report all potential privacy and/or security breaches – PHI, HI – or policy breaches. Moreover, the policy and its companion *Information Breach Report* form have been designed to make it easy for ICES’ Agents to do so. The policy clearly articulates the chronological steps and provides a series of flowcharts to demonstrate the movement through the entire process - from discovery to notification - hierarchy external to ICES.

“When a breach is discovered, a cadence of notification must be initiated. The Agent discovering or suspecting a breach begins the process by informing his/her immediate supervisor or the CPO of the finding or suspicion immediately and initiating containment of the breach as quickly as possible. Although all breaches are important by their very nature, of particular importance is the assessment of inadvertent public disclosure (outside ICES physical structure) of PHI.”

“The notification process will be expanded by these Agents— CPO to the CEO/Deputy CEO and CISO of ICES— and, as the situation requires, up to and including the IPC. A notification chart is part of the breach reporting document to enable documentation of escalation of notification. Notification should be done in person or by telephone, with email only when the first two modalities do not result in contact and notification.

(a) In the case of a breach of PHI related to information collected under ICES’ data-sharing agreement with the MOHLTC, immediate notification of the MOHLTC and the IPC is required (see notification chart).

(b) In case of a breach of PHI or HI related to a data-sharing agreement (DSA) with one or various health information custodians (HICs), ICES is required by statute to notify the HIC(s) who provided the PHI of the information breach, in order that the HIC may notify the individuals to whom the PHI relates when required pursuant to subsection 12(2) of the Act. ¹³⁰

Upon being notified of a breach or suspected breach, the CPO/CISO and Security Lead are required to determine if a breach has in fact occurred and, if so, to the extent possible, what kind of breach has happened and if PHI has been breached. The documentation related to the discovery is commenced immediately by the Agents who made the discovery and the CPO, using the *Information Breach Form*. It is used in an ongoing fashion to collect the chain of events, descriptors and circumstances. Containment, documentation and notification are always encouraged concomitantly, though not always possible. The Agents who discovered the breach initiate the Breach Form with baseline information; the CPO/LPO assume responsibility once that is complete, but will usually consult back to these individuals as the investigation develops. The policy also requires that senior management, including the CEO and Deputy CEO be notified.

“The individual who discovers the information breach is responsible for immediate notification. In order of preference, this should be done in person or by telephone.

¹³⁰ ICES’ *Information Breach Policy*. pp1-3

Part 2 – Security Documentation

- *Notify his/her immediate supervisor in person*
- *Notify the ICES CPO, CISO or Security Lead. If none are on site, notify the CEO or Deputy CEO”*

ICES’ *Information Breach Policy* also addresses containment in a comprehensive fashion, ensuring that it is clear that **containment must begin immediately**, where possible. Agents are required to take reasonable steps to ensure that additional privacy and/or information security breaches cannot occur through the same means. Pursuant to the policy, the CPO and CISO/Security Lead are responsible for reviewing containment measures and ensuring they are effective and sufficient.

“The process of containment is to be initiated by the discoverer of the breach in order to prevent further release of information. As is possible, the containment process is as follows:

- *Determine what if any information has been disclosed;*
- *Retrieve as much of the breached information as possible (ideally all breached information);*
- *Ensure no copies of the PHI or HI have been made or retained by the individual who was not authorized to retrieve or receive the information;*
- *Ensure that further breaches cannot occur through the same means at this time;*
- *Determine whether the privacy breach would allow unauthorized access to any other PHI (e.g. an electronic information system) and take whatever necessary steps are appropriate (e.g. change passwords, identification numbers and/or temporarily shut down a system (or server)).”¹³¹*

The *Information Breach Policy* clearly defines ICES’s notification requirements and cadence of notification, based on the type and extent of breach suspected. The policy requires that the notification include:

- The extent of the breach;
- The nature of the PHI or HI at issue;
- The measures implemented to contain the breach;
- Further actions that will be undertaken, including investigation and remediation.

As per policy, ICES is also required to notify through the CPO or CISO/Security Lead an escalating list of stakeholders, up to and including the IPC, depending on the nature and extent of the breach. The CISO/Security Lead or CPO must notify the data-providing organization from whom the breached PHI was collected at the first reasonable opportunity and whenever required by any agreement with a custodian. These are clearly listed in a notification table contained with the *Information Breach Policy*.

¹³¹ ICES’ *Information Breach Policy*. p5

Part 2 – Security Documentation

Under ICES' *Information Breach Policy*, the CPO and/or CISO/Security Lead are responsible for investigating the breach, in accordance with the process set out in ICES' policy.

“Documentation of breach is initiated as a tool for collecting all appropriate information to aid in the investigation of the event (and as part of ongoing ICES threat risk assessment), as well as to inform future policy and SOP evaluation and change.”

The *Information Breach Report* started will be an invaluable tool in the investigation phase of the privacy or health information security breach. The extent of the investigation is dependent on the type of information breach:

- Most frequently, internal breaches are policy breaches, and PHI is not exposed. Because of the great care taken to de-identify PHI as its first use, and archiving of original media in a highly-secured area in a vault, the opportunities for PHI breach internally are extremely limited. In the case of the internal breach (as defined in the policy), the ICES' CPO, CISO/Security Lead and members of the Privacy & Security Committee will investigate the breach, and provide recommendations to the core Breach Team;
- In the case of either an internal or external breach of PHI (as defined in the policy), ICES, working with the IPC and other appropriate authorities, will conduct an investigation of the information breach.

The objectives of all breach investigations are the following:

- Interview Agents involved with the breach or individuals who can provide information about a process and confirm details captured in the *Information Breach Report*;
- Ensure any issues surrounding containment and notification have been addressed by ICES;
- Discuss the concern with all parties and obtain any relevant evidence (if required);
- Create documentation of the breach and the response to it.

According to the extent and the impact of the information breach, several actions may be taken:

- The need for the extent of notification will be assessed by the Core Breach Team in consultation with the Privacy & Security Committee as required;
- In the case of any breach, review of existing policies and necessary changes to ICES policies and procedures must be made in order to avoid another breach of a similar nature;
- In the case of an internal breach, the Privacy & Security Committee may also recommend action for the core Breach Team to implement;
- An education campaign within ICES will be carried out by the CPO, CISO/Security Lead (and members of the Privacy & Security Committee) in order educate ICES' Agents on how to avoid similar breaches;
- A review of the ICES *Information Breach Policy* will also be done in order to improve the response to a breach and ensure that a clear, concise protocol is in place;

- Finally, should it be determined, the Agent(s) responsible for the breach will be disciplined or terminated according to the terms in the ICES Confidentiality Agreement, in consultation with ICES HR Department and the CEO/ Deputy CEO.

In order to close the loop on remediation and risk management, ICES's policy contains a process for managing the recommendations arising from a security audit, as previously described in this document. Learning from breach incidents is used by the CPO, CISO/Security Lead to develop new or remediate existing policy instruments.

Pursuant to the policy, the CPO or designate is responsible for maintaining a log of all breaches, and is responsible for tracking to ensure that all recommendations arising from the investigation are addressed within the identified timelines. Documentation relating to the breach is required to be kept on the ICES' shared Privacy and Security Directory.

The *Information Breach Policy*, like all ICES policies, requires all Agents to comply with its terms and its compliance is enforced by annual signing of the ICES Confidentiality Agreement. It clarifies that breach of the policy may result in discipline, up to and including termination.

18. Log of Information Security Breaches

ICES, has a blended approach to privacy and security breaches. ICES Agents/CPO and privacy staff maintain a *Log of Suspected/Actual Privacy and/or Information Security Breaches* with the input of security and IT Agents as is needed. The log contains the following elements and can be found on ICES' shared Privacy and Security Directory¹³²:

- The date of the notification or discovery of the breach;
- Description of Suspicion/Privacy/Security/Policy Breach:
- Internal or External to ICES?
- PHI involved?
- Containment Measures (immediate and longer-term) and the nature of the containment measures;
- Notification of HICs;
- Date the investigation commenced;
- Date investigation completed;
- Recommendations arising from the investigation;
- Date each recommendation was or is expected to be addressed and by whom; and
- The manner in which each recommendation was or is expected to be addressed.

¹³² ICES' *Information Asset Management System*

***IMPORTANT ADDITIONAL GENERAL INFORMATION RELATED TO PRIVACY/
SECURITY OF INFORMATION AT ICES:***

ICES' Director, Information Management, has recently implemented an important foundational set of documents entitled the "*Information Asset Management (IAM) Program*". The objective of the Program is to ensure that all ICES information assets are accessed and used appropriately and kept secure from unauthorized individuals. The "*ICES Information Asset Management (IAM) Program*"¹³³ document is the complete statement of the program; all ICES' Agents must be familiar with the contents. The "*Guide to Appropriate Use of ICES Information*"¹³⁴ is a condensed version with all the essential information needed for appropriate handling and use of ICES information.

"Guiding Principles of the IAM documents are:

- *Information at ICES, whether in the form of health data, finance, strategic, operational or other data, research documents or corporate documents are valuable and sensitive assets that must be adequately protected from unauthorized use or exposure;*
- *Access to sensitive information is granted based on role and the need to know the information to execute one's job responsibilities;*
- *Designating ownership for all information assets establishes responsibility and accountability in the management of the assets;*
- *Classifying information assets by sensitivity level allows for the implementation of organization-wide standards and controls over access and handling of the assets;*
- *Classifying technology assets (hardware) according to the sensitivity of the information assets resting on or passing through them allows for appropriate hardening and security measures to be implemented;*
- *A Health Information Asset Registry which tracks the life-cycle of ICES health information assets is an important component of ICES privacy compliance.*"¹³⁵

"ICES has defined, a system of eight information security classification levels:

- *four for individual level health information and;*
- *four for all other information that is created at ICES or that ICES holds here*

By health information, ICES means any information about the health status or care of an individual whether or not the individual is identified. So, for example, a drug formulary is not health information by this definition, but the list of drugs prescribed to an individual is."

¹³³ ICES' *Information Asset Management Program*. p1

¹³⁴ ICES' *Guide to Appropriate Use of ICES Information*. pp1-2

¹³⁵ ICES' *Information Asset Management Program*, pp12

Part 2 – Security Documentation

“These categories will enable security protections to be implemented appropriate to the sensitivity of the information asset:

1. Health Information

1.1 PHI – PHI contains direct identifiers such as name or health number

1.2 SHI – Site-identified Health Information contains site-specific identifiers such as medical record number but no other direct identifiers such as name or health number

1.3 LHI – Limited-Use Health Information contains no direct identifiers such as name or health card number but may contain indirect identifiers such as birth date or postal code.

1.4 DHI – De-Identified Health Information contains no identifiers as defined by PHIPA, i.e. no direct identifiers or indirect identifiers such as birth date, postal code, etc.

2. Non-Health Information

2.1 Restricted – information that is highly sensitive and critical in nature and is only available on a very limited need-to-know basis

2.2 Confidential – Information of a sensitive nature that is limited to a specific group of individuals as required

2.3 Internal Use – Information which can be openly used for organizational purposes within the corporate secure area

2.4 Public - Information which has been made available for public distribution”

“Information Assets in Scope:

- *Health Data Sets including:*
 - *Administrative health data*
 - *Primary-collected health data (electronic and paper)*
 - *3rd party health data*
 - *Survey data*
- *Supplemental Research Data*
- *EDC Applications and components*
- *SAS programs and macros*
- *Research Documents including, but not limited to:*
 - *research findings and publications,*
 - *project documentation,*
 - *grant applications*
- *Corporate documents including, but not limited to:*
 - *Human Resource records,*
 - *financial records,*
 - *policies, procedures, SOPs*
 - *data documentation*
- *Any other documents, data, programs or applications residing in ICES information systems”*

Part 2 – Security Documentation

“Technology Assets:

The scope of this program covers all information systems, applications including end-user computing, networks, databases, and computer equipment owned, managed, or used by ICES for processing. The scope also covers all electronic and physical media (such as computer printouts, reports, tapes, computer disks, etc.) where ICES data and documents are stored or shared with any internal or external entity.”

This measured program of information asset management transcends all layers of privacy/security protections and considerations throughout the document. There is not a single, specific place in the framework of the *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities* into which it fits, but it is pertinent to both Part 1 and Part 2.

Part 3 - Human Resources Documentation

Privacy Training and Awareness

1. Policy and Procedures for Privacy/Security Training and Awareness

Privacy/Security orientation is required for all Agents who are commencing employment or contractual or other working relationship with ICES that will require access to the ICES-Central premises or at an ICES satellite site in any capacity. ICES has a mandatory training requirement for all Agents to attend privacy and security training, as well as ongoing training requirements, which are described in ICES' *Privacy and Security Orientation Policy*.

All new Agents are required to complete initial privacy/security training on the first or second day of employment. **THERE ARE NO EXCEPTIONS TO THIS POLICY.** This rapid orientation requirement is particularly important for analysts, prior to gaining access to the UNIX system (and to de-identified health information, as access to PHI is only provided to Data Covenantors). Similarly, all Agents must sign an *ICES Confidentiality Agreement* and annually re-sign this agreement at the start of each fiscal year. *Non-disclosure Agreements (NDAs)* must be signed by any collaborating scientist whose role is simply to review and contribute to peer-review manuscripts. These individuals never have access to ICES or to data. Additionally, third party contractors/vendors in the process of tendering to conduct work for ICES sign NDAs.

The ICES' *Privacy and Security Orientation Policy* designates the CPO (or designate) or the Director, Information Management, as responsible for preparing and delivering the privacy/security training. The training content has been approved by the CPO and CISO/Security Lead prior to its delivery.

Each individual Agent will be verbally orientated by the Privacy Office Agents (CPO, LPO, Privacy Coordinator or designate) using a standardized PowerPoint presentation previously described and supplemented by information specific to their role. The Agent providing the training also promotes the interest of the Privacy/Security Offices in being perceived as an ICES resource: accessible, approachable and available to all Agents for information, clarification, further training and consultation. Additionally, access to the ICES' Privacy/Security-related Handbook, Privacy Code and all policy instruments will be provided in both print and electronic formats (made available on the ICES intranet), in acknowledgement of and to facilitate different learning styles.

Orientation training in privacy/security is delivered in accordance with the following process:

- i) The following Agents – the Directors/Managers/Program Administrator, Human Resources – notify the Privacy Office concerning new hires commencing employment at ICES; arrangements are made in advance of start date for privacy and security training.
- ii) Privacy/Security training is provided by Privacy Office staff using a standard PowerPoint Presentation, which is additionally supplemented and customized to the Agent's role at ICES;

Part 3 – Human Resources Documentation

- iii) upon completion of this presentation, written materials (*ICES Privacy Code; ICES Questions and Answers FAQ* and *ICES Privacy/ Security Handbook*) are provided to the new Agent;
- iv) *ICES Confidentiality Agreement* is signed;
- v) *ICES Confidentiality Agreement* is logged alphabetically and a paper copy is retained in the Confidentiality Agreement binder in the Corporate Offices.
- vi) The Privacy/Security Orientation log is also updated and reviewed regularly as the dates for the scheduled privacy trainings are booked and documented in the log. No UNIX access to de-identified data is ever provided until verification by IS/IT staff of completion of the privacy/security orientation and that the confidentiality agreement has been signed is provided by the Privacy staff.

While initial privacy/security orientation training is constantly updated and adjusted, the ICES' *Privacy/Security Orientation Policy* sets out the minimum content for the training in order to ensure some standardization. It always includes:

- ICES' status under PHIPA and the duties and responsibilities that arise as a result of this status;
- The nature of the PHI collected and from whom this information is typically collected;
- The purposes for which PHI is collected and used and how this collection and use is permitted by PHIPA and its Regulation;
- Limitations placed on access to and use of PHI by Agents (the limitation is no access);
- The procedure that must be followed in the event that an Agent is requested to disclose PHI;
- An overview of ICES' privacy and security policy instruments and the obligations arising from these;
- The consequences of breach of the privacy/security policies, SOPs and other procedures, standards, guidelines and practices implemented;
- An explanation of the privacy/security programs, including the key activities of the program and the CPO and CISO/Security Lead;
- The administrative, technical and physical safeguards implemented by ICES to protect PHI and its de-identified information against theft, loss and unauthorized use or disclosure and to protect records of PHI and de-identified information against unauthorized copying, modification or disposal;
- The duties and responsibilities of Agents in implementing the administrative, technical and physical safeguards put in place by ICES;
- A discussion of the nature and purpose of the Confidentiality Agreement that Agents must execute and the key provisions of the Confidentiality Agreement; and
- The *ICES Information Breach Policy* includes the procedures for identifying, reporting and containing a privacy breach. The duties and responsibilities which are imposed on Agents are to: identify, report, contain and participate in the investigation and assist as requested in remediation of both privacy breaches and information security breaches.
- Privacy/Security training will be provided in an ongoing basis through presentations, updates at monthly staff meetings, through electronically distributed privacy updates and print materials, webcasts and via role group discussions. Additionally, annual re-

Part 3 – Human Resources Documentation

training on privacy/security principles using computer-based internal training software is being implemented and is mandatory.

The ongoing privacy and security training also has some standard requirements to ensure its efficacy. These are laid out in the policy and include:

- role-based training relating to Agents' day-to-day duties;
- any new privacy/security policies, SOPs and other procedures, standards, tools, guidelines and practices and significant amendments to existing privacy and security policy instruments; and
- changes made to training models and/or updates based on recommendations from system-wide PIAs, the investigation of information security breaches, the conduct of security audits, including threat-risk assessments, security reviews, vulnerability assessments, penetration testing, ethical hacks and reviews of system control and audit logs.
- any recommendations with respect to privacy and security training made in system-wide privacy impact assessments (PIAs), privacy audits and the investigation of privacy breaches and privacy complaints.

In order to ensure compliance with the mandatory training requirements, and in accordance with ICES' *Privacy/Security Orientation Policy*, ICES maintains a spreadsheet log to track attendance at both the initial training and the various processes and instruments for ongoing privacy/security training. The Privacy Office Agents are responsible for maintaining this log, which is stored on the privacy/security shared drive. The log is the responsibility of the Agents of the Privacy Office (CPO, Privacy Co-ordinator and Privacy Office Administrator) and includes these details related to the documentation that must be completed, provided and/or executed to verify attendance;

- Privacy/Security training will be provided initially and in an ongoing fashion using a variety of modalities: presentations, updates at monthly staff meetings, electronically distributed privacy updates and print materials, webcasts and via role group discussion. Additionally, annual re-training on privacy/security principles using computer-based internal training software is being implemented and is mandatory.
- The Privacy/Security Orientation log is also updated and reviewed regularly (dates for the scheduled privacy trainings are booked and documented in the log). In reviews executed every six months, UNIX access is reassessed. Access is suspended if verification by Agents of the IS/IT staff of completion of the privacy/security training and the re-signing of confidentiality agreements is not confirmed against the logs.

Each Role Group leader or Principle Investigator/designate is responsible to ensure that all members of project teams have undergone security and privacy training. Security and privacy training is mandatory for all individuals who are commencing employment, contractual or other working relationships with ICES that will require them to work on the premises prior to being given access to any de-identified health information or at an ICES satellite site in any capacity.

Part 3 – Human Resources Documentation

ICES' Scientists are additionally responsible to facilitate access to privacy orientation for external, non-ICES collaborating scientists, even when they have no access to data and are working only on methodology problems or manuscript review. This facilitates their own understanding of ICES security/privacy culture, important for expanding understanding of the security and privacy protections in place at ICES when responding to issues or questions from external stakeholders or interested parties. These orientations are offered with a comprehensive slide deck for mutual viewing, using teleconferencing OR other similar technologies, such as *Webinar*.

Without exception, every effort is made to provide an appointment for privacy/security training in a timely fashion. Failure to attend this training will result in the denial of physical access to ICES and immediate revocation of any access privileges.

Non-disclosure Confidentiality Agreements must be signed by any scientists who only review manuscripts or persons who are in the process of tendering to conduct work for ICES. Please see Part 3, section 1 for more details previously described.

ICES is committed to ensuring a culture of privacy and security at ICES and to ongoing privacy/security awareness outside of its formal privacy and security training program. Therefore, ICES has consequently adopted a multi-pronged approach to its awareness program, including:

- Information disseminated at monthly staff meetings by CPO, IT Technical Manager, Security Lead or CISO;
- Information disseminated at monthly Research Coordinator/Project Manager meetings by CPO, CISO, LPO or Privacy Coordinator;
- Privacy & Security Committee monthly meetings;
- One-on-one consultative or didactic sessions;
- Privacy & Security Agent Surveys;
- A new ICES Privacy Newsletter, *PSsst* is produced on an 'as needed' basis:
 - Volume 1 – Issue 1 – July 2009: Testing Privacy Knowledge-Survey Results
 - Volume 1 – Issue 2 – October 2009: All about PIA Forms
 - Volume 1 – Issue 3 – March 2010: Confidentiality Agreements, Encryption Update and Phishing
 - Volume 2 – issue 1 – October 2010: Protect your Online Privacy/Messages from the Commissioner
 - Volume 2 – Issue 2 – March 2011: 2011 Privacy Quizz Answers
- Multiple PowerPoint decks for various trainings internally and externally (examples: REB, how data is linked, types of data held, Policies/practices and procedures [P3])
- Urgent Email direct to ICES' Agents outlining important issues and ICES' response to the issue (for example, discussing mobile device theft [led to HO-004] and USB key loss [led to HO-007] for which ICES already had developed a Mobile Devices policy. Since encryption was already well entrenched, this re-enforced the need for encryption).

The ICES' *Privacy/Security Orientation Policy* requires all Agents to comply with its terms. Compliance is enforced by the CPO and CISO/Security Lead, assisted by the Manager Administration, Principal Investigators (student Supervisors) and the Role Group Directors and Managers. It is in ICES' best interests to engage all supervisory roles in compliance assurance.

Part 3 – Human Resources Documentation

The policy clarifies that breach of policy may result in discipline, up to and including termination. As indicated in the *Discipline and Corrective Action Policy* or *Termination of Employment, Resignation and Discharge Policy*, compliance will be audited in accordance with ICES' *Privacy Audit Policy* twice annually and that the CPO and CISO/Security Lead will be responsible for conducting the audit.

From the HR perspective, ICES' *Information Breach Policy* and reporting framework not only includes instructions on what to do in the event of a breach or potential breach of information, but instructs on the seriousness of adherence to ICES' privacy and security policy instruments. Please also see Part 1 Privacy, section 29 and Part 2 Security, section 17:

“...should it be determined, the Agent(s) responsible for the breach will be disciplined or terminated according to the terms in the ICES Confidentiality Agreement, in consultation with ICES' HR Department and CEO and Deputy CEO¹³⁶”

ICES' culture has been built on the core belief that Privacy and Security work hand-in-hand. ICES, recognizes that security emphasis is technological by nature; privacy is more policy-driven. However, it is our preference to intermingle the disciplines in the context of training so that all Agents think of both when contemplating projects. ICES' core project document – the *Project-specific Privacy Impact Assessment (PIA)* form – provides an option to consult with the CISO or Security Lead should there be any new technological requirements, or if a novel project is being planned. The same is true for Privacy, where scientists are asked to indicate where there may be the need for new policies, practices or SOPs.

Requirements are set out in ICES' *Privacy/ Security Orientation Policy*:

- New Agents are required to complete initial security/privacy training as soon as possible (optimally their first day of employment) and must have signed *Confidentiality Agreements*;
- Formal security and privacy training must be attended at the time of hire or at the commencement of a project for which an Agent is hired;
- ICES' *Confidentiality Agreement* must be re-signed at the beginning of each fiscal year. Section 6 of ICES' *Confidentiality Agreement* particularly outlines the obligation of each Agent to be familiar with and agree to adhere to ICES' policies:

“you have an obligation to familiarize yourself and to comply with all policies, practices and procedures of ICES relating to privacy and security, including the policies, practices and procedures implemented from time to time after the date of this agreement.”¹³⁷

The *Privacy/ Security Orientation Policy* designates the CPO, LPO, Privacy Coordinator or designate as responsible for preparing and delivering the security/privacy training. The training content is always approved by the CPO/CISO/Security Lead prior to its delivery.

¹³⁶ ICES *Information Breach Policy*. P7

¹³⁷ ICES *Confidentiality Agreement* pp1-3

Part 3 – Human Resources Documentation

Orientation training in security/privacy is delivered in accordance with the following process:

- i) Security/privacy training is provided by a standard PowerPoint Presentation which is supplemented and customized to the Agent's role at ICES;
- ii) Upon completion of this presentation, written materials (*ICES Privacy Code*; *ICES Questions and Answers FAQ* and *ICES Privacy and Security Handbook*) are provide to the new Agent;
- iii) *ICES Confidentiality Agreement* is signed;
- iv) *ICES Confidentiality Agreement* is logged alphabetically and paper copy is retained in the Confidentiality Agreement binder in the Corporate Office.

While the initial security and privacy orientation training is constantly updated and adjusted, the *Privacy and Security Orientation Policy* sets out the minimum content for the training in order to ensure some standardization. It always includes:

- An overview of ICES' security/privacy policies and the obligations arising from these policies, procedures and practices;
- The consequences of breach of the security/privacy policies, procedures and practices implemented;
- An explanation of the security/privacy program, including the key activities of the program and the roles of the CPO, LPOs, Privacy Coordinators, CISO/Security Lead and the Privacy Office;
- The administrative, technical and physical safeguards implemented by ICES to protect PHI and de-identified information against theft, loss, unauthorized use or disclosure, unauthorized copying, modification or disposal;
- The duties and responsibilities of Agents in implementing ICES' administrative, technical and physical safeguards; and
- An explanation of the *Information Breach Policy* and the duties and responsibilities imposed on Agents in identifying, reporting, containing and participating in the investigation and remediation of information security breaches.

The ongoing security/privacy training also has some standard requirements to ensure its efficacy. These are laid out in the policy and include:

- Role-based training relating to their day-to-day duties;
- Any new security/privacy policies, SOPs and other procedures, standards, tools, guidelines and practices and significant amendments to existing ones; and
- Changes made to training models and/or updates based on recommendations from system-wide PIAs, the investigation of information security breaches, the conduct of security audits, threat-risk assessments, security reviews, vulnerability assessments, penetration testing, ethical hacks and reviews of system control and audit logs.

In order to ensure compliance with the mandatory re-training requirements, and in accordance with *Privacy/Security Orientation Policy*, ICES maintains a log to track attendance. The Privacy Office Agents are responsible for maintaining this log, which is kept in a shared drive folder for

Part 3 – Human Resources Documentation

tracking attendance. Details regarding the documentation that must be completed, provided and/or executed to verify attendance include:

- Name of Agent
- Title of Agent
- Supervisor of the Agent
- ICES privacy staff who conducted the privacy and security training
- Date of the privacy and security training

2. Log of Attendance at Initial Privacy/Security Orientation and Ongoing Privacy/Security Training

As described in Section 1, the Agents of the Privacy Office maintains the log of attendance at initial privacy/security training and ongoing privacy/security training activities. It contains the following fields:

- Name of the Agent and date the Agent attended the initial privacy/security training or retraining
- Agent's title and Supervisor
- Who conducted the privacy/security training or retraining

3. Policy and Procedures for the Execution of Confidentiality Agreements by Agents

ICES, requires all Agents who enter into a relationship with ICES to execute a *Confidentiality Agreement* in accordance with the *Confidentiality Agreement Policy*. Signing ICES' confidentiality agreement at the time of scientific appointment or starting employment at ICES obligates the signatory to comply with ALL ICES policies. Importantly, in relation to the requirements of the Manual, this obligation is not reiterated in every policy or SOP document because it is a condition of (ongoing) employment or appointment.

The *Confidentiality Agreement Policy* plus the *ICES Privacy/Security Orientation Policy* lays out the process governing this requirement, as well as the requirement that Agents re-execute the agreement on an annual basis, beginning of each fiscal year (April 1st).

ICES, ensures that all Agents execute the Confidentiality Agreement (as per the *Confidentiality Agreement Policy*) in accordance with the process set out below:

“1. Role Group leaders and/or Principle Investigators/designates should contact the Privacy Office by phone or email to book privacy training for new staff, students or external collaborators at the commencement of employment and/or prior to being given new access to health information.

2. *ICES Scientists should additionally facilitate access to privacy orientation for external, non-ICES collaborating scientists. Every effort will be made to provide an appointment for privacy/security training in a timely fashion.*

3. *Each individual will be verbally orientated by the CPO/LPO/Privacy Coordinator or designate to promote the interest of the Privacy and Security Offices in being perceived as an ICES resource: accessible, approachable and available to Agents for information, clarification, further training and consultation.*

4. *Additionally, access to the Privacy/Security-related Handbook, Privacy Code and all policies, SOPs and other procedures, standards, guidelines and practices, will be provided in both print and electronic formats (made available on the ICES intranet), in acknowledgement of and to facilitate different learning styles.”¹³⁸*

Policy instruments implemented by ICES are explained, and where they are posted and can be accessed. When this process has been concluded, an ICES *Confidentiality Agreement* will be signed as per the *Confidentiality Agreement Policy*.

As previously described in Sections 1 and 2, ICES requires mandatory initial privacy and security training for all Agents and additionally provides multi-modality ongoing training. The *Privacy/Security Orientation Policy* requires that ICES’ Manager Administration and Project Managers maintain the logs of executed Confidentiality Agreements; the related documentation is kept in locked file cabinets in their offices.

The *Confidentiality Agreement Policy* includes the following practice:

- The Manager Administration and designate are responsible for ensuring that a Confidentiality Agreement is executed with each Agent at the commencement of employment or appointment and thereafter on annual basis;
- The process for notification of the Agents of the Privacy Office is noted above;
- Confidentiality Agreements are tracked; failure to execute a new agreement annually within a pre-specified period results in revocation of all access; access is only restored when the Confidentiality Agreement is signed and presented to the Manager, Administration.

The *Privacy/Security Orientation Policy*, *ICES Privacy Code* and the *Confidentiality Agreement Policy* require Agents to comply with its terms; compliance is enforced by the CPO/CISO/Security Lead/ LPOs and Directors of the various ICES’ Role Groups. It clarifies that breach of the policy may result in disciplinary action up to and including termination. As indicated in the *Privacy/Security Orientation Policy*, compliance will be audited in accordance with ICES’ *Human Resources, Discipline and Corrective Action* annually.

¹³⁸ ICES *Privacy/Security Orientation Policy*. P 1

The *Human Resources, Discipline and Corrective Action Policy* and the *ICES Confidentiality Agreement Policy* include statements related to breach of *Policy*:

*“The Confidentiality Agreement specifically outlines the obligation of the individual to familiarize himself/herself with all ICES policies, practices and procedures in an ongoing fashion and to comply with these.”*¹³⁹

*“Any breach of this Agreement may result in disciplinary action being taken by ICES, up to and including a termination of any relationship you have with ICES, including without limitation any employment or other contractual relationship with ICES.”*¹⁴⁰

*“Corrective action ranging from warnings through to discharge may be initiated for culpable conduct (misbehaviour) or for any non-culpable conduct (e.g. incompetence). ICES' response will generally depend on the nature and severity of the misconduct, the employee's work record, seniority/service and other relevant factors.”*¹⁴¹

4. Template Confidentiality Agreement with Agents

ICES' *Confidentiality Agreement* has previously been reviewed and approved by the IPC in October 2005 and again in October 2008. Signing ICES' Confidentiality Agreement obligates the signatory to comply with ALL ICES policies. Importantly, this obligation is not reiterated in every policy instrument because it is a condition of affiliation with ICES. Suggested modifications to the agreement were put in place with the consultation of ICES' counsel.¹⁴²

ICES believes that the *Policy and Procedures for the Execution of Confidentiality Agreements* by Agents meets all the stated requirements on pages 111-112 in the Manual (as per previously approved documents in 2005 and 2008).

5. Logs of Executed Confidentiality Agreements with Agents

ICES' maintains a log of executed confidentiality agreements that includes:

- The name of the Agent;
- The date of the initial confidentiality agreement and start date of relationship with ICES;
- The dates of annual mandatory re-execution of the confidentiality agreement
- Agent's title
- Agent's Supervisor
- Who conducted the privacy/security orientation

¹³⁹ ICES Confidentiality Agreement Policy. P1

¹⁴⁰ ICES Confidentiality Agreement. Clause 9, page 3

¹⁴¹ ICES Discipline & Corrective Action Policy. P3

¹⁴² ICES Confidentiality Agreement, Clause 6.

Responsibility for Privacy and Security

6. Job Description for the CPO

At ICES, the CPO has been delegated day-to-day authority to manage the privacy program. The CPO reports directly to the CEO.

The job description identifies the key responsibilities and obligations for the role and includes the minimum obligations set out in the *IPC Manual for the Review and Approval of Prescribed Persons and Prescribed Entities*, including:

- Developing, implementing, reviewing and amending privacy policies, practices, procedures, SOPs, standards and guidelines [policy instruments];
- Ensuring compliance with the privacy policy instruments;
- Ensuring transparency of the privacy policy instruments implemented;
- Facilitating compliance with PHIPA and its Regulation;
- Ensuring Agents are aware of PHIPA and its Regulation and their duties/obligations/responsibilities in relation to PHIPA ;
- Ensuring Agents/vendors/consultants are aware of ICES' privacy policies and are appropriately informed of their duties and obligations in relation to PHIPA;
- Directing, delivering or ensuring the delivery of the initial privacy orientation and the ongoing privacy training and fostering a culture of privacy;
- Conducting, reviewing and approving system-wide and project-specific PIAs;
- Receiving, documenting, tracking, investigating, remediating and responding to privacy complaints pursuant to the *Complaints and Inquiries Policy*;
- Receiving and responding to privacy inquiries pursuant to the *Complaints and Inquiries Policy*;
- Receiving, documenting, tracking, investigating and remediating privacy breaches or suspected privacy breaches pursuant to the *Information Breach Policy*; and
- Conducting privacy audits pursuant to the *Privacy and Security Audit Policy*.

7. Job Description for the CISO

At ICES, the CISO has been delegated the day-to-day authority to manage the security program. The CISO reports directly to the Senior Director, Research Operations and through dotted-line report directly to the CEO.

The job description identifies the key responsibilities and obligations for the role and includes the minimum obligations set out in the *IPC Manual for the Review and Approval of Prescribed Persons and Prescribed Entities*, including:

- Developing, implementing, reviewing and amending security policies, practices, procedures, SOPs, standards and guidelines [policy instruments];

- Ensuring compliance with the security policy instruments implemented;
- Ensuring Agents /vendors/consultants are aware of ICES’ security policy instruments and are appropriately informed of their duties/obligations/responsibilities in relation to PHIPA;
- The ICES-wide Privacy and Security orientation and signing of the Confidentiality Agreement is undertaken by the Privacy Office; further detailed Security orientation is provided to the Agent by the CISO or designate depending on the requirements of the position the Agent has been hired to undertake;
- Directing, delivering or ensuring the delivery of the initial security orientation and the ongoing security training and fostering a culture of information security awareness;
- Receiving, documenting, tracking, investigating and remediating information security breaches or suspected information security breaches pursuant to the *Information Breach Policy*; and
- Conducting security audits pursuant to the *Privacy and Security Audits Policy*.

Termination of Relationship

8. Policy and Procedures for Termination or Cessation of the Employment or Contractual Relationship

ICES has a *Termination of Employment/Resignation & Discharge Policy* and well-established exit procedures which ensure that all ICES’ Managers, Directors and the Deputy CEO are notified of any Agent terminating their relationship with ICES. This includes all employment and contractual relationships. The policy requires that all ICES property, including access cards, identification badge, computer equipment, electronic devices and Marlok keys are returned prior to leaving the premises.

Termination of Employment-Resignation & Discharge Procedure:

- “1. The determination to discharge an employee from employment at ICES must be made in consultation with the Deputy CEO and Human Resources Manager.*
- 2. ICES must ensure that all relevant policies, legislative requirements are adhered to and the discharge is completed in a humane and caring manner.*
- 3. Information Systems Department must be notified in advance to ensure that computer, voice mail and building access is terminated at the time of discharge.*
- 4. The Role Group Director/Manager will be responsible for obtaining all ICES property such as Agent identification badge, keys, cell phones, laptop computers, passwords, etc. prior to the person leaving the premises. **Note: No PHI is in the possession of ICES’ Agents.***

Part 3 – Human Resources Documentation

5. *The Role Group Director/Manager must ensure that communications to staff are appropriate to the situation.*¹⁴³

The *Termination of Employment/Resignation & Discharge Policy*, like all ICES policies, requires all employees to comply with its terms and is overseen by the Deputy CEO and the Manager, Human Resources. All requirements of the Manual are presently met in our existing *Termination of Employment/Resignation & Discharge Policy*.

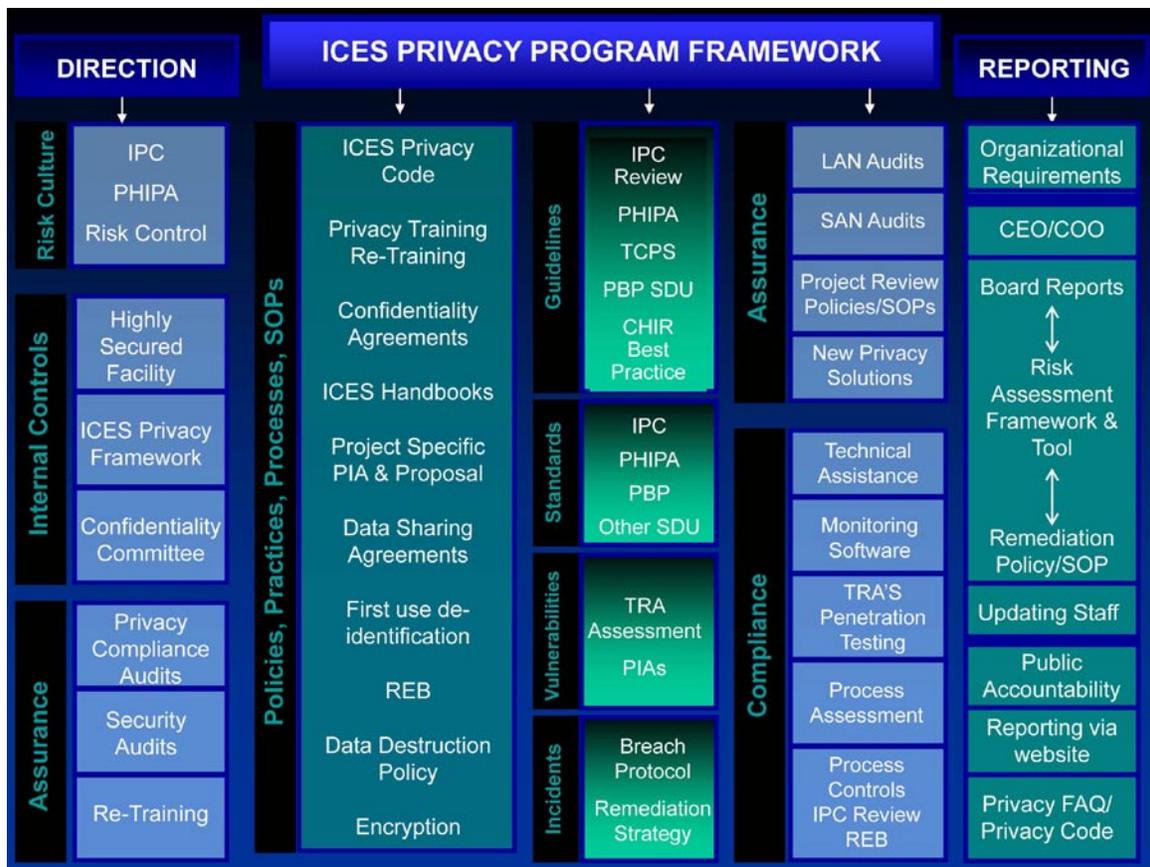
¹⁴³ ICES *Termination of Employment/Resignation/Discharge Policy*. p2

Part 4 - Organizational and Other Documentation

Governance

1. Privacy and Security Governance and Accountability Frameworks

ICES has two mutually-supporting documents – ICES’ *Privacy Program Framework* and the *Information Security Framework* – that describe schematically its privacy and security governance and accountability frameworks. These frameworks define/direct the privacy and security focus at ICES, by providing simple but workable foundations which are reflective of the many “influencers” in the ICES’ environment. The frameworks facilitate identification of basic programs and point the way to the necessary concomitant privacy and security requirements found in its core documents. Because security technology evolves continuously and privacy best practices change rapidly, ICES considers many of its practices, procedures, guidelines and standards as *living* documents. ICES also approaches privacy and security with a variety of policy instruments. All are intended to provide pathways to effective and robust privacy/security best practices.



Part 4 – Organizational and Other Documentation

The ICES Privacy Program Framework

The purpose of the *Privacy Program Framework* is to define and direct the privacy focus at ICES in a format that is simple, integrative and informative to facilitate achieving core privacy goals.

The CPO is responsible for ensuring that ICES is compliant with the requirements of PHIPA and its Regulation, as well as with all privacy policies at ICES, thus ensuring that its Agents can successfully carry out the statistical and evaluative projects and studies which are helping to manage and inform change of Ontario’s health care system – thus fulfilling ICES’ Mandate¹⁴⁴.

At each of ICES’ expansion sites, a LPO and/or Privacy Coordinator are responsible for creating the culture of privacy that ICES espouses and ensuring the sites’ compliance with PHIPA and ICES’ policies. The IPC has been kept abreast of and participated in evaluating the ICES’ expansion project since undertaking the first pilot site at ICES@Queen’s – input that has been highly valued.

The CPO, Privacy Staff of ICES-Central and LPOs/Privacy Coordinators of the expansion sites collectively form a team of privacy specialists, mandated to assist and facilitate the work at all ICES expansion sites. The primary foci of the Privacy Office include:

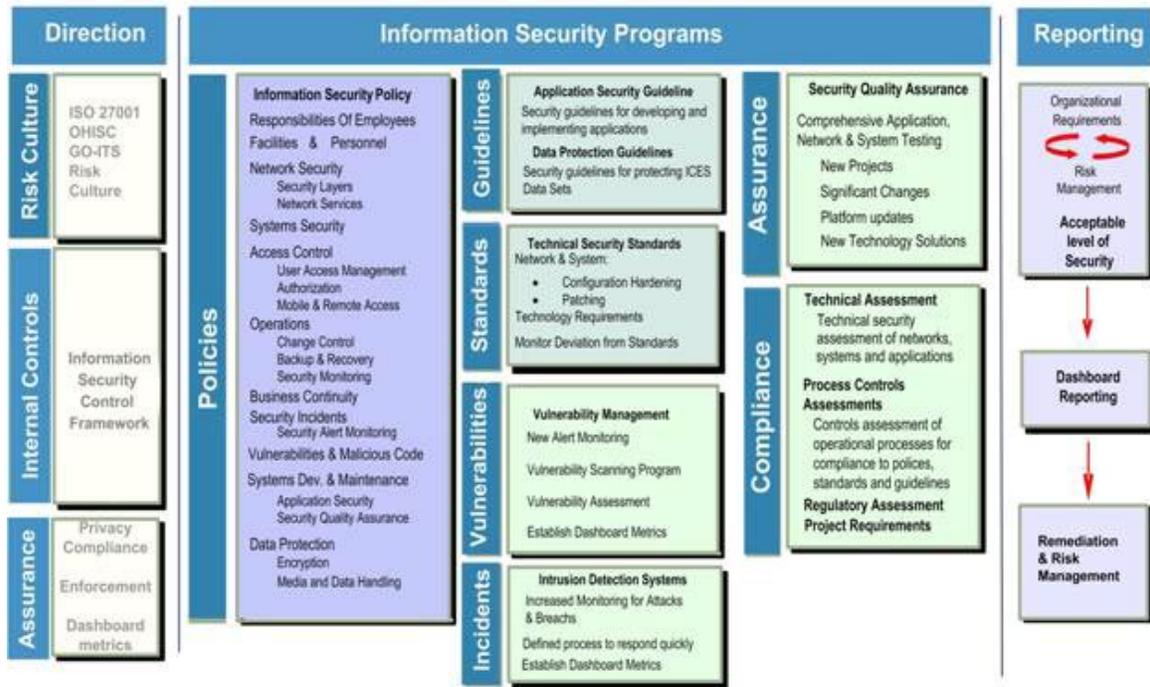
- ongoing training and education of privacy staff;
- facilitating the certification of ICES’ Agents/privacy staff with CIPP/C credentials;
- improving knowledge transfer capacity to all ICES’ Agents across the network. The Agents of the Privacy Office will work individually and collectively with ICES Agents to problem-solve, facilitate new data acquisitions, and insure compliance with ICES’ approved policies;
- providing opinion and advice related to studies planned for execution and their methodologic compliance with PHIPA under s. 45(1), to assist in the achievement of ICES ‘core business goals – to conduct research that contributes to the effectiveness, quality, equity and efficiency of health care and health services in Ontario’;
- providing “cross-coverage” for purposes of collaborative review of grants and other submissions, reviewing project-specific PIAs, and during vacation or sickness-related time at other sites as needed.

Weekly teleconference meetings for all Privacy Agents across the Network help create collegial relationships, foster a setting of learning and sharing, and an environment where review and constructive criticism are welcome. Additional professional meeting attendance and commitment to achieving International Association of Privacy Professionals – Canada (CIPP/C) certification – are encouraged.

¹⁴⁴ See http://www.ices.on.ca/webpage.cfm?site_id=1&org_id=26

The ICES Information Security Framework

ICES Information Security Framework



In the ICES context, Security has a clear and obvious position in the support of the privacy efforts already well ingrained in the organizational culture. The CISO and Security Lead are responsible for ensuring that ICES maintains a robust security posture to adequately secure the information held within our systems, either ICES’ own informational assets or information being handled and/or retained for partners and stakeholders.

The CISO has developed an *Information Security Framework*. The purpose of the framework is to define and direct the security focus in the institute, by providing a simple but workable foundation to identify key programs and the necessary concomitant security requirements (see Part Two, Number 1 for schematic representation).

The CISO, Security Lead and staff of the Security Office provide:

- (1) leadership around security;
- (2) governance for key ICES projects; and
- (3) operates in an Advisory role for the gaps and challenges of new projects, including:
 - o leadership in security programs, such as the Security Quality Assurance (SQA) assessment program now in place for ICES internal projects. SQA is an ISO 27001-based assurance program that is composed of 10 modular assessment components. Each of

Part 4 – Organizational and Other Documentation

these components addresses areas of compliance for information security such as technical scanning and legislative compliance, among others. SQA is a ‘living’ assessment program, which helps define and apply the security requirements that are appropriate and applicable, and will facilitate the ongoing assessment and review of key projects in which ICES will be engaging over the coming years as it is repeatable and measurable;

- from a governance perspective, the CISO/Security Lead and staff will leverage the initial assessments of a project as a baseline for future compliance reviews year after year. The issues and areas of non-compliance that are discovered during SQA reviews will be tracked for remediation purposes to ensure that the appropriate ‘compensating controls’ are applied to effectively reduce risk to ICES;
- from an Advisory point of view, the CISO and the Security Lead will work to solve security problems that present themselves in the context of planned projects and the ‘challenges of the day’. The questions that are not already answered are addressed in the detailed and growing body of policies and SOPs.

*ICES’ Organizational Chart*¹⁴⁵ and the *Remote Site Operational Reporting Structure Chart*¹⁴⁶ for the ICES Expansion Sites sets out that the day-to-day operational privacy and security functions have been delegated to ICES’ CPO and CISO, assisted by the Security Lead. ICES’ CEO, briefed and assisted by the CPO and CISO, is ultimately accountable for ICES and its Agents’ compliance with PHIPA and its regulation, as well as with all privacy instruments at ICES.

The *Job Descriptions*¹⁴⁷ of the CPO, CISO, the Security Lead and the *Terms of Reference*¹⁴⁸ for the various committees illustrate that the CPO and CISO are well-supported in managing their programs by various individuals, teams and committees, including:

Privacy:

- The ICES Privacy Office, including an Privacy Coordinator (.5FTE) and a Privacy Program Administrator (0.5 FTE)
- Each ICES Expansion Site has its own LPO.
 - ICES@Queen’s has a 0.5 FTE LPO and a 0.5 FTE Facility Coordinator who alternate in this role. There is also an Senior Analyst who participates in and reinforces the secure data practices additionally. The LPO is CIPP/C certified;
 - ICES@uOttawa has a 0.5 FTE LPO and a 1.0 FTE Facility Coordinator. The LPO is CIPP/C and CIPP/IT Certified. A Privacy Coordinator/Admin Support Agent has been hired who alternates

¹⁴⁵ *ICES Management Structure, 9 September 2010*

¹⁴⁶ *ICES Remote Site Operational Reporting Structure Chart, December 2010*

¹⁴⁷ *See Part 3: Sections 8 and 9. Human Resources Documentation*

¹⁴⁸ *See Part 4: Section 3 Terms of Reference for Committees with respect to the Privacy/Security Programs*

Part 4 – Organizational and Other Documentation

both roles, who is CIPP/C certified. All Privacy staff from ICES-Central, the two currently functioning expansion sites (ICES@Queen's and ICES@uOttawa), and the two sites *in development* (ICES@ Western and ICES@UofT) cross-cover each other for illness, vacations, grant and project review and assistance with general privacy issues. They meet by weekly teleconference and as needed for problem-solving privacy and security issues. These Agents are working towards CIPP/C certification as well.

Security:

- Security Lead (1.0 FTE)
- The Agents of the Information Systems/Technology (IT) and Information Security form a team of six individuals, including IS and helpdesk analysts, application development specialists, database and system specialists. The structure of the IS/IT team is integrative and flexible to meet the current needs of the organization
- Each ICES expansion site has its own local appointed security specialist who works closely with the ICES-Central team.

Mutually (Privacy & Security) supported by:

- Director, Information Management and two administrative data covenantors; four primary data covenantors; four application /system covenantors.
- Health Information Officer
- HIPS – the Agents/Health Information, Privacy, Security, Research Program, Senior Analysts (Directors and Leads)
- Agents of the Privacy and Security Committee (all role groups)
- Agents of the Operations Committee (Directors and Deputy CEO)

ICES is governed by a voluntary Board of Directors, whose collective range of experience and expertise guides our strategic direction and research priorities. This Board meets five times annually. ICES' Board of Directors does not actively participate in Privacy and Security day-to-day management issues, nor do they approve privacy/security policy instruments (these come through ICES' Operations Committee and Subject Matter Experts [SMEs]). However, they do approve *corporate* policies, such as finance and procurement procedures, and guide and approve the undertakings of ICES. The Board is updated about privacy/security concerns and their mitigation in the submission of ICES' Risk Report by these Agents: the CEO, Deputy CEO, Senior Director Corporate Services and Director Finance. The CPO and CISO may report through the Chairman of the Board's Risk and Audit Committee or directly to the Board, particularly if there are issues of immediate concern.

Updates to the ICES' Board of Directors include:

- Important initiatives undertaken by the privacy and security programs;
- A discussion of security/privacy audits and privacy impact assessments (PIAs) conducted, including the results of and recommendations arising; and
- Any breaches or complaints that were investigated, including the results of and any recommendations arising from these investigations

Part 4 – Organizational and Other Documentation

The Privacy and Security Governance and Accountability Frameworks are posted on the ICES' intranet for all Agents, including the ICES Expansion Sites. Using special accounts called "outside ICES", all other Agents and other stakeholders can have access to the *Research Practice* section of the intranet to maximize accessibility to research-related information of all types.

2. Security Governance and Accountability Framework

Described above.

3. Terms of Reference for Committees with Roles with Respect to the Privacy Program and/or Security Program

ICES, has written terms of reference for each committee that has a role in the privacy or security programs. These include:

- Identification of members of the committee
- The Agent chairing the committee
- The committee mandate and responsibilities in respect of privacy and security
- The frequency of meetings
- To whom the committee reports

4. Corporate Risk Management Framework

The original scope of ICES' Risk Management Committee was to develop and test a framework using privacy and data security risks related to projects. However, ICES' Agents who researched the risk management literature for best practices found that it supported the development of an 'enterprise-level' solution, including both *strategic* and *operational* types of risk for corporate decision-making, as well as risk assessment related to the execution of projects and studies. The IPC has endorsed the need for a framework for continuous risk assessment for prescribed entities. In the literature review undertaken, ICES also benefitted from the IPC review of other large agencies maintaining PHI, making it very clear that a risk management framework is a core requirement.

ICES formally recognized 'risk' in F2007/08 by developing an *Integrated Risk Management Framework* that addresses the risks to which the organization – and the data it holds – is exposed. ICES has implemented a framework that is designed to allow the continual identification, assessment, mitigation and monitoring of risks, including risks to its ability to protect the privacy and confidentiality of individuals whose PHI it has received. This framework was originally presented to the IPC for review and comment 28 May 2008. Importantly, ICES has developed a strong project risk assessment and management process, consisting of a formal template and categories to assess risk.

Part 4 – Organizational and Other Documentation

This process has been formalized as part of the ICES' Expansion Sites Project. Expansion Site Agents have been oriented and trained on Risk Assessment and are required to submit documentation on risk prior to *the build*. Importantly, the Privacy and Security components of these documents are based on both IPC and ISO 27001 standards. ICES' Expansion Sites at ICES@Queen's and ICES@uOttawa have been integrated into the risk process, and all ICES' expansion sites of the future (ICES@uToronto, ICES@UWO, and others pending) must also complete risk assessments prior to construction, and in an ongoing fashion thereafter.

The Deputy CEO, Director Project Integration Office and Senior Director Corporate Services are responsible for managing the ICES *Integrated Risk Management Framework* in accordance with the process set out in the document.

ICES defines risk management as:

*“the systematic application of management policies, practices and procedures to the task of identifying, analyzing, assessing, treating and monitoring risk”*¹⁴⁹

The purpose of an *Integrated Risk Management Framework*¹⁵⁰ is to:

- provide guidance to advance the use of a more corporate and systematic approach to risk management;
- contribute to building a risk-smart workforce and environment that allows for innovation and responsible risk-taking while ensuring legitimate precautions are taken to protect the public interest, maintain stakeholder trust, and ensure *due diligence*; and,
- propose a set of risk management practices that departments can adopt, or adapt, to their specific circumstances and mandate.

Application of the framework is designed to strengthen management practices, decision-making and priority setting; to enhance stewardship by strengthening capacity to safeguard the health data of the province yet maximize research interests; and, facilitate ICES' compliance with reporting requirements (e.g., the MOHLTC and the IPC) by ensuring that significant risk areas associated with policies, plans, programs and operations are identified and assessed, and that appropriate measures are in place to address unfavourable impacts and to benefit from opportunities.

This philosophy combines a strong commitment to four key elements: sound risk management; the application of an appropriate system of control and reporting; performance reporting (financial /non-financial); and values and ethics.

¹⁴⁹ ICES *Integrated Risk Management Framework* p1, citing Cameron WJ. *Managing Risk in the Public Sector: Good Practice Guide*. Auditing in the Public Interest. Office of the Auditor-General, Melbourne AUS; 2004. ISBN 0 9752308 1 6

¹⁵⁰ Treasury Board of Canada Secretariat. *Integrated Risk Management Framework*. Excerpts from this document are included throughout ICES' framework as encouraged in the original Treasury Board file

Part 4 – Organizational and Other Documentation

In emphasizing the need for more active and frequent consultation and risk communication, this approach to risk management has led to shared responsibility for managing risk among more of the Directors from all of ICES’ role groups.

The *Integrated Risk Management Framework* includes another important component: the *Risk Assessment Tool*. The tool facilitates documentation of risks and scoring of their likelihood of happening and the potential impact of the risk, using a three-by-three table with on-page definitions to maximize objectivity. The tool is particularly useful in doing project-specific risk assessments.

ICES maintains a detailed Security Risk Register based on ISO27001 Standards.

The identification of risk related to protecting the privacy interests of citizens and the security of the data, has lead ICES to employ an iterative approach, on a needs basis, to the reassessment of policies, practices and procedures – or the introduction of new policies, practices and procedures – to mitigate risks. A Schematic – the *Continuous Risk Management Process* – and a description of the approach can be found in ICES’ *Working Document 1: Integrated Risk Management Framework*.¹⁵¹ Additionally, the second document in the suite of Risk Management tools – *Working Document 2: Summary Approach to the Integrated Risk Management Framework*¹⁵² – lays out clearly the approach to this methodology of risk management.

Four elements are defined (Developing the Corporate Risk Profile; Establishing an Integrated Risk Management Function; Practicing Integrated Risk Management; Ensuring Continuous Risk Management Learning) and their core tasks, expected outcomes, and approach have helped provide the blueprint for rolling this strategy out. ICES has almost completed three of the four elements to date, leaving only the roll-out of the “Risk Management Orientation and Training” to all Agents, the development of regular risk management communications forums to support continuous learning, and the development of risk performance metrics and audits. ICES’ active Expansion Sites at ICES@Queen’s and ICES@uOttawa, as well as the other sites preparing for their “builds” (ICES@uToronto and ICES@Western), will be actively involved in this training.

The project has been somewhat slowed at ICES-Central because of resource constraints; ICES is interested in rolling this approach out in the Science and Corporate function areas and in creating a formal training program – completion is planned forward into fiscal 2011/12 and 2012/13. As mentioned above, Privacy and Security Risk Assessment evaluations at the Expansion Sites already do have these metrics /audits built in to their requirements.

¹⁵¹ ICES’ *Working Document 1: Integrated Risk Management Framework*. p 13

¹⁵² ICES *Working Document 2: Summary Approach to the Integrated Risk Management Framework*. p1-3

5. Corporate Risk Register

The *ICES' Risk Register* is planned as an ICES-wide corporate risk register that is updated annually for two purposes; the use of the ICES executive team and for presentation to ICES Board of Directors.

Currently, the Register contains the following key elements:

- Identified risks
- Ranking of risks based on the likelihood of the risk occurring and the potential impact to ICES if the risk does materialize
- Strategies to mitigate the risks are identified
- Timelines and a process to implement the mitigation strategies are developed

A corporate list of initiatives (i.e., ICES Expansion) is augmented by briefing notes developed for the Board documenting risk mitigation activities.

- Linked risks and risk drivers;
- A ranking of the risk; likelihood score/impact score = risk rating;
- Mitigation actions implemented;
- Retained (Net) Risk;
- Any additional mitigation required;
- Risk owner

As of spring 2011, ICES now has an active Board-level *Audit and Risk Committee*. ICES CEO, Deputy CEO, Senior Director Corporate Services, Director Project Integration and Director Finance are working toward the development of an expanded Risk Register process that will add Science and Corporate (see section 4) to Privacy, Security and Finance – and will report updates against the Register to the Committee and the Board on an annual basis. This strategy is planned to be finalized by F2012/13. In the meantime, ongoing status reports on risk are reported regularly to the Board.

6. Policy and Procedures for Maintaining a Consolidated Log of Recommendations

ICES, has implemented a policy *Maintaining a Consolidated Log of Recommendations* that requires the CPO, CISO/Security Lead/designates to maintain a consolidated log of recommendations to improve its privacy and security programs. The recommendations in the log are drawn from the following sources:

- System-wide Privacy Impact Assessments (PIAs)
- Privacy audits
- Security audits (threat-risk assessment, penetration testing, physical security)
- The investigation of privacy, security and policy breaches

Part 4 – Organizational and Other Documentation

- The investigation of privacy inquiries and complaints

A spreadsheet of the IPC's tri-annual review of ICES is maintained in the same privacy subdirectory; privacy and security breaches are also maintained in that subdirectory. A multi-page approach to one comprehensive document proved unwieldy, so these documents are clustered in the same directory for ease of access and use. Access to these files is restricted to members of the Privacy & Security Committee and Agents of the Privacy Office. All logs will be moved into a 2011 ICES Prescribed Entity Review library as legacy documents and to facilitate easy revision and change by Agents in the future.

The log, like most of ICES documents, is considered a “living” document, and is updated after any of the foregoing events and is reviewed as is required in relation to these activities. At a minimum, logs are reviewed annually as many of these functions are routine. Each new undertaking, such as database-related system-wide PIAs, will increase the scrutiny of the recommendations across the board. Recommendations that are risk-rated as critical or high risk are always prioritized and remediated immediately (or as soon as technologically possible). Recommendations carrying medium-to-low risk are attended to once the highest priority issues are dealt with. Issues related to breach investigations are evaluated immediately and recommendations acted upon as quickly as possible. The interconnectedness of recommendations is considered in planning forward.

7. Consolidated Log of Recommendations

ICES' consolidated log of recommendations located on ICES' privacy shared directory contains the following data elements for each recommendation in the log:

- The Agent/author, title, version number and date of the review document;
- The system reviewed;
- Agent responsible for the review and addressing the recommendation;
- A description of the recommendation;
- The date the recommendation was addressed.

The mitigation or manner in which the recommendations are addressed are included in the Change Management Table, as previously described in Part 2, Number 12.

Business Continuity and Disaster Recovery

8. Business Continuity and Disaster Recovery Plan

ICES has worked with third party experts to help in the development of an improved, comprehensive *Business Continuity and Disaster Recovery Plan* to ensure the continued availability of the information technology environment in general, and the health information holdings in particular, in the event that there is a business interruption or threats to ICES’ operating capability.

ICES engaged Deloitte LLP to assist its business continuity planning (BCP) initiative. Key phases of the BCP development consist of current state assessment; business impact analysis (BIA); continuity risk assessment; recovery strategy options; and, the development of recovery plans and procedures. To date, Deloitte has assisted ICES in completing the first three phases of the BCP development. ICES will be assembling an internal Task Force in F2011 to review recommendations and create a final plan for approval by ICES’ Executive (and the Board). In addition, ICES will be upgrading the ICES IT Network in F2011 which will provide the necessary technical infrastructure to support many of the BCP requirements and will improve the recoverability of ICES’ technological infrastructure.

The recoverability of mission-critical business processes and critical resources is typically guided by the formulation and implementation of appropriate business continuity strategies that will make it possible for critical operations to resume within specific periods following the occurrence of a disaster or disruption. Critical resources have been identified and recovery objectives have been defined. The categories of critical resources typically consist of “People”, “Facilities and Equipment”, “IT”, “Data”, “Third Parties” and “Process Knowledge”. These resource categories are used to identify specific instances of critical resources and provide a comprehensive yet practical approach to business continuity planning.

Deloitte has guided ICES’ Agents in completing a business impact analysis exercise and has thus identified its mission-critical business processes and critical resources. The business impact analysis exercise has also resulted in the definition of recovery objectives to address business requirements around the recovery and restoration of critical resources following a disaster or disruption. These outcomes have thus prepared the grounds for ICES to plan appropriate strategies to recover and restore various critical technology resources within specific time frames as required by the business.

Deloitte has assisted ICES to review its current business continuity strategies and has also assisted in the identification of opportunities for improvement and made recommendations on new strategies to satisfy the needs of the Institute.

The draft *Business Continuity Policy* and the draft *Business Continuity and Disaster Recovery Plan* will cover the following key elements in detail:

- i) Notification of the Interruption – roles and responsibilities, the contact list, timeframes, and form of notification

Part 4 – Organizational and Other Documentation

- ii) Assessment of the Severity of the Interruption – roles and responsibilities, criteria for assessment and documentation, initial impact assessment, a detailed damage assessment
- iii) Resumption and Recovery – activation of the business continuity and disaster recovery plan, an inventory of all critical applications and business functions, procedures for recovery of every critical application and business function, prioritization of recovery activities, recovery time objectives, roles and responsibilities, and documentation
- iv) Governance During an Event – the procedure by which decisions are made, the Crisis Management Team making the decisions
- v) Testing, Maintenance and Assessment of the Plan – frequency of testing, roles and responsibilities, plan amendments process, approval of the plan and amendments thereto

ICES has learned significantly from this consultation, and is working to refine and review plans to complete the process undertaken with Deloitte and with the support of the ICES' Board of Directors. Targeted date of completion for this project is fiscal 2012/13 (see Appendix FOUR).

The CEO, Deputy CEO, CISO, Security Lead, IT Manager, the Director Communications and other designated individuals are responsible for communicating the plan when finalized to all appropriate Agents across the network and for managing all communications during an interruption or threat event.

ICES' Alternate Data Centre (ADC)

An important part of the ICES Business Continuity/Disaster Recovery plan that has been accomplished is the establishment/ maintenance of an operational Alternate Data Center (ADC), that provides redundancy for IT materials and resources that are considered critical to the ongoing operation of the organization. The strategic location of the ADC provides geographical separation from the ICES-Central grid and yet affords access to the systems within a day. Support of the ICES' Expansion Network is important - in the event of a failure at ICES-Central, all activity can be migrated to the ADC through connection configuration.

ICES' CISO/Security Lead have consulted extensively with the IPC security experts in this "build", and the IPC Senior Security Analyst has visually inspected the site and reviewed all security testing reports with the CISO prior to operationalization.

"The ADC provides highly secured housing for a replica of the de-identified data that ICES holds. Not all data will immediately be replicated to the ADC; however, the de-identified data holdings from the ICES-Central UNIX systems will be replicated on a regular basis to allow ICES to achieve the Recovery Time Objective (RTO) stated in the Business Continuity Plan (BCP)... the present targets for the replication and RTO are that replication

Part 4 – Organizational and Other Documentation

will occur at least once every 24 hours to support an organizational RTO of 6 days.”

“All access to the data center is highly controlled/restricted...only ICES Agents have access unless otherwise directed by named ICES personnel¹⁵³... access to the cage area is controlled through controlled access to the raised floor and mechanical key locks [sic] to the cage and all racks”¹⁵⁴

Other corporate data may be stored in the cages at the ADC on other static media such as tape. Finally, ICES Agents continue to follow ICES’ *Data Backup SOP* daily and store sensitive data in its fireproof vault, as previously described in Part 2, Section 13.

The 2011 ICES Review document was prepared by Pamela Slaughter, Janice A. Richards, Raluca Blidaru, Susan Rohland, Stella Desouza and Don DeBoer, with the support and assistance of ICES’ Deputy CEO, CISO, Director Information Management, other ICES’ Directors and ICES’ Expansion Sites Privacy Staff. ICES thanks and acknowledges the support of colleagues at other organizations: CIHI (Mimi Lepage, Mary LeDoux, Cal Marcoux, and through them, Pam Snively and Adam Kardash); CCO (Pamela Spencer, Swapna Petrelli, Sara Azargive); POGO (Madeline Riehl, Bruna DiMonte).

¹⁵³ ICES’ *Request for Alternate Data Centre Access SOP*

¹⁵⁴ ICES’ *Alternate Data Center Policy*. p1

Appendix One: Privacy Indicators

Part 1 – Privacy Indicators

Categories	Privacy Indicators	ICES Response
<p>General Privacy Policies, Procedures and Practices</p>	<p>The dates that the privacy policies and procedures* were reviewed by the prescribed entity since the prior review of the Information and Privacy Commissioner of Ontario (IPC).</p> <p>(*at ICES, as suite of ‘privacy instruments’ are in place, including policies, practices, standard operating procedures and other procedures, tools, guidelines and standards. Reference to policies and procedures will include these various instruments which are policy equivalents, as described in the Introductory section of this document [About This Report])</p> <p>General Deficiency: ICES has always noted the date (month/year) of modification to policies, SOPs, practices, procedures, standards, guidelines and logs as per the requirements in the Manual, but does not track the extensive detail requested in the IPC review of our submission.</p> <p>ICES will build more comprehensive logs going forward for the institutional 2014 review.</p> <p>This deficiency is included in the first row of the Table of Deficiencies in Appendix FOUR.</p>	<p><i>Ongoing Privacy and Security Training Policy</i> first adopted December 2010</p> <p><i>Review of Privacy and Security Policy, Procedures and Practices</i> first adopted August 2008; revised November 2010</p> <p><i>Business Continuity Policy</i> first adopted October 2010</p> <p><i>Review and Approval of Project Submissions: PIA, PAW, Proposal</i> first adopted October 2010</p> <p><i>General Public Inquiry Relating to PHI Protection Policy</i> first adopted December 1998; revised October 2005; October 2010</p> <p><i>Privacy and Security Audit Policy</i> first adopted October 2010</p> <p><i>Destruction of 3rd Party Health Data SOP</i> created July 2010</p> <p><i>Policy and procedures for executing DSAs</i> first adopted June 2010</p> <p><i>ICES Information Breach Policy</i> first adopted June 2004; revised October 2005, January 2008, November 2008, May 2010, May 2011</p>

Appendix One: Privacy Indicators

Categories	Privacy Indicators	ICES Response
		<p><i>Maintaining a Log of Recommendations</i> first adopted May 2010</p> <p><i>Receiving and Processing Administrative Data SOP</i> created March 2008; reviewed January 2010</p> <p><i>Small Cell review Panel Terms of Reference Policy</i> first adopted August 2009</p> <p><i>Creating and Disturbing Case Lists for Primary Data Collection SOP</i> created March 2008; reviewed March 2009</p> <p><i>Information Breach Policy</i> first adopted June 2004; revised October 2005, January 2008, November 2008, November 2010, May 2011</p> <p><i>Protecting Personal Health Information on Mobile Devices Policy</i> first adopted in February 2008; revised October 2008</p> <p><i>Shredding of Confidential Material Policy</i> first adopted in May 2003; revised October 2005, August 2008</p> <p><i>Privacy and Security Orientation Policy</i> first adopted August 2008</p> <p><i>Standard Operating Procedures for Data Management Policy</i> first adopted March 2008</p> <p><i>Data Destruction Policy</i>, first adopted June 2004; revised November 2006, January 2008</p> <p><i>Confidentiality Agreement Policy</i> first adopted December 1998; revised January</p>

Appendix One: Privacy Indicators

Categories	Privacy Indicators	ICES Response
		<p>2008</p> <p><i>Challenging Compliance Policy</i> first adopted in December 1998; revised October 2005</p> <p><i>General Public Inquiry Relating to Management & Protection of Personal Health Information Policy</i> first adopted in December 1998; revised October 2005</p> <p><i>Individual Access to Personal Health Information Policy</i> first adopted in December 1998; revised October 2005</p> <p><i>Importing External Datasets to ICES Policy</i> first adopted in November 2004; revised October 2005</p> <p><i>Ethics Review Process for ICES Research projects</i> first adopted December 1998; revised October 2005</p> <p><i>ICES Standards for Project Close-out SOP</i> created July 2009; reviewed July 2010; retired on October 18, 2010 (replaced by the <i>ICES Standards for the Organization of Project Files and Project Closure</i>)</p>
	<p>Whether amendments were made to existing privacy policies and procedures as a result of the review, and if so, a list of the amended privacy policies and procedures and, for each policy and procedure amended, a brief description of the amendments made.</p>	<p>See above</p> <p>Please refer to existing policy instruments. Do not document revisions routinely: See Appendix FOUR: Table of Deficiencies</p>

Appendix One: Privacy Indicators

Categories	Privacy Indicators	ICES Response
	<p>Whether new privacy 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.</p>	<p>New policies and procedures as included in Appendix Four: Table of Deficiencies for list. Language derived from <u>Manual for the Review and Approval of Prescribed Persons and Prescribed Entities</u> as required. Lists of policy deficiencies requiring remediation are also appended; please see Appendix Four: Table of Deficiencies for list.</p>
	<p>The date that each amended and newly developed privacy policy and procedure was communicated to employees and, for each amended and newly developed privacy policy and procedure communicated to employees, the nature of the communication.</p>	<p>Dates of implementation included in header of policy or SOP. Documents are posted on ICES intranet (www.insideices.on.ca) which is the central repository for all Agents for all documents.</p>
	<p>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.</p>	<p>Please see Appendix THREE: please see Recommendations Table for changes made. Internal documents remain internal as per ICES' Information Asset Management Program; changes to outward-facing documents on the webpage (www.ices.on.ca) as per recommendations.</p>
<p>Collection</p>	<p>The number of data holdings containing personal health information (PHI) maintained by the prescribed entity.</p>	<p>ICES has 28 data holdings containing PHI (archived in vault). <u>Only de-identified information with HCN encrypted are used for the articulated purposes on which ICES</u></p>

Appendix One: Privacy Indicators

Categories	Privacy Indicators	ICES Response
		<p><u>work is based.</u></p>
	<p>The number of statements of purpose developed for data holdings containing PHI.</p>	<p><u>ONE General Statement of Purpose</u> for each holding of PHI has been drafted in a tabular format. This list of Data Holdings with statements of purpose can be found in Appendix TWO.</p> <p>“PHI is disclosed by custodians for the purpose of analysis or compiling statistical information with respect to the management of, evaluation or monitoring of, the allocation of resources to or planning for all or part of the health system, including the delivery of services” (s.45 (1) PHIPA).</p> <p>All proposed projects are evaluated against that purpose (see ICES <i>Project-specific Privacy Impact Assessment Form</i>) as these data are used constantly for the approved project purposes. However, the data has been de-identified before the use is undertaken and is no longer PHI.</p>

Appendix One: Privacy Indicators

Categories	Privacy Indicators	ICES Response
	The number and a list of the statements of purpose for data holdings containing PHI that were reviewed since the prior review by the IPC.	NONE
	Whether amendments were made to existing statements of purpose for data holdings containing PHI as a result of the review, and if so, a list of the amended statements of purpose and, for each statement of purpose amended, a brief description of the amendments made.	Statements of purpose by each administrative database developed as per request. See Appendix TWO.
Use	The number of Agents/data covenantors granted approval to access and use personal health information for purposes other than research.	As reported to the IPC and the MOHLTC: 3 Administrative Data covenantors 7 Primary Data covenantors 1 ICES@Queen’s Primary Data Covenanter
	The number of requests received for the use of PHI <u>for research</u> since the prior review by the IPC.	NONE
	The number of requests for the use of PHI <u>for research</u> purposes that were granted and that were denied since the prior review by the IPC.	NONE
Disclosure	The number of requests received for the <u>disclosure of PHI</u> for purposes other than research since the prior review by the IPC.	NONE

Appendix One: Privacy Indicators

Categories	Privacy Indicators	ICES Response
	The number of requests for the <u>disclosure of PHI</u> for purposes other than research that were granted and that were denied since the prior review by the IPC.	NONE
	The number of requests received for the <u>disclosure of PHI for research</u> purposes since the prior review by the IPC.	NONE
	The number of requests for the <u>disclosure of PHI</u> for research purposes that were granted and that were denied since the prior review by the IPC.	NONE
	The number of Research Agreements executed with researchers to whom PHI <u>was disclosed</u> since the prior review by the IPC.	NONE
	The number of requests received for the <u>disclosure of de-identified and/or aggregate information</u> since the prior review by the IPC.	October 1, 2008 – September 30, 2009 = 169 October 2009 – September 2010 = 199 October 1, 2010 –31 March 2011 = 134 1 March 2011 – 13 June 2011 = 32 Total = 534

Appendix One: Privacy Indicators

Categories	Privacy Indicators	ICES Response
	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 by the IPC.	The number of agreements executed for de-identified use: the <i>cd-link</i> project = 9 The number of requests for aggregated data disclosed for other purposes = 4 Public Health(OAHPP/CDC/Health Canada agreements) Aggregated information resides on ICES' website for the public and scientists in all publications
Data Sharing Agreements	The number of Data Sharing Agreements (DSAs) executed for the collection of PHI by the prescribed entity since the prior review by the IPC.	2008 – 88 2009 – 118 2010 – 55 Total = 261
	The number of DSAs executed for the disclosure of PHI by the prescribed entity since the prior review by the IPC.	NONE
Agreements with Third Party Service Providers	The number of agreements executed with third party service providers with access to PHI since the prior review by the IPC.	NONE
Data Linkage	The number and a list of data linkages of De-identified data approved since the prior review by the IPC.	NONE: no linkages of PHI. Data is de-identified/ health card numbers encrypted in a two-step process electronically BEFORE linkage.

Appendix One: Privacy Indicators

Categories	Privacy Indicators	ICES Response
		<p>Extensive, project-specific PIA logs are maintained including each use of de-identified linked data and datasets used.</p> <p>1 October 2008 – 30 September 2009 = 169 1 October 2009 – 30 September 2010 = 199 1 October 2010 – 31 March 2011 = 134 1 March 2011 – 13 June 2011 = 32</p>
<p>Privacy Impact Assessments</p>	<p>The number and a list of privacy impact assessments (PIAs) completed since the prior review by the Information and Privacy Commissioner of Ontario and for each privacy impact assessment:</p> <ul style="list-style-type: none"> – The data holding, information system, technology or program, – The date of completion of the privacy impact assessment, – 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. 	<p>One PIA has been conducted at ICES: Pre-migration Citizenship & Immigration Canada Landed Immigrant Database (CIC-LIDS/FOSS) data = 1</p> <p>Privacy impact assessment for disclosure of personal information in Citizenship and Immigration Canada’s Landed Immigrant Data System, started 24 March 2010, completed 17 May 2010. Recommendations met, dated.</p> <ul style="list-style-type: none"> • It is recommended that this PIA be treated as a “living” document and updated/amended as plans for disclosure for research proceed. It should be reviewed and updated as plans for the disclosure evolve (change management table) • It is recommended that ICES provide an example of a single ‘dummied’ research-ready record, including CIC data fields augmented with fields

Appendix One: Privacy Indicators

Categories	Privacy Indicators	ICES Response
		<p>from records from other ICES data sets. This will demonstrate the effect of de-identification and the reasonably low risk of re-identification. NOTE: ICES responded to this recommendation on July 7, 2010;</p> <ul style="list-style-type: none"> • The exact fields to be provided need to be determined prior to disclosure. 7 Feb 2011 • It is recommended that CIC and ICES amend the existing DSA to permit use of the LIDS health data set created under the 2002 agreement to allow further linkage with ICES data sets for further research, specifying that ICES privacy policies, practices and procedures and associated limits on use and disclosure of identifying information continue to be applied to handling of the health data. 7 Feb 2011 • The DSA should specify the terms of reuse, termination, and a date for data disposal. 7 Feb 2011 • The DSA should reference ICES policies, practices and procedures and that these will be applied to the disclosure. 8 Mar 2010, 11 March

Appendix One: Privacy Indicators

Categories	Privacy Indicators	ICES Response
		<p>2010</p> <ul style="list-style-type: none"> • The DSA should be revisited by CIC and ICES yearly to consider the following: <ul style="list-style-type: none"> a. The exact set of fields chosen would be specified in an addendum to the DSA. If a field does not fulfill the criteria set out in Section 4.3.1.2 then some form of privacy assessment should be done. b. After the fields to be disclosed have been identified, resolve whether the previous year’s disclosure may be destroyed without risk to disaster recovery. • It is recommended that the PI disclosed be archived at ICES in accordance with its normal best practices, for the duration set out in the DSA.7 Feb 2011 • Two questions remain open that can be decided and noted either within this PIA or as an appendix to the DSA. Both decisions are based on technical best practices for security. As the best practices and

Appendix One: Privacy Indicators

Categories	Privacy Indicators	ICES Response
		<p>technology may evolve, it would be best to revisit these decisions as appropriate.</p> <p><u>1. Transmission (disclosure method)</u>: Transmission of the data from CIC to ICES could follow either:</p> <ul style="list-style-type: none"> a. the CIC method of delivery of an encrypted CD which is destroyed after transfer; this method matches a documented policy¹⁵⁵ with ICES for secure transfer; or b. the ICES preferred method, of providing a secure portal (SSL-VPN) and file transfer location. <p><u>2. Disposal (destruction)</u>: Should it be decided that the original PI at ICES should be destroyed, the method of disposal could follow either</p> <ul style="list-style-type: none"> a. the CIC model of destruction of the CD; or b. the ICES model of planning and certifying destruction of data, as per the ICES IPC-approved data destruction policies and procedures. 7 Feb 2011

¹⁵⁵ SOP: Receiving project-specific data sets from external sources DM001_jan2810.pdf, ICES

Appendix One: Privacy Indicators

Categories	Privacy Indicators	ICES Response
		<ul style="list-style-type: none"> • Going forward, the security personnel at both CIC and ICES will need to work collaboratively to determine the best method for yearly transmissions of data and appropriate disposal. • It is recommended that CIC keep an exact copy of the data sent to ICES, in case of the need to check for data corruption or loss. 7 Feb 2011 • Access to a CIC content expert for CIC’s FOSS/LIDS should be part of the DSA with ICES. This will help notify ICES of any changes and resolve any interpretive issues. It helps to ensure the notion of “data integrity” as applied to research and to ensure that ICES is able to properly and most effectively interpret the data, in the spirit of CIC’s mandate in providing the data for research. 7 Feb 2011 • Should new research be published using the CIC-sourced data, the DSA should state that CIC wishes to be notified by a written report prior to publication so that they

Appendix One: Privacy Indicators

Categories	Privacy Indicators	ICES Response
		<p>can have communications prepared should any be necessary. 7 Feb 2011</p> <ul style="list-style-type: none"> • The CIC Research and Evaluation Branch has indicated its support for additional and ongoing research using the LIDS/FOSS health data set. The Branch does not require that it approves each and every research project, but requests that it be kept up-to-date and informed about the projects making use of the data set. Accordingly, it is recommended that the DSA be amended to reflect that ICES will, at an agreed upon interval, update the Research and Evaluation Branch with regard to new projects making use of the LIDS/FOSS health data set. 7 Feb 2011
	<p>The number and a list of PIAs undertaken but not completed since the prior review by the IPC and the proposed date of completion.</p>	<p>TWO Pre-migration MYCS data = 1 (draft status; tabled with MYCS for review July/August 2011) Pre-migration PIA for RCSN data = 1 (being developed)</p>

Appendix One: Privacy Indicators

Categories	Privacy Indicators	ICES Response
	The number and a list of PIAs that were not undertaken but for which PIAs will be completed and the proposed date of completion.	NONE
	The number of determinations made since the prior review by 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.	NONE
	The number and a list of PIAs reviewed since the prior review by the IPC and a brief description of any amendments made.	NO OTHERS: completion of CIC-LIDS/FOSS PIA as described above
Privacy Audit Program	<p>The dates of audits of Agents granted approval to access and use PHI since the prior review by the IPC and for each audit conducted:</p> <ul style="list-style-type: none"> - 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. 	<p>NONE</p> <p>ICES does not audit its covenantors; see Appendix FOUR: Table of Deficiencies</p>

Appendix One: Privacy Indicators

Categories	Privacy Indicators	ICES Response
	<p>The number and a list of all other privacy audits completed since the prior review by the Information and Privacy Commissioner of Ontario and for each audit:</p> <ul style="list-style-type: none"> – 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 – The manner in which each recommendation was addressed or is proposed to be addressed. 	<p>ICES’ electronic LAN audit done January-February 2011.</p> <p><u>Change of Methodology:</u> Resource constraints precluded ~500 hours of personal audit time by CPO. To make this more cost-effective, electronic audit of LAN performed over a 4 day period rather than manual audit. Audit usually reveals files with suspicious names which actually turn out to be benign. The automated internal audit revealed 13 accounts out of 150 which requires review by IT Agents and the CPO. Review by IT Agents/CPO underway to validate/invalidate findings; to be completed August 2011</p> <p>See Appendix FOUR: Table of Deficiencies</p>
<p>Privacy Breaches</p>	<p>The number of notifications of privacy breaches or suspected privacy breaches received by the prescribed entity since the prior review by the IPC.</p>	<p>NONE</p> <p>ICES Policy Breaches, none of which involved PHI</p> <p>2008 = 4</p> <p>2009 = 6</p> <p>2010 = 5</p>
	<p>With respect to each privacy breach or suspected privacy breach:</p> <ul style="list-style-type: none"> – 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, 	<p>No breaches of PHI.</p> <p>See log of internal policy breaches maintained with this data</p>

Appendix One: Privacy Indicators

Categories	Privacy Indicators	ICES Response
	<ul style="list-style-type: none"> – The containment measures implemented, – The date(s) that the containment measures were implemented, – The date(s) that notification was provided to the health information custodians 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. 	
<p>Privacy Complaints</p>	<p>The number of privacy complaints received since the prior review by the IPC.</p>	<p>NONE</p>
	<p>Of the privacy complaints received, the number of privacy complaints investigated since the prior review by the IPC and with respect to each privacy complaint investigated:</p> <ul style="list-style-type: none"> – The date that the privacy 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 	<p>NONE</p>

Appendix One: Privacy Indicators

Categories	Privacy Indicators	ICES Response
	<p>complaint describing the nature and findings of the investigation and the measures taken in response to the complaint.</p>	
	<p>Of the privacy complaints received, the number of privacy complaints not investigated since the prior review by the IPC and with respect to each privacy complaint not investigated:</p> <ul style="list-style-type: none"> – 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. 	<p>NONE</p>

Security Indicators

Part 2 – Security Indicators

Categories	Security Indicators	ICES Response
<p>General Privacy Policies, Procedures and Practices</p>	<p>The dates that the security policies and procedures were reviewed by the prescribed entity since the prior review of the IPC.</p> <p>General Deficiency: ICES has always noted the date (month/year) of modification to policies, SOPs, practices, procedures, standards, guidelines and logs as per the requirements in the Manual, but does not track the extensive detail requested in the IPC review of our submission.</p> <p>ICES will build more comprehensive logs going forward for the institutional 2014 review.</p> <p>This deficiency is included in the first row of the Table of Deficiencies in Appendix FOUR.</p>	<p><i>Ongoing Privacy and Security Training Policy</i> first adopted December 2010</p> <p><i>Review of Privacy and Security Policy, Procedures and Practices</i> first adopted August 2008; revised November 2010</p> <p><i>Review and Maintenance of System Controls and Audit Logs Policy</i> first adopted November 2010</p> <p><i>Business Continuity Policy</i> first adopted October 2010</p> <p><i>Privacy and Security Audit Policy</i> first adopted in October 2010</p> <p><i>Maintaining a Log of Recommendations</i> first adopted May 2010</p> <p><i>Confidentiality & Security of Data Policy</i> first adopted January 1999; revised October 2005, January 2008, August 2009</p>

Appendix One: Security Indicators

Categories	Security Indicators	ICES Response
		<p><i>Appropriate Use of Computer Equipment Policy</i> first adopted in May 2002; revised June 2009</p> <p><i>Building/Office Access/Security Policy</i> first adopted in January 1999; revised October 2005, January 2008</p> <p><i>Confidentiality Agreement Policy</i> first adopted December 1998; revised January 2008</p> <p><i>Ethics Review for ICES Research Projects Policy</i> first adopted December 1998; revised October 2005, January 2008</p> <p><i>Visitors to ICES Policy</i> first adopted in December 1998; revised October 2005, January 2008</p> <p><i>LAN Password Policy</i> first adopted May 2003; revised January 2008</p> <p><i>Software/Hardware Support Policy</i> first adopted in May 2002</p> <p><u>Titles of Change Management SOPs</u> IM001: SOP Initiate – Request for Change (RFC) – January 1, 2009</p>

Appendix One: Security Indicators

Categories	Security Indicators	ICES Response
		<p>IM002: SOP Approve – Request for Change (RFC) – January 1, 2009</p> <p>IM003: SOP Implement – Request for Change (RFC) – September 17, 2008</p> <p>IM004: SOP Evaluate – Request for Change (RFC) – September 17, 2008</p>
	<p>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.</p>	<p><i>Appropriate Use of Computer Equipment Policy</i> - revised June 2009</p> <p><i>Confidentiality & Security of Data Policy</i> - revised August 2009</p> <p>ICES does not log word changes to policies as previously mentioned.</p> <p>See Appendix FOUR: Table of Deficiencies</p>
	<p>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.</p>	<p><i>Business Continuity Policy</i> first adopted October 2010</p> <p><i>Review and maintenance of System Controls and Audit Logs Policy</i> first adopted November 2010</p> <p><i>Privacy and Security Audit Policy</i> first adopted in October 2010</p> <p><i>Review of Privacy and Security Policy, Procedures and Practices</i> first adopted</p>

Appendix One: Security Indicators

Categories	Security Indicators	ICES Response
		<p>August 2008; revised November 2010</p> <p><i>Ongoing Privacy and Security Training Policy</i> first adopted December 2010</p> <p><i>ICES Queens LAN Audit Policy and Procedure</i> first adopted March 2008</p> <p><i>Security Monitoring of Web Database Application Response Plan – ICD Registry</i> first adopted February 2007; revised February 2007; revised February 2010</p> <p><i>Alternate Data Centre Policy</i> first adopted September 2010</p> <p><i>Incident Management Policy</i> first adopted September 2010</p> <p><i>ICES Asset Management Program - Information and Physical Assets Classification and Handling Procedures –</i> first adopted June 2009; revised September 2010</p>
	<p>The dates that each amended 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.</p>	<p>ICES teams are small and communication is continuous and ongoing. Dates of posting not tracked; posting is done quickly to ICES intranet as well as verbal communication within role groups by Managers/Directors.</p> <p>See Appendix FOUR: Table of Deficiencies</p>

Appendix One: Security Indicators

Categories	Security Indicators	ICES Response
	<p>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.</p>	<p>Dates of posting are not tracked when posted on the intranet (insideices.on.ca), available to all Agents and through special authorized accounts.</p>
<p>Physical Security</p>	<p>The dates of audits of Agents granted approved to access the premises and locations within the premises where records of PHI are retained since the prior review by the IPC and for each audit:</p> <ul style="list-style-type: none"> – 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. 	<p>Logs audited every six months by CPO, CISO, Manager IT and Manager Administration (access UNIX, building, email)</p> <p>No recommendations: validation of appropriate removal of Agents who have resigned and Agent access is correct.</p> <p>Formal secure area network (SAN) Audits every year; LAN audits every three years. These findings are presented in a table in Part 2, section 16.</p> <p>Audit findings are presented annually to the IPC (CISO / Security Lead to IPC Senior Security Analyst) and included in logs maintained.¹⁵⁶ AS ICES is one organization with all sites working on data on centralized servers, consistent and across-the-organization reporting is provided in audit reports.</p> <p>Mitigation and/or remediation disclosed at those presentations, and included in the logs.</p>

¹⁵⁶ ICES Information Asset Management Program – restricted process information

Appendix One: Security Indicators

Categories	Security Indicators	ICES Response
		<p>See table in Report Part 2, section 16. Moving entirely from Marlok system to card access with anti-passback capacity: installation Summer 2011, functionality anticipated Fall 2011. Access coding of cards remains current to ICES policy.</p>
<p>Security Audit Program</p>	<p>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.</p> <p>Please note: spreadsheet logs of all audits are maintained which incorporate dates, third party reviewers, scope, findings, and remediation.</p>	<p>June 1, 2011 = ICES-Central LAN users, Fortress VPN Users, Sharepoint Users logs May 25, 2011= ICES-Central Marlok logs, UNIX user logs May 17, 2011 = ICES@uOttawa security review (policies) May 13, 2011 = ICES@uOttawa security review(policies) Feb 1 - March 18, 2010 = ICES Central Security Assessment March 13, 2010 = ICES@uOttawa security review October 30, 2010 = ICES@uOttawa physical security review April 3, 2009 = ARM Application (Primary Data collection servers) Security Assessment April 3, 2009 = HOBIC Application Security Assessment</p>

Appendix One: Security Indicators

Categories	Security Indicators	ICES Response
		<p>Change management process used; remediation noted in master logs. ICES' <i>Information Asset Management System (IAMS)</i>....."restricted" classification. Presented to the IPC Senior Security Analyst by Agents/ CISO/Security Lead</p> <p>April 3, 2009 = ICES Central Security Assessment</p> <p>See table in Report Part 2, section 16 for recommendations and remediation.</p>
	<p>The number and a list of security audits completed since the prior review by the IPC and for each audit:</p> <ul style="list-style-type: none"> - 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. 	<p>Two (f2009/2010 and 2010/2011)</p> <p>ICES has a routine pattern of the CISO reporting the findings of audits to the <u>Senior Security Lead</u> at the IPC as they are executed and completed. The log may be inspected on-site by the IPC as desired.</p> <p>ICES' Change Management processes used as described in Part 2.</p>
<p>Information Security Breaches</p>	<p>The number of notifications of information security breaches or suspected information security breaches received by the prescribed entity since the prior review by the IPC.</p>	<p>NONE</p>

Appendix One: Security Indicators

Categories	Security Indicators	ICES Response
	<p>With respect to each information security breach or suspected information security breach:</p> <ul style="list-style-type: none"> – 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 health information custodians 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 <p>The manner in which each recommendation was addressed or is proposed to be addressed.</p>	<p>NONE</p>

Human Resources Indicators

Part 3 – Human Resources Indicators

Categories	Human Resources Indicators	ICES Response
<p>Privacy Training and Awareness</p>	<p>The number of Agents who have received initial privacy/security orientation since the prior review by the IPC.</p>	<p><u>ICES Central</u> 2008 - 86 2009 - 109 2010 - 103 2011 – 86 (as of June 12, 2011)</p> <p><u>ICES@uOttawa</u> F2009/10 – 38 F2010/11 – 42</p> <p><u>ICES@Queen’s</u> 2008 = 11 2009 = 20 2010 = 17 2011 = 11</p> <p>Additionally, <u>sites in development</u> <u>ICES @uToronto</u> - 2 <u>ICES@Western</u> - 5</p> <p>All individuals received orientation at all sites: policy requirement</p>

Appendix One: Human Resources Indicators

Categories	Human Resources Indicators	ICES Response
	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.	NONE All sites report that all staff have received privacy/security orientation
	The number of Agents who have attended and who have not attended ongoing privacy training each year since the prior review by the IPC.	All employees receive the variety of training modalities and messaging described on the third page of this section in an ongoing fashion. See Part 3, Section 1, pp 116 in the report for details.
	The dates and number of communications to Agents by the prescribed entity in relation to privacy since the prior review by the IPC and a brief description of each communication. ICES does not create separate brief descriptions of training or communications. See Appendix FOUR: Table of Deficiencies	# CISO emails = 9 # CPO emails = 9 E-Newsletters = 4 Training decks = 4 Survey = 1
Security Training and Awareness	The number of Agents who have received and initial security/privacy orientation since the prior review by the IPC.	<u>ICES Central</u> 2008 - 86 2009 - 109 2010 - 103; 11 data covenantors 2011 – 86 (as of June 12, 2011) <u>ICES-uOttawa</u> F2009/10 – 38 F2010/11 - 42 <u>ICES@Queen’s</u> 2008 = 11

Appendix One: Human Resources Indicators

Categories	Human Resources Indicators	ICES Response
		2009 = 20 2010 = 17; 1 data covenantor 2011 = 11 Additionally, sites in development <u>ICES @uToronto</u> – 2 <u>ICES@Western</u> - 5 All scientists, employees and students received orientation at all sites
	The date of commencement of the employment, contractual or other relationship for Agents that have yet to receive initial security/privacy orientation and the scheduled date of the initial security orientation.	NONE All sites report that all Agents have received privacy/security orientation
	The number of Agents who have attended security/privacy training each year since the prior review by the IPC.	All Agents receive the variety of training modalities and messaging described in HR, Part 3, section 1. in an ongoing fashion. See Appendix FOUR: Table of Deficiencies
	The dates and number of communications to Agents by the prescribed \ entity in relation to information security since the prior review by the IPC. ICES, does not create separate brief descriptions of training or communications. See Appendix FOUR: Table of Deficiencies	# CISO emails = 9 # CPO emails = 9 E-Newsletters = 4 Training decks = 4 Survey = 1

Appendix One: Human Resources Indicators

Categories	Human Resources Indicators	ICES Response
	<p>The number of Agents who have executed Confidentiality Agreements each year since the prior review by the IPC.</p>	<p><u>ICES Central</u> 2008 = 478 + 10 Data Covenanters 2009 = 501 + 10 Data Covenanters 2010 = 476 + 11 Data Covenanters 2011 = 481 + 10 Data Covenanters</p> <p><u>ICES@Queen's</u> 2008 = 69 2009 = 129 2010 = 104 2011 = 11</p> <p><u>ICES@uOttawa</u> F2009/10 – 38 (as of December 17, 2010) F2010/11 –</p> <p>Additionally, sites in development <u>ICES @uToronto</u> – 2 <u>ICES@Western</u> – 5</p>
	<p>The date of commencement of employment, contractual or other relationship for Agents that have yet to execute the Confidentiality Agreement and the date by which the Confidentiality Agreement must be executed.</p>	<p>NONE Not Applicable as <u>no access to ICES</u> without signing Confidentiality Agreement annually. Dates of agreements tracked in logs</p>

Appendix One: Human Resources Indicators

Categories	Human Resources Indicators	ICES Response
Termination or Cessation	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 prescribed entity.	2008 36 Agents (staff = 26, Scientists = 0, Students = 10) 2009 34 Agents (staff = 22, Scientists = 0, Students = 12) 2010 24 Agents (Staff = 16, Scientists = 2, Students = 6) 2011 4 Agents (Staff = 4 [June 11], Scientists = 2, Students = 9)

Organizational Indicators

Part 4 – Organizational Indicators

Categories	Organizational Indicators	ICES Response
<p>Risk Management</p>	<p>The dates that the corporate risk register was reviewed by the prescribed entity since the prior review by the IPC.</p>	<p>Revisions related to twice-yearly Board Reporting 23 November 2010 15 July 2010 13 April 2010 27 April 2011 – revising risk reporting procedures</p> <p>Revisions related to twice-yearly Board Reporting 30 Nov 2009 26 Oct 2009 23 Oct 2009 16 Oct 2009 Sept 2009 20 July 2009 11 May 2009</p> <p>Process of Risk Assessment being developed/tested 31 Oct 2008 29 Oct 2008 24 Sept 2008 10 June 2008</p>

Appendix One: Organizational Indicators

Categories	Organizational Indicators	ICES Response
	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.	Amendments made: previous risk rating preserved + mitigation/mitigation revision on Register. This is internal information, not for public distribution. No privacy or security risk changes; new sites are doing separate assessments. ICES only tracks changes to the corporate risk register when reporting to the Board. See Appendix Four: Table of Deficiencies
Business Continuity and Disaster Recovery	The dates that the business continuity and disaster recovery plan was tested since the prior review by IPC.	Draft currently. Has not been completed as yet – completion anticipated in fiscal 2012/13 See Appendix Four: Table of Deficiencies
	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.	None made as testing not yet undertaken. See Appendix Four: Table of Deficiencies

Appendix Two: List of ICES Data Holdings Containing PHI

APPENDIX TWO: List of ICES Data Holdings Containing PHI:				page 152
Administrative/Health Services data (15):	Acronym	Source of the PHI/DSA authority	Years of Data	Statement of Purpose/Need for PHI in Relation to the Purpose
Continuing Care Reporting System	CCRS	MOHLTC	July 1996 - March 2010	To help understand the resources, staffing requirements, facilities required for complex continuing care in Ontario. As an example, CCRS contains information on physical, cognitive, behavioural, psychosocial diseases, health conditions, treatments and procedures which can be studied/evaluated to improve care.
Canadian Organ Replacement Register	CORR	CIHI	Ontario Donor ~ 1991-2008/2009 Recipient ~ 1981 - F2008/09	To understand organ replacement and renal care in Ontario. As an example, CORR contains information related to donor/recipient profile for specific organs; kidney, heart, liver, lung/heart-lung, enabling provision of resources, outcomes of care evaluation etc.
Client Profile Database	CPRO	Ontario Association of CCACs	2003 - 2009	To understand the waiting and demographic information for long term and home care: information in this database includes LTC home application/placement information which enables resource planning, staffing, etc.

Appendix Two: List of ICES Data Holdings Containing PHI

Discharge Abstract Database	DAD (CIHI)	MOHLTC and CIHI	April 1988 - March 2010	This database helps understand hospital performance: information facilitates creation of performance measures/indicators (length of stay, readmissions), quality of hospital care, transfers to and out of hospital to other environments, practice patterns; and diagnostic and procedural information can be used to create disease/procedure based population cohorts and estimate wait times, understand outcomes.
Home Care Database	HCD	MOHLTC	April 2001 - March 2010	The information found in this database helps understand the services provided by CCACs and their association with other medical services for Ontarians. Information can also be linked to other clinical datasets to provide a more complete picture of health care utilization. Aids in planning, resourcing.
National Ambulatory Care Reporting System	NACRS	MOHLTC	July 2000 - March 2010	This database contains information that enables understanding of ambulatory and emergency hospital performance, which helps create performance measures/indicators (length of stay, readmissions), quality of hospital care, transfers to and out of hospital to other environments, practice patterns; diagnostic and procedural information used to create disease. From this, procedure-based population cohorts are constructed to facilitate evaluation of things such as wait times and resource requirements.
National Rehabilitation System	NRS	MOHLTC	April 2000 - March 2010	This database contains information that helps evaluation of rehabilitation services in Ontario. As an example, NRS contains information on length of rehab after certain diagnoses such as cardiac surgery, orthopedic surgery (hip & knee), stroke rehabilitation, etc.

Appendix Two: List of ICES Data Holdings Containing PHI

Ontario Case Costing Initiative	OCCI	MOHLTC	April 2005 - March 2008	The information contained in this database facilitates evaluation of more detailed costing in a certain complement of hospitals (who are submitting such information to the MOHLTC). Enables resourcing.
Ontario Drug Benefit Claims	ODB	MOHLTC	April 1990 - September 2010	Enables understanding of the use of prescription drugs that are covered under Ontario's publicly funded drug program. Information in this database includes DINS, provides information on drugs used, number of prescriptions, provides information on intensity of drugs used, as examples. Enables planning and resourcing.
Ontario Health Insurance Plan Claims Database	OHIP	MOHLTC	July 1991 - September 2010	Used to evaluate the use of publicly-funded medical services in Ontario through the use of physician claims. For example, diagnostic information is linked with other data sets to develop disease-based cohorts; fee code is used to assess use of publicly funded treatments, physician practice variations; fee paid is used to examine costs of medical services and diagnostic testing in various settings
Ontario Mental Health Reporting System	OMHRS	MOHLTC	October 2005 - March 2010	The information in this database allows evaluation and understanding of inpatient health provision and functional status of persons in psychiatric units in Ontario hospitals, enabling resourcing and planning.

Appendix Two: List of ICES Data Holdings Containing PHI

Home Care Database, RAI-HC, Inter-RAI-CA		Ontario Association of CCAC	3 data sets: 1. Home Care Database from April 2005 to March 2010 2. RAI-HC 2006 to 2010; 3. Inter RAI-CA from April 2010 to Dec 2010	These combined datasets provide detailed information to better understand the use of home care services provided publicly and the functional status of persons requiring care within the system. Enables resourcing and planning.
Ontario Trauma Registry	OTR	MOHLTC	F2005 - 2009	The information in this database helps evaluate and understand the use of trauma injuries and services in Ontario to contribute to the reduction of injuries and related deaths in Ontario by identifying, describing and quantifying trauma. The evaluation of these data provides insights into injury-prevention and treatment programs needed thus enabling resourcing and planning.
Resident Assessment Instrument - Home Care	RAI-HC	MOHLTC	2005 - 2008/9	This database of slightly earlier information helps as well to understand the functional status of persons using long-term care or home care services. Enables resourcing and planning.
Vital Statistics Death Data	ORG Vital Stats	Office of the Registrar General	1990 - 2010	To understand the cause of death in the evaluation and monitoring of health services use in Ontario. The information in this database provides outcome information that contributes to understanding of complications, urgent/emergent care, etc.
Population & Demographics (4):	Acronym	Source of the PHI/DSA authority	Years of Data	Statement of Purpose/Need for PHI in Relation to the Purpose p.153

Appendix Two: List of ICES Data Holdings Containing PHI

Landed Immigrant Database - Ontario portion	CIC data	Citizenship and Immigration Canada	1985 - 2010	This database helps promote understanding of health system use in this population and helps evaluate system response, needs of this population, gaps in services -- enables planning and resourcing.
Client Agency Program Enrollment	CAPE	MOHLTC	January 2000 - June 2010	To understand the complement and characteristics and number of patients who are rostered to primary care physicians in new funding models. This information aids in estimations of Human Health Resources, access, effectiveness studies.
Best yearly postal code from eligible RPDB	PSTLYEAR	Created at ICES using Stats Canada postal code conversion file (public access file) and other linked data	1990-2010	Received from Statistics Canada; relates small geographic regions, including postal code up to LHINs; no PHI
Corporate Provider Database	CPDB	MOHTLC	to June 2010	To understand the composition and characteristics of physicians registered by the college of physicians: no PHI
Registered Persons Database file	RPDB	MOHTLC; modified at ICES	April 1990 - September 2010	This database is used to de-identify PHI (create the IKN, age, area of residence) and to determine best date of death/transfer/eligibility for health care and births as flagged by new health card numbers
Acquired Cohorts / Registries (5):	Acronym	Source of the PHI/DSA authority	Years of Data	Statement of Purpose/Need for PHI in Relation to the Purpose
Cardiac Care Network data	CCN	Cardiac Care Network	1991-2008	The information in this database helps to evaluate the use of medical/surgical care for persons who were treated through a Cardiac Care Treatment Network

Appendix Two: List of ICES Data Holdings Containing PHI

Ontario Cervical Screening Database	Cytobase	Cancer Care Ontario	1999 to 2009	This database helps to understand the use and medical care of women participating in the Ontario Cervical Screening Program (Pap smear tests and results). Enables planning, resourcing, and in understanding access/uptake.
Ontario Breast Screening Program	OBSP	Cancer Care Ontario	1990-2008	To evaluate the use of medical care for women who have had a mammogram funded through the Ontario Breast Screening Program. Enables planning, resourcing, and in understanding access/uptake.
Ontario Cancer Registry	OCR	Cancer Care Ontario	Incidence 1964-2009	The information in the database aids in evaluation of the use of medical care for people who have had cancer, as defined through the Cancer Care Ontario's Ontario Cancer Registry
Registry of the Canadian Stroke Network	RCSN	Registry of the Canadian Stroke Network	July 2003 - March 2004	The information in this database can be used to evaluate the use of medical care for persons in Ontario who have had a stroke, as defined through the Registry of the Canadian Stroke Network and the Ontario Stroke Registry. The information allows planning and resource activities, but also provides information to improve stroke care and outcomes.
Surveys (4):	Acronym	Owner/Data sharing agreement authority	Years of Data	Statement of Purpose/Need for PHI in Relation to the Purpose
Canadian Community Health Survey	CCHS	MOHLTC	2001-2008 unlinked & linked data	This consent-based database potentiates understanding of self-reported determinants of health. Consent-permitted linkage with actual health service enables study of resources related to well-being or diminished health status; can be used only through permission of MOHLTC
Primary Care Access Survey	PCAS	MOHLTC	January 2006 - June 2010	Population-based survey information collected by the MOHLTC to evaluate satisfaction to primary care access in Ontario. This information facilitates understanding of access issues, enables planning and resourcing

Appendix Two: List of ICES Data Holdings Containing PHI

	Acronym	Owner/Data sharing agreement authority	Years of Data	Statement of Purpose/Need for PHI in Relation to the Purpose
Surveys (4):				
National Population Health Survey (no longer used)	NPHS	MOHLTC	1994; 1996	Population-based survey facilitates understanding of self-reported determinants of health; similar to the CCHS Database as far as information available. Can be used only through permission of MOHLTC
Ontario Health Survey (no longer used)	OHS	MOHLTC	1990; 1996	Population-based survey facilitates understanding of self-reported determinants of health; similar to the CCHS Database as far as information available. Can be used only through permission of MOHLTC

Appendix Three: Recommendation Table

Summary of Recommendations	Text Recommendations	Addressed (indicate ✓)	Assigned To	Date Completed
breaches.	<p>It is unclear <u>why this recommendation is limited to external information breaches.</u></p> <p>An internal information breach may nonetheless <u>require amendments to policies and procedures in order to prevent a similar information breach in future</u> and therefore it is recommended that the <i>Information Breach Policy</i> be amended accordingly.</p>	<p>✓ Revised</p> <p>✓ Policy and form amended</p>		17 May 10
<p>2 Develop and implement a written policy and procedure with respect to the de-identification and anonymization of personal health information.</p> <p><i>The policy should relate to day-to-day de-identification and anonymization procedures.</i></p> <p><i>A description of de-identification “in the field” (unique number and separated table used in primary data collection</i></p>	<p>It is also recommended that ICES develop and implement a policy and procedure with respect to the de-identification and anonymization of personal health information in order to clarify and ensure consistency as to the meaning ascribed by ICES to the terms “de-identified information” and “anonymized information,” and in order to clarify and ensure consistency in the process for de-identifying and anonymizing personal health information.</p> <p>In particular, the policy and procedure should define the terms “de-identified information” and “anonymized information” and should clarify the distinction between these terms. It should also identify the information that must be removed, encrypted and/or truncated in order to de-identify</p>	<p>✓ Pre-existing algorithm 1994</p> <p>Data integration FAQ Don deBoer</p> <p>Data linkage: how do we do it? Karey Iron</p> <p>✓ <i>Linkage of Records of Personal Health Information</i></p>	<p>Don DeBoer Kathy Sykora Karey Iron</p> <p>Don DeBoer Kathy Sykora</p>	<p>23 June 10</p> <p>October 10</p> <p>Summer 10</p>

Appendix Three: Recommendation Table

Summary of Recommendations	Text Recommendations	Addressed (indicate √)	Assigned To	Date Completed
<p><i>studies) should be written (SOP).</i></p> <p><i>A separate description of de-identification/ anonymization procedures in cd-link should be prepared as well (SOPs).</i></p>	<p>personal health information and the information that must be removed, encrypted and/or truncated in order to anonymize personal health information. The policy and procedure should also identify those responsible for de-identifying and anonymizing personal health information.</p> <p>It is also recommended that ICES explore new tools that are being developed to assist in the development of de-identification policies and procedures in order to ensure that these policies and procedures are based on an assessment of the actual risk of re-identification.</p>	<p>standard</p> <p><i>Building Databases for primary Data Collection with laptops standard</i></p> <p><i>Data-sharing Agreement template</i></p> <p><i>Data covenantor confidentiality agreement</i></p> <p>√ <i>cd-link data de-identification SOP</i></p>	<p>Terri Swabey Annette Robertson</p> <p>Don DeBoer Nelson Chong Derek Browne Kathy Sykora Dr. Craig Earle Dr. Khaled El-Emam</p>	<p>1 Feb 10</p>
<p>3 Amend the information made available to the public and stakeholders to:</p>	<p>It appears that the public and other stakeholders may not clearly understand the purpose for which ICES collects personal health information and the purposes for which ICES may use personal health</p>	<p>√</p>	<p>Susan Shiller with input from Pam Slaughter</p>	<p>Spring 10</p>

Appendix Three: Recommendation Table

Summary of Recommendations	Text Recommendations	Addressed (indicate ✓)	Assigned To	Date Completed
<p>(a) Clearly set out the purposes for which ICES, as a prescribed entity under section 45 of the <i>Act</i>, collects and uses personal health information, the statutory authority for such collection and uses and the policies, procedures and practices and the applicable statutory requirements related to the collection and uses of the personal health information;</p> <p>(b) Discuss the “Pan-Ontario ICES” initiative and the consequences of this initiative on the privacy and security policies, procedures and practices of ICES; and</p> <p>(c) Ensure that it continues to be accurate in light of the “Pan-Ontario ICES” initiative.</p>	<p>information under the <i>Act</i> and its regulation.</p> <p>It is therefore recommended that the information made available to the public and stakeholders be amended to clearly set out the purposes for which ICES, as a prescribed entity under section 45 of the <i>Act</i>, collects and uses personal health information, the statutory authority for such collection and uses and the policies, procedures and practices and the applicable statutory requirements related to the collection and uses of the personal health information.</p> <p>In addition, the information currently made available to the public and stakeholders does not reflect the fact that while ICES remains a single organization, ICES is now geographically located at two sites with further sites currently being contemplated as a result of the “Pan-Ontario ICES” initiative.</p>	<p>On website as well as in <i>ICES Privacy Code</i></p> <p><i>Linked to websites for both ICES@Queen’s and for ICES@uOttawa</i></p> <p><i>Updated in 2011 Review document</i></p>		<p>Spring 10</p> <p>Spring 10</p>

Appendix Three: Recommendation Table

Summary of Recommendations	Text Recommendations	Addressed (indicate √)	Assigned To	Date Completed
<p>4 Amend the <i>Ethics Review Process Policy</i> to set out when and in what circumstances research ethics board approval is required and when and in what circumstances the research ethics board approval must be project-specific and when and in what circumstances the approval may be an expedited approval or a modified expedited approval.</p>	<p>ICES only uses de-identified information. Personal health information is de-identified by persons known as Data Covenantors. Data Covenantors have access to personal health information for purposes of removing personal identifiers, for purposes of inserting an encrypted identifier and for purposes of record linkage.</p> <p>Prior to the use of personal health information for research purposes, ICES requires that a research plan be prepared and that the research plan be approved by a research ethics board in accordance with the <i>Act</i> and its regulation.</p>	<p>√</p>	<p>Don DeBoer Jan Richards</p>	
	<p>It is recommended that the <i>Ethics Review Process Policy</i> be amended to make explicit that ICES requires research ethics board approval prior to the use of personal health information for research purposes pursuant to the <i>Act</i> and its regulation, and for the use of personal health information for the purpose described in section 45(1) of the <i>Act</i>, regardless of the fact that the personal health information is de-identified prior to use.</p>	<p>√ ICES does not use PHI for research purposes</p>	<p>Pam Slaughter Sue Powell Annette Robertson</p>	
<p>5 Refine its policies, procedures and practices relating to the secure destruction of records of personal health</p>	<p>It is recommended however, that the agreement between ICES and the third-party service provider be amended to ensure consistency with Order HO-001 and with the provisions set out in <i>Fact Sheet 10: Secure Destruction of Personal Information</i>,</p>	<p>√ <i>Sunnybrook-ICES Contract</i> Iron Mountain is</p>	<p>Don DeBoer Lucy Gerry</p>	<p>Winter 2008 Investigated</p>

Appendix Three: Recommendation Table

Summary of Recommendations	Text Recommendations	Addressed (indicate ✓)	Assigned To	Date Completed
<p>information, including:</p> <p>(a) Amending the agreement with the third-party service provider retained to securely destroy records of personal health information in accordance with Order HO-001 and <i>Fact Sheet 10: Secure Destruction of Personal Information</i> issued by the IPC;</p> <p>(b) Amending the <i>Data Destruction Policy</i> pursuant to the comments in this report;</p> <p>(c) Implementing a process to require that the date of destruction and the date of termination in the <i>Data Agreement Log</i> and the <i>Primary Data Collection Tracking Log</i> be completed prior to the collection of personal</p>	<p>issued by the IPC.</p> <p>In particular, it is recommended that the agreement be amended to explicitly state that the third- party service provider shall destroy the records of personal health information in a secure manner, to provide a definition of secure destruction consistent with subsection 1(5.1) of Regulation 329/04 to the <i>Act</i> and to specify the manner in which personal health information will be securely destroyed, including under what conditions and by whom. The agreement should also require the third-party service provider to provide a certificate of destruction setting out the date, time, location and method of secure destruction employed and bearing the signature of the person who performed the secure destruction and to require the third-party service provider to agree that:</p> <ul style="list-style-type: none"> ▪ Its services will be performed in a professional manner, in accordance with industry standards and practices and by properly trained employees and agents; ▪ Its employees and agents understand that a breach of the security and confidentiality of the information may lead to disciplinary measures; and 	<p>still in place – MOHLTC vendor of record and previously IPC reviewed/ approved</p> <p><i>SOP: Destruction of 3rd Party Health Data</i></p> <p><i>Data Destruction Policy</i></p>	<p>Don DeBoer Stella Desouza</p> <p>Don DeBoer Stella Desouza Lucy Gerry</p>	<p>July 10</p> <p>July 10</p>

Appendix Three: Recommendation Table

Summary of Recommendations	Text Recommendations	Addressed (indicate ✓)	Assigned To	Date Completed
<p>the <i>Act</i>, from whom ICES collects personal health information, in accordance with the comments provided in this report.</p>	<p>date of termination in the <i>Data Agreement Log</i> and the <i>Primary Data Collection Tracking Log</i> are completed by the project manager prior to the collection of personal health information by ICES. It is also recommended that the <i>Data Agreement Log</i> and <i>Primary Data Collection Tracking Log</i> be amended to include a column entitled “Actual Date of Destruction” to record the date that the information was actually destroyed in accordance with the <i>Data Sharing Agreements</i> and in accordance with the research plans approved by the research ethics boards</p>	<p><i>Destruction Policy</i></p> <p><i>Certificate of Data Destruction</i></p>		<p>Revised July 10</p>
	<p>It is recommended that the template <i>Data Sharing Agreement</i> be amended to clearly set out the purpose for which ICES is collecting the personal health information, the statutory authority for this collection and the statutory conditions, if any, that apply to the collection of the personal health information.</p>	<p>✓</p>	<p>John Wilkinson</p>	<p>Dec 09</p>
	<p>For example, in the <i>Data Sharing Agreement</i> with the Canadian Stroke Network it states that the Canadian Stroke Network is a health information custodian. However, the Canadian Stroke Network in respect of the Registry of the Canadian Stroke Network is a prescribed person pursuant to subsection 39(1)(c) of the <i>Act</i>.</p>	<p>X</p> <p>RCSN staff initiated/drafted this change but did not send forward for signatures as planning</p>	<p>Annette Robertson Melissa Stamplecoski</p>	<p>Spring 09 ongoing</p>

Appendix Three: Recommendation Table

	Summary of Recommendations	Text Recommendations	Addressed (indicate √)	Assigned To	Date Completed
			incomplete as to whether registry status was planned to be revoked		
		To require ICES to provide a certificate of destruction setting out the setting out the date, time, location and method of secure destruction employed and bearing the signature of the person who performed the secure destruction.	√	Lucy Gerry Don DeBoer Stella Desouza	Revised summer 10
		It is also recommended that the provisions in the template <i>Data Sharing Agreement</i> that restrict ICES from contacting the individual to whom the personal health information relates and from using and disclosing personal health information in a form in which the individual can be identified unless ICES has received the prior written authority of the “data custodian,” be amended to further restrict the contact, use or disclosure, as the case may be, to circumstances where the contact, use or disclosure is permitted by law.	√	John Wilkinson	Winter 09 and revised August 10
7	Develop and maintain a consolidated and centralized log of all	Currently, the Senior Web Developer and the Manager of Information Systems each maintain their own log of recommendations arising from	√ Logs consolidated into	Derek Browne Jan Richards J-R Kidston	Summer 10

Appendix Three: Recommendation Table

Summary of Recommendations	Text Recommendations	Addressed (indicate ✓)	Assigned To	Date Completed
<p>recommendations arising from privacy impact assessments, penetration testing, vulnerability assessments, threat-risk assessments, security assessments and security reviews.</p>	<p>penetration testing, vulnerability assessments, threat-risk assessments, security assessments and security reviews and the Chief Privacy Officer maintains her own log of recommendations arising from privacy impact assessments.</p> <p>It is recommended that ICES develop and maintain a consolidated and centralized log of all recommendations arising from privacy impact assessments, penetration testing, vulnerability assessments, threat-risk assessments, security assessments and security reviews. This consolidated and centralized log should be updated regularly and should set out how each recommendation was addressed, when each recommendation was addressed and by whom the recommendation was addressed. For those recommendations that have yet to be addressed, it is recommended that the log set out how each recommendation will be addressed, the date by which each recommendation will be addressed and who is responsible for addressing each recommendation.</p>	<p>shared library and mashed spreadsheet document when possible</p>	<p>Pam Slaughter Stella Desouza</p>	

Appendix Four: Deficiencies to be Addressed/Timelines

Appendix Four: Deficiencies to be Addressed/Timelines					
General Deficiency: ICES has always noted month/year of development or modification on policies, SOPs, practices, procedures, standards, guidelines and logs, but does not track the extensive detail requested in the Manual. We will build in going forward for institution/completion for 2014 review. Please note that new policies developed are listed in the indicators table below with dates noted. They are also noted in the Indicators appendix.					
Section of Manual	Noted Deficiency	Required change or documentation	Agents/ Director/designate responsible for execution	Resourced?	Anticipated completion date
Part 1: Privacy Policy Review Section 2	Unable to review all policies annually	ICES is currently restructuring, reorganizing and is resource challenged. Policies, practices and SOPs scanned for deficiencies but no formal process currently due to constraints.	Chief Privacy Officer and staff	To be determined	F2011/12
Part 1: Policy and Procedures for Statements of Purpose for Data Holdings	ICES does not have such a policy.	A document stating how ICES uses data holdings is included in Appendix TWO of this document and is being posted on the website. Draft this document as best possible using Manual, with assistance from IPC.	Health Information Officer and Director, Health Information	Not required	F2011/12
Part 1: Review and Approval Process-Limiting Agent Access Section 8	ICES does not have a policy laying out Manual requirements to Abstractor access.	ICES must review the Manual to decide on reconciliation of the documentation that is already in place: Abstractors hired, MRNs used, dates of use, training of Abstractors and their	Manager, HR Director, Information Management Lead, Primary Data Collection	Not required	F2011/12

Appendix Four: Deficiencies to be Addressed/Timelines

Appendix Four: Deficiencies to be Addressed/Timelines					
		signing of Confidentiality Agreements			
Part 1: Policy and Procedures for Disclosure of PHI Section 13	Develop policies and procedures for disclosures of de-identified information for research purposes	ICES now being approached to disclose de-identified information for research purposes using a variety of approaches (see document Part I, number 13 for information). ICES, is currently restructuring and reorganizing and will work to develop this line of work. New research agreement drafted. Policies will build on usual processes.	Chief Privacy Officer and staff	To be determined	F2011/12
Part 1: Privacy Section 20	ICES does not have a <u>standardized template Research Agreement</u> . These are drafted to fit the circumstances of the project, usually in the DSA.	ICES follow its <i>Sourcing and Procurement Policy</i> for third party agreements and its <i>template data-sharing agreement</i> for projects. Any additional requirements related to the project are included as schedules to the data-sharing agreement. Have few requests for this type of agreement: ICES work aligns more with DSAs, but request level is going up.	Sourcing and Procurement Office Chief Privacy Officer (DSAs) Chief Privacy Officer, Sourcing and Procurement Office	To be determined	F2011/12
Part 1: Privacy	ICES does not have a	ICES treats SysPIAs as “living”	Health	To be	F2013/14

Appendix Four: Deficiencies to be Addressed/Timelines

Appendix Four: Deficiencies to be Addressed/Timelines					
Section 25	requirement to review completed Systematic PIAs (SPIAs)	documents, equipped with change management tables so that as issues related to these documents arise, they are summarized, assigned, completed. Will continue this approach but more documentation related to changes.	Information Officer, CISO and Chief Privacy Officer (others as required)	determined	
Part 1: Privacy Sections 27 & 28	ICES does perform LAN audits at ICES Central, ICES@Queens. These audits have been automated and are also verified manually.	Needs to implement at the newest ICES site @uOttawa. Logs will include recommendations, date addressed or to be address and how.	Chief Privacy Officer	None required	F2011/12 LAN audit for this year will be verified in August 11
Part 1: Privacy Section 31	ICES does not have a policy specific to privacy complaints	ICES has a blended policy related to complaints, inquiries and concerns about compliance. Missing policy requirement will be amended	Chief Privacy Officer and staff	None required	F2011/12
Part 1: Privacy Section 33	ICES does not have a policy specific to privacy inquiries	ICES has a blended policy related to complaints, inquiries and concerns about compliance. Missing policy requirements will be amended	Chief Privacy Officer and staff	None required	F2011/12
Part 2: Security Policy Review Section 2	Unable to review all policies annually	ICES is currently restructuring, reorganizing and is resource challenged. Policies, practices and	Chief Information Security Officer and Security Lead	To be determined	F2011/12

Appendix Four: Deficiencies to be Addressed/Timelines

Appendix Four: Deficiencies to be Addressed/Timelines					
		SOPs scanned for deficiencies but no formal process currently due to constraints. Need to meet documentation standards as found in Manual related to changes to policy instruments	Chief Information Security Officer and Security Lead	To be determined	F2011/12
Part 2: Security Policy Communication	ICES doesn't track communication dates of new policies. The content is posted on our intranet. The records themselves could be retrieved and maintained by the internal webmaster	Will request this type of tracking related to dates and content of new policies communicated to staff.	Chief Information Security Officer and Security Lead	None required	F2011/12
Part 2: Security -- System Control and Audit	ICES does track physical and system security findings and recommendations within spreadsheets	We track types of audits, dates executed, remediation required related to recommendations and when executed. We have a new Change Management system and processes to enable	Chief Information Security Officer and Security Lead	To be determined	F2001/12
Part 3: Human Resources	ICES needs more formal, standardized approaches for routine annual	The Privacy Office is working with the Manager HR and staff to develop more approaches to routine re-training	Chief Privacy Officer and the Manager HR	To be determined	F2011/13

Appendix Four: Deficiencies to be Addressed/Timelines

Appendix Four: Deficiencies to be Addressed/Timelines					
	retraining of Agents				
Part 3: Human Resources	ICES does not track communication dates and content. The records themselves are maintained	Director Communications will be asked for additional suggestions other than public posting and presentation of privacy/ security communications.	To be determined	To be determined	F2011/13
Part 4. Organizational: Risk Management	The risk register is amended for twice-annual presentation to the Board. Previous ratings are part of the register to show changes provoked by mitigation. These amendments are only tracked/ changes noted when reporting to the Board.	Descriptive documentation of amendments is not currently part of register presentation format. This process is being revised to improve register. Annual reporting being considered. Privacy, E-Security and Physical Security Risk Assessments have been made standard for Expansion sites	Chair, Risk Committee Project Manager, Expansion Sites	None required None required	To be implemented Spring 2012 Implemented F2009
Part 4. Organizational: Business Continuity and Disaster Recovery	Only three of five planned components of the BCP have been considered with the assistance of Deloitte /Touche:	More work is needed on business impact analysis (BIA) and continuity risk assessment (ties into item above) Components 3, 4 and 5 to be completed: Recovery, strategies	ICES is assembling an internal Task Force in F2011 to review recommendations and created a final plan for approval by ICES' Executive	Approvals will be sought to complete	F2011 - F2013

Appendix Four: Deficiencies to be Addressed/Timelines

Appendix Four: Deficiencies to be Addressed/Timelines					
	current state assessment; business impact analysis (BIA); and continuity risk assessment;	development; and, the development of recovery plans and procedures.	and Board – then will go ahead with this work.		
Part 4. Organizational: Business Continuity and Disaster Recovery	Testing of the BCP and Disaster Recovery Plan	To be completed when Components 4 and 5 are completed and ready for testing: recovery strategies and the development of recovery plans and procedures. Off ICES-grid backup server functional F2011 and site inspected by IPC senior security staff	ICES is assembling an internal Task Force in F2011 to review recommendations and created a final plan for approval by ICES' Executive and Board.	Approvals will be sought to complete	F2011 - 2013
Indicators: Newly-developed privacy and/or security policies, procedures and SOPs since last approval Awaiting final re-structuring information for final approval process					
General Privacy Policies, Procedures and Practices:					
Ongoing Privacy and Security Training Policy first adopted December 2010					
Business Continuity Policy first adopted October 2010					
Review and Approval of Project Submissions: PIA, PAW, Proposal first adopted October 2010					
Review of Privacy and Security Policy, Procedures and Practices first adopted August 2008; revised November 2010					
Review and Maintenance of System Controls and Audit Logs Policy first adopted November 2010					
Privacy and Security Audit Policy first adopted in October 2010					
Maintaining a Log of Recommendations first adopted May 2010					
Policy and Procedures for Privacy Complaints (amend)					
Policy and procedures for Privacy Inquiries (amend)					
ICES Information Breach Policy first issued June 2004; revised October 2005; January 2008; November 2008; May 2010; June 2011					
Indicators: Newly-developed privacy and/or security policies, procedures and SOPs since last approval (Approval has been granted)					
Confidentiality & Security of Data Policy first adopted January 1999; revised October 2005, January 2008, August 2009					
Appropriate Use of Computer Equipment Policy first adopted in May 2002; revised June 2009					

Appendix Four: Deficiencies to be Addressed/Timelines

Appendix Four: Deficiencies to be Addressed/Timelines
General Improvements Needed in Indicators
Prepare brief descriptions of all amendments made to privacy policy instruments, dates, reason why and by whom; communication to staff dates and modality.
Prepare brief descriptions of all amendments made to security policy instruments, dates, reason why and by whom; communication to staff dates and modality.
The number and list of data linkages of de-identified data must be tracked and reported; these are already logged
Physical Security audits must report a brief description of the indicators required are date, brief description of each recommendation, how addressed, by whom.
Security Audits must report a brief description of the type of audit, the recommendation made, how addressed and by whom.
Dates and the type of communication to staff, brief description of what is communicated, to be tracked.
Data holdings of PHI and statements of purpose have been drafted
Audit of those who have access to PHI (Agent/Data Covenantors)

Appendix Five: Registry of the Canadian Stroke Network

Canadian Stroke Network

The Canadian Stroke Network (CSN) – one of Canada’s *Networks of Centres of Excellence* – is a unique collaborative effort bringing together scientists, students, government, industry and the non-profit sector¹⁵⁷. Currently, the Network has more than 100 scientists at 24 universities across the country. The CSN, which began in 1999 with \$4.7 million in seed funding from the federal government, is a not-for-profit corporation, governed by a Board of Directors and headquartered at the University of Ottawa. Since the inception, the CSN has been granted two seven year cycles of funding from the Networks of Centres of Excellence, which will sunset in 2013.

CSN has been highly successful in creating the Registry of the Canadian Stroke Network (RCSN) and in effectively studying the delivery and outcomes of stroke care in Ontario, with the ultimate aim of optimizing stroke care in Ontario and elsewhere through its published evaluations.

Registry of the Canadian Stroke Network

The RCSN has been functioning as a *prescribed person* within the meaning of subsection 39(1)(c) of PHIPA. Its designation as a prescribed registry under PHIPA has allowed RCSN to collect Personal Health Information (PHI) through chart abstraction without consent. RCSN is also tailored to monitor the effectiveness of the Ontario Stroke Network (OSN), in partnership with the Ministry of Health and Long Term Care (MOHLTC). Under the umbrella of its prescribed registry status, the RCSN has been able to collect data efficiently and effectively on a wider range of stroke patients using the Ontario Stroke Audit (OSA) and *Stroke Performance Indicators for Reporting Improvement and Translation* (SPIRIT) applications.

PHI has been collected for the following defined purposes:

- To monitor and evaluate the quality of stroke care delivery in participating hospitals in Canada across the stroke continuum of care;
- To monitor and evaluate the performance of the Ontario Stroke System across the stroke continuum of care;
- To provide feedback to Ontario institutions, to the Ontario Stroke System Evaluation Advisory Committee and to the Ontario Ministry of Health and Long- Term Care on the quality of stroke care delivery and on the performance of the Ontario Stroke System in each region and Local Integrated Health Network (LHIN);
- To investigate and propose testable solutions to health and social issues related to stroke;

¹⁵⁷ Source: RCSN website accessed June 3, 2010; www.canadianstrokenetwork.ca/eng/about/registry.php

Appendix Five: Registry of the Canadian Stroke Network

- To decrease the functional, economic and social consequences of stroke on the individual, the healthcare system and society;
- To facilitate or contribute to the effectiveness, quality, equity, and efficiency of stroke health care;
- To carry out health services research in areas of clinical relevance from a population-wide perspective in accordance with the provisions of PHIPA and its regulation;
- To document national and provincial patterns of stroke care; and
- To develop and disseminate information for use by patients, practitioners, clinician-managers, administrators, policymakers and the general public about stroke.

Currently, this health information is transferred to and resides securely at ICES in Toronto, where it is used for statistical and evaluative purposes which contribute to the effectiveness, quality, equity and efficiency of health care and health services in Ontario. All data are de-identified with health card numbers encrypted as per ICES' standards to protect the privacy interests of individuals. Through data-sharing agreements, unlinked de-identified stroke information has been used by the RCSN for research purposes.

The RCSN centralized office is housed at ICES and receives in-kind support of its activities including privacy, security and IT support.

The Databases

The historical database (2001-2009 Stroke data related to the "early years") and the Ontario Stroke Audit (OSA) databases of RCSN are housed on an isolated, secure server at ICES that can only be accessed by ICES' Agents within the building.

The RCSN has three active databases:

- 1 OSA: a retrospective random sampling of approximately 20% of stroke patients arriving at acute care hospitals; the data is collected annually via a retrospective chart audit process. The OSA is housed on a dedicated server at ICES.
- 2 SPIRIT Acute: web-based prospective data collection at nine regional stroke centers and to enhanced district stroke centers. The SPIRIT database is being moved from its previous location at an ESP located in Ottawa;
- 3 SPIRIT Secondary Prevention Centers (SPC): web-based prospective data collection at approximately 20 stroke secondary prevention clinics.

Data collected via the web-based SPIRIT (Secondary Prevention) Clinics and SPIRIT Acute are housed with TrialStat/Jubilant:Clinsys, an Electronic Services Provider (ESP) located in Ottawa. The contract with this ESP expires on August 31, 2011. Presently, ICES is developing a web-based data collection application for collecting, transferring and storing SPIRIT data.

Appendix Five: Registry of the Canadian Stroke Network

The RCSN also maintains a website, www.rcsn.org, which will be linked to the ICES website pending redesign.

Next Steps

As the funding currently in place for CSN/RCSN will cease in 2013, and given the importance of the registry in providing high quality information related to stroke care in Ontario to clinicians and the MOHLTC, the Principals of the CSN/RCSN have approached ICES to assume the RCSN under its' section 45 Prescribed Entity status as one of its clinical registries to continue that legacy.

The CSN will end its association with the RCSN; a regulation will be made under the Regulation to PHIPA to revoke the status of the CSN as a prescribed person in respect of the RCSN prior to October 31, 2011, the date that the IPC is required to approve the practices and procedures of ICES and CSN in respect of the RCSN.

ICES has received a letter from Alison Blair, Director of the Information Strategy and Policy Branch at the MOHLTC, dated February 25, 2011 stating that January 2012 is the target date for public revocation of their prescribed status in the Regulation (attached).

ICES presented a project charter and migration strategy to the MOHLTC, IPC and CSN and entered into agreements with CSN to move all RCSN-related data to ICES by 31 August 2011. ICES is presently in the process of building a new web-based data collection application to replace the TrialStat data collection tool.

A crosswalk table has been prepared outlining the existing CSN policies and procedures and the corresponding ICES policies and procedures which provides a clear statement of congruency and also identifies the policy deficiencies (policies under development regarding the functionality of the new web-based data collection application presently being built by ICES to replace the TrialStat application).

The complexity of the migration project has many details on which the Agents of CSN, RCSN and ICES are working collaboratively to ensure a successful transition. All RCSN databases will reside at ICES by the completion of the migration activities. By August 31, 2011, the SPIRIT data will be transferred from TrialStat to ICES and be accompanied by a letter of data destruction from TrialStat (ICES needs to be satisfied that all the data has been transferred successfully). A Privacy Impact Assessment (PIA) is being executed related to the movement of data and integration into ICES.

This detailed procedure for migrating the RCSN data to ICES has been documented. Once the migration has been completed, the RCSN will no longer have prescribed status and will be required to comply with all ICES' policies and policy instruments to collect, use and disclose personal health information, as regulated by ICES Section 45 prescribed status of PHIPA.

Appendix Five: Registry of the Canadian Stroke Network

Update: the following activities have been accomplished OR are being planned as part of the preparation for migration of the RCSN to ICES:

a)	Discussions related to the acceptability of this plan with the IPC and the MOHLTC	COMPLETE February 25, 2011 letter signed
b)	Discussion of the procedure to rescind prescribed registry status with the MOHLTC and the IPC	February 25, 2011 letter signed - MOH request update mid-October 2011
c)	Development of a Letter of Intent, which has been signed by both CSN and ICES	COMPLETE September 9, 2010 signed Letter of Intent
d)	Meeting with a representative of TrialStat/Jubilant:Clinsys to discuss potential migration strategies	Data collection at the Regional Stroke sites is being closed out on a site-by-site basis; confirmation of data completeness is being verified; a procedure to transfer data to ICES has been implemented; request for a data destruction document from TrialStat (once all data has been received at ICES)
e)	Development of a comprehensive Project Charter, which has been agreed upon and signed by both CSN and ICES	COMPLETE January 5, 2011 email confirmation
f)	Planning a Privacy Impact Assessment exercise pre-migration	In progress
g)	Development of a mutually-acceptable budget for the activities related to this migration	COMPLETE January 5, 2011 email confirmation
h)	Independent third party Security Assessment of the related databases and their current status (initiated 4 January 2011)	COMPLETE: awaiting final letter
i)	ICES' Review of the 2008 IPC Review of the RCSN and all CSN/RCSN-related contracts to clarify current status and understand current needs for remediation and/or amendment	Submitted to IPC in the January 10, 2011 report
j)	Review and revision of all policies, procedures and practices to identify differences and align with those of ICES	In progress – crosswalk table – identify existing CSN policies with corresponding ICES policies and identifying deficiencies (which are in progress)
k)	Development of a secure web-based data collection tool by	Presently in progress at

Appendix Five: Registry of the Canadian Stroke Network

	ICES Application Developers (approved by CSN & to be developed by late Summer 2011)	ICES
l)	Discussion with the Principals of the legacy use of the data by scientists	Discussions underway with RCSN Investigators & ICES Program Scientific Lead
m)	Re-branding of the Registry	To be decided by CSN and RCSN
n)	Developing concordance for statistical/evaluative and health services research projects with ICES' standards	Discussions underway with RCSN Investigators & ICES
o)	Developing a Communication Plan outlining the brand change and all new related processes for both RCSN and ICES stakeholders	To be developed by CSN and ICES Communication departments
p)	ICES' website improvements to reflect the changes for both ICES and RCSN	www.rcsn.org – online - need to incorporate into ICES website – discussions underway with ICES Director, Communication

The OSN will collect stroke data in their biennial province-wide Ontario Stroke Audit using encrypted laptop computers with specialized secure data entry application.

The OSA data collection application has undergone a security assessment by an independent third party (Security Compass). Initial testing began January 4, 2011. The initial draft report was delivered on January 12, 2011; ICES began remediation of issues in mid-January. Validation of the remediation testing started January 26th and we are presently awaiting the letter from ICES Security Lead.

The SPIRIT web-based data collection (both SPIRIT Acute and SPIRIT Secondary Prevention Clinics) is now an ICES Application Development work project; development of this new application has begun and ICES is anticipating that the SPIRIT data collection application will be ready for use by August 2011.

Attachments:

1. Letter from Alison Blair, Director of the Information Strategy and Policy Branch, MOHLTC, dated February 25, 2011

**Migration activities are continuing between ICES and RCSN.
Further communication with the IPC will be necessary prior to October 31, 2011.**

An updated status report will be submitted to the IPC by September 30, 2011.

Appendix Five: Registry of the Canadian Stroke Network

Ministry of Health and Long-Term
Care

Health System Information
Management and Investment Division

Information Management Strategy &
Policy Branch

1075 Bay Street, 13th Floor
Toronto ON M5S 2B1
Tel.: 416 212-4433
Fax: 416 314-6731

Ministère de la Santé et des Soins de
longue durée

Division de la gestion de l'information et de
l'investissement pour le système de santé

Direction des stratégies et des politiques de
gestion de l'information

1075, rue Bay, 13e étage
Toronto ON M5S 2B1
Tél. : 416 212-4433
Télééc. : 416 314-6731



FEB 25 2011

Ms. Pam Slaughter
Chief Privacy Officer
Institute for Clinical Evaluative Sciences
G Wing, 2075 Bayview Avenue
Toronto ON M4N 3M5

Dear Ms. Slaughter: *Pam*

RE : Target date for revoking prescribed registry status of Canadian Stroke Network

Thank you for your February 10, 2011 email to Joe Racz concerning the preferred date for revoking the prescribed registry status of the Canadian Stroke Network (CSN).

As indicated in your email, the Institute for Clinical Evaluative Sciences (ICES) and the Canadian Stroke Network group have selected January 1, 2012 as the target date for revocation of CSN's prescribed registry status. The concerned parties believe this date maximizes the opportunity for the secure migration of the registry database to ICES and the successful execution of transition of authority under PHIPA.

The ministry will aim to have the registry's prescribed status revoked by this date. However, timing is dependent on Cabinet scheduling, which the ministry cannot control.

To help the ministry with its work planning for the revocation, we would appreciate it if you could provide us an update on the progress of the registry transitioning in mid-October 2011.

Sincerely,

A handwritten signature in red ink, appearing to read "Alison Blair".

Alison Blair
Director

Appendix Six: Affidavit

Appendix Six [Appendix “D” Requirement]

AFFDAVIT OF DR. DAVID A. HENRY, PRESIDENT AND CHIEF EXECUTIVE OFFICER OF THE INSTITUTE FOR CLINICAL EVALUATIVE SCIENCES (ICES)

I, Dr. David A. Henry, of the City of Toronto, in the Province of Ontario, MAKE OATH AND SAY:

1. I am the President and Chief Executive Officer of THE INSTITUTE FOR CLINICAL EVALUATIVE SCIENCES and have submitted a written report (the “Report”).
2. During the period covered by the Report, THE INSTITUTE FOR CLINICAL EVALUATIVE SCIENCES’ PRESIDENT AND CHIEF EXECUTIVE OFFICER formally delegated the supervision and management of day-to-day operations of the privacy portfolio to Pamela M. Slaughter, Chief Privacy Officer; and also formally delegated the supervision and management of day-to-day operations of the IT security portfolio to and Derek J. Browne, Chief Information Security Officer.
3. THE INSTITUTE FOR CLINICAL EVALUATIVE SCIENCES has in place privacy and security policies, procedures, protocols, practices, standards, tools, guidelines and other instruments (“Privacy and Security Policies”) to protect the privacy of the individuals whose personal health information it receives and to maintain the confidentiality of that information.
4. THE INSTITUTE FOR CLINICAL EVALUATIVE SCIENCES has submitted the 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*, as issued by the Information and Privacy Commissioner of Ontario on April 19, 2010.

