CIHI Submission

2020 Prescribed Entity Review

The Canadian Institute for Health Information Report to the Information and Privacy Commissioner of Ontario — Three-Year Review as a Prescribed Entity under PHIPA, October 2020

Canadian Institute for Health Information
Institut canadien d'information sur la santé

Table of Contents

CANADIAN INSTITUTE FOR HEALTH INFORMATION

Introduction

The Canadian Institute for Health Information ("CIHI") is an independent, not-for-profit, pan-Canadian organization whose mandate, as agreed to by the federal, provincial and territorial Ministers of health, is to deliver comparable and actionable information to accelerate improvements in health care, health systems performance and population health across the continuum. In order to support its national mandate, CIHI has offices located in Ottawa and Toronto in addition to regional offices in Victoria and Montreal.

Background

The *Personal Health Information Protection Act, 2004* (the Act) came into effect on November 1, 2004. The Information and Privacy Commissioner of Ontario (IPC/ON) has been designated as the oversight body responsible for ensuring compliance with the Act. The Act establishes rules for the collection, use and disclosure of personal health information by health information custodians that protect the confidentiality of, and the privacy of individuals with respect to, that personal health information. In particular, the Act provides that health information custodians may only collect, use and disclose personal health information with the consent of the individual to whom the personal health information relates or as permitted or required by the Act.

Subsection 45(1) of the Act permits health information custodians to disclose personal health information 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 subsection 45(3).

Subsection 45(3) of the Act requires each prescribed entity to have in place practices and procedures to protect the privacy of individuals whose personal health information it receives and to maintain the confidentiality of that information. Subsection 45(3) further requires each prescribed entity to ensure that these practices and procedures are approved by the IPC/ON in order for health information custodians to be able to disclose personal health information to the prescribed entity without consent and for the prescribed entity to:

- be able to collect personal health information from health information custodians;
- use personal health information as if it were a health information custodian for the purposes of paragraph 37(1)(j) and subsection 37(3) of the Act;
- disclose personal health information as if it were a health information custodian for the purposes of sections 44, 45 and 47 of the Act;
- disclose personal health information back to health information custodians who provided the personal health information; and
- disclose personal health information to governmental institutions of Ontario or Canada as if it were a health information custodian for the purposes of section 43(1) (h).

CIHI was first recognized as a prescribed entity on October 31, 2005 and, following a second statutory review by the IPC/ON, CIHI had its status renewed on October 31, 2008. While satisfied that CIHI had practices and procedures in place that sufficiently protected the privacy of individuals whose personal health information it received, in both instances the IPC/ON did make certain recommendations to further enhance these practices and procedures. The recommendations made during the 2005 and 2008 reviews to enhance CIHI's privacy and security program have all been addressed by CIHI. CIHI's prescribed entity status was again renewed effective October 31, 2011. The IPC/ON's review resulted in only one recommendation to further enhance the practices and procedures of CIHI and the other prescribed entities in Ontario. The recommendation was to prohibit the transfer, by way of courier or regular mail, of records containing personal health information. CIHI was already in compliance with this recommendation. Coming out of the 2014 review process, the practices and procedures of CIHI were approved for a further three-year period. The review by the IPC/ON resulted in two recommendations to further enhance the information practices and procedures of CIHI relating to the annual review of its policies and procedures and to the categorization and tracking of security incidents and breaches.

In 2017, the IPC/ON recommended that, at a minimum, all the privacy policies, procedures and practices put in place by CIHI, be reviewed by CIHI at least once prior to each scheduled review of these policies, procedures and practices by the IPC/ON pursuant to section 45(4) of the *Act.* This is a lessening of the previous requirement set out in the *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities* (the IPC/ON Manual) that required a review of policies and procedures at a minimum on an annual basis.

Subsection 18(2) of Regulation 329/04 to the Act further requires each prescribed entity to make publicly available a plain language description of its functions. This includes a summary of the practices and procedures to protect the privacy of individuals whose personal health information it receives and to maintain the confidentiality of that information.

In addition, subsection 18(7) of Regulation 329/04 to the Act permits CIHI to disclose personal health information to a person outside Ontario where the disclosure is for the purpose of health planning or health administration; the information relates to health care provided in Ontario to a person who is a resident of another province or territory of Canada; and the disclosure is made to the government of that province or territory.

Review Process

Subsection 45(4) of the Act requires that the practices and procedures implemented by CIHI to protect the privacy of individuals whose personal health information it received and to protect the confidentiality of that information must be reviewed by the IPC/ON every three years. Subsection 45(4) of the Act also requires that such approvals be in place in order for a health information custodian to be able to continue to disclose personal health information to CIHI and for CIHI to be able to continue to collect, use and disclose personal health information as permitted by the *Act* and its regulation.

For the 2011 renewal process, the IPC/ON prepared the IPC/ON Manual which set out in detail the requirements imposed on such entities and outlined the new review process to be followed. This Report is an update to CIHI's 2017 prescribed entity review submission and reflects any changes that have been made to CIHI's privacy and security program in the intervening period.

Throughout the IPC/ON Manual, prescribed entities are asked to comment on overall compliance and audit processes across a span of corporate-wide activities. CIHI has chosen to address this here. At CIHI, all agents[1] are expected to comply with the terms and conditions of all CIHI policy instruments. Compliance is enforced through various means depending on the policy itself. For example, the President and CEO, via the Director of Human Resources and Administration, is responsible for ensuring compliance with CIHI's *Code of Business Conduct* (the Code).

CIHI implemented the Code in 2010. It describes the ethical and professional behaviour related to work relationships, information, including personal health information, and the workplace. In particular, the Code spells out the general obligations imposed on CIHI agents around the rules of use and disclosure of personal health information. This includes obligations to comply with all privacy and security policies and procedures. The Code applies to members of CIHI's Board of Directors and its staff. Similar obligations are contained in third-party agreements that are used to retain external consultants or third-party service providers.

The Code requires all individuals to comply with the Code and all CIHI's policies, protocols and procedures. Violations of the Code may result in disciplinary action up to and including termination of employment. All agents are responsible for reporting actual, potential or suspected violations of the Code to their immediate supervisor/manager. Agents, on a biennial basis, are required to reaffirm that they have read and will comply with the terms of the Code. The Code is distributed to each new agent upon commencement of his or her employment. Moreover, compliance with CIHI's privacy and security programs is monitored in various ways. The goal of CIHI's Privacy Audit Program is to ensure compliance with its statutory privacy requirements, contractual obligations and privacy policies and procedures. The Privacy Audit Program is also designed to ensure that external third parties who enter into an agreement with CIHI meet their contractual obligations. CIHI has developed criteria to be used in the selection of privacy audit activities based on risk factors set out in a multi-year audit plan.

In addition to CIHI's Privacy Audit program, CIHI's Information Security Audit program is designed to assess the following:

- Compliance with information security policies, standards, guidelines and procedures,
- Technical compliance of information processing systems with best practices and published architectural and security standards,
- Inappropriate use of information processing systems,

[1] For purposes of this report and review, the term "agent" is used to describe CIHI staff, external consultants or other third-party service providers who access and use personal health information, on a need-to-know basis, when required to perform their duties and/or services.

- Inappropriate access to information or information processing systems,
- Security posture of CIHI's technical infrastructure, including networks, servers, firewalls, software and applications, and
- CIHI's ability to safeguard against threats to its information and information processing systems.

Instances of non-compliance with privacy and security policies are managed through the *Privacy and Security Incident Management Protocol* and referred to Human Resources as appropriate.

This report, especially with regard to the Indicators, covers the period from November 1, 2016 up to and including October 31, 2019. The following is CIHI's submission.

Part 1 - Privacy Documentation

General Privacy Policies, Procedures and Practices

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

Home to 30+ data holdings, 20 of which contain personal health information and/or de-identified data, (see CIHI's Products and Services Guide), CIHI continues its tradition of delivering unbiased, credible and comparable health information. CIHI has developed, therefore, an overarching privacy policy that sets out its commitment to protect the privacy of individuals whose personal health information it receives. This commitment is at the core of all of CIHI's practices and informs CIHI's actions and decisions at all levels of the organization. The *Privacy and Security Framework, 2010*, is the backbone of CIHI's overall privacy program which also includes CIHI's *Privacy Policy on the Collection, Use, Disclosure and Retention of Personal Health Information and De-Identified Data (Privacy Policy, 2010)*, and other privacy specific policies, procedures and protocols.

Status under the Act

Section 45 of the Act allows health information custodians to disclose personal health information to prescribed entities and authorizes prescribed entities to collect personal health information for the purposes of analysis or the compiling of statistical information for the planning and management of a health system.

CIHI's *Privacy Policy, 2010*, Part 1: Introduction / Commitment to Privacy and Security makes specific reference to CIHI's status as a prescribed entity under PHIPA and the duties and responsibilities that arise as a resuly of this status, in particular, that CIHI has implemented policies, procedures and practices to protect the privacy of individuals whose personal information it receives and to maintain the confidentiality of that information, and to adhere to the provisions of PHIPA and its regulation applicable to prescribed entities. It also identifies that these policies, practices and procedures are subject to review by the IPC/ON every three yearsand that this report forms part of that review process.

CIHI's *Privacy and Security Framework, 2010* also sets out CIHI's status as a prescribed entity under section 45 of the Act and is designed to enable the effective integration and coordination of CIHI's privacy and security policies. The Framework states clearly that CIHI maintains a comprehensive suite of privacy and information security policies, procedures, standards and guidelines. These policy instruments inform all information practices within the organization. As well, CIHI has a comprehensive set of privacy and information security standards, procedures and protocols to support the goals in the policies; examples include those on secure information life cycle, incident management and acceptable use of information systems.

Privacy and Security Accountability Framework

CIHI recognizes the vital importance of a clear accountability framework to ensure compliance with its own privacy and security policies, practices and procedures, as well as with the Act and its regulation. Accountability must start at the top of the organization and therefore CIHI's *Privacy and Security Framework, 2010*, clearly indicates that the President and Chief Executive

Officer 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 Chief Privacy Officer and the Chief Information Security Officer, respectively. The duties and functions of the key privacy and security roles and committees are clearly articulated in section 2 of CIHI's *Privacy and Security Framework, 2010*.

Finally, both the Framework and *CIHI's Privacy Policy, 2010*, clearly state that CIHI remains responsible for the personal health information used by its agents. More specifically, CIHI policies, procedures and practices ensure that its agents only collect, use, disclose, retain and dispose of personal health information in compliance with the Act and its regulation and in compliance with CIHI's privacy and security programs.

Collection of Personal Health Information

Entities prescribed under section 45 of the Act are permitted to collect personal health information that is disclosed to them 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.

CIHI's *Privacy Policy, 2010*, outlines the policies, procedures and practices it has implemented to ensure that both the amount and the type of personal health information collected is limited to that which is reasonably necessary for its purpose.

Section 1 of CIHI's *Privacy Policy, 2010*, identifies the purposes for which personal health information is collected, the types of personal health information collected and the persons or organizations from which personal health information is typically collected.

These identified purposes are all consistent with the Act and its regulation. Further, section 2 of the *Privacy Policy, 2010*, articulates CIHI's commitment not to collect personal health information if other information will serve the purpose and not to collect more personal health information than is reasonably necessary to meet the purpose.

Use of Personal Health Information

CIHI ensures that all access to and use of the personal health information in its data holdings is consistent with the Act and its regulation. Specifically, Sections 1 and 2 of CIHI's *Privacy Policy, 2010*, identify the purposes for which CIHI uses personal health information, all of which are consistent with the uses of personal health information permitted by the Act and its regulation. Further, section 3 of CIHI's *Privacy Policy, 2010*, articulates CIHI's commitment not to use personal health information if other information, such as de-identified and/or aggregate information, will serve the purpose and not to use more personal health information than is reasonably necessary to meet the purpose.

Section 10 of CIHI's *Privacy Policy, 2010*, clearly sets out that access to personal health information by CIHI's agents is limited to a "need-to-know" basis when required to perform their duties and/or services.

The related *Privacy Policy Procedures* set out the following specific requirements:

(1) prohibit staff from using de-identified and/or aggregate information, either alone or with other information, to identify an individual including attempting to decrypt information that is encrypted, attempting to identify an individual based on unencrypted information and attempting to identify an individual based on prior knowledge (section 3.1);

(2) prohibit staff from accessing and using personal health information, if other levels of information such as de-identified and/or aggregate information will serve the identified purpose (section10.1); and

(3) prohibit staff from accessing and using more personal health information than is reasonably necessary to meet the identified purpose (section 10.2).

Section 7 of CIHI's *Privacy Policy, 2010*, states that CIHI uses personal health information and de-identified data in a manner consistent with its mandate and core functions, and in compliance with all applicable legislation, including privacy legislation. Access to personal health information by CIHI's agents is granted only after they have met the mandatory privacy and security education requirements. This mandatory education requirement extends to certain external consultants and other third-party service providers as set out in section 12 of CIHI's *Privacy Policy, 2010*, where these individuals require access to CIHI data or information systems in order to perform their duties or services. CIHI has segregated the roles and responsibilities of agents, where feasible and possible, based on a need-to-know principle, to avoid a concentration of privileges.

When signing-on to a CIHI information system, agents must confirm, prior to each log-on attempt, their understanding that they may not access or use the computer system without CIHI's express prior authority or in excess of that authority.

CIHI does not use personal health information for research purposes as contemplated by paragraph 37(1)(j) of the Act nor does CIHI use aggregate or de-identified data for research purposes. In keeping with its mandate and core functions, CIHI only uses personal health information, de-identified data and aggregate data for statistical analysis and reporting purposes. Analyses are undertaken to support decision-making for stakeholders such as Health Canada, Statistics Canada and ministries of health and health system managers. Section 7.1 of CIHI's *Privacy Policy Procedures* specifically prohibits the use of personal health information, de-identified and/or aggregate data for research purposes.

Disclosure of Personal Health Information

The *Act* permits a prescribed entity to disclose personal health information for research purposes in compliance with section 44 of the *Act*, to another prescribed entity for planning and management of the health system in compliance with section 45 of the *Act* and to a health data institute in compliance with section 47 of the *Act*. Permissible disclosures also include disclosures to prescribed persons for purposes of facilitating or improving the provision of health care pursuant to section 39(1)(c) of the *Act* and subsection 18(4) of the regulation. The Act and

its regulation further permit a prescribed entity to disclose personal health information back to health information custodians who provided the personal health information and to disclose personal health information to governmental institutions of Ontario or Canada as if it were a health information custodian for purposes of paragraph 43(1)(h), if permitted or required by law. The disclosure of personal health information back to the health information custodian that provided the personal health information must not contain additional identifying information as required pursuant to subsection 18(45 of the regulation.

In addition, subsection 18(7) of Regulation 329/04 to the Act permits CIHI to disclose personal health information to a person outside Ontario where the disclosure is for the purpose of health planning or health administration; the information relates to health care provided in Ontario to a person who is a resident of another province or territory of Canada; and the disclosure is made to the government of that province or territory.

CIHI's *Privacy Policy, 2010*, clearly distinguishes between (1) the purposes for which and the circumstances in which personal health information is disclosed and (2) the circumstances in which and the purposes for which de-identified and/or aggregate information is disclosed.

Sections 40 - 44 of CIHI's *Privacy Policy, 2010*, set out clear rules for the disclosure of personal health information and the requirements that must be satisfied prior to such disclosures, including the purposes for which and the circumstances in which personal health information is disclosed, to whom such disclosures are typically made and the statutory or other requirements that must be satisfied prior to such disclosures. The *Privacy Policy Procedures* further require that agents must consult with Privacy and Legal Services prior to disclosing personal health information. Privacy and Legal Services will review the proposed disclosure and all relevant documentation to ensure there is lawful authority. CIHI will not disclose personal health information if other information will serve the purpose and will not disclose more personal health information than is reasonably necessary to meet the purpose. As with collection and use, section 45 of CIHI's *Privacy Policy, 2010*, articulates its commitment not to disclose personal health information if and when aggregate or de-identified record-level data will serve the purpose. In all instances, CIHI is committed to only disclosing the amount of information that is reasonably necessary to meet the purpose. The *Policy* further identifies procedures to this end.

Sections 45 – 50 of CIHI's *Privacy Policy, 2010*, set out clear rules for the disclosure of de-identified data and the requirements that must be satisfied prior to such disclosures, including that data disclosures are made at the highest degree of anonymity possible, while still meeting the research and/or analytical purposes. This means that, whenever possible, data are aggregated. The associated *Privacy Policy Procedures* require program area staff to determine whether aggregate data is sufficient for the researcher to achieve the objectiv(s) of the research study and/or analytical purpose(s).

Further, section 51 states that, prior to disclosure, programs areas will evaluate the de-identified data to assess and subsequently minimize privacy risks of re-identification and residual disclosure, and to implement the necessary mitigating measures to manage residual risks.

Secure Retention, Transfer and Disposal of Records of Personal Health Information

Section 4 d. of CIHI's *Privacy and Security Framework, 2010,* addresses, at a high level, the secure retention of records in both paper and electronic form. It recognizes that information is only secure if it is secure throughout its entire lifecycle: creation and collection, access, retention and storage, use, disclosure and disposal. Accordingly, CIHI has a comprehensive suite of policies 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 the associated standards, guidelines and operating procedures reflect best practices in privacy, information security and records management for the protection of the confidentiality, integrity and availability of CIHI's information assets.

Section 3 of CIHI's *Privacy Policy, 2010*, states that, consistent with its mandate and core functions, CIHI may retain personal health information and de-identified data recorded in any way regardless of format or media, for as long as necessary to meet the identified purposes, with the exception of ad hoc linked data, which will be destroyed in a manner consistent with section 29 of the *Policy*.

The manner in which records of personal health information will be securely transferred and disposed of is detailed in CIHI's *Secure Information Transfer Standard* and the *Secure Destruction Policy* and the related *Secure Destruction Standard*.

Implementation of Administrative, Technical and Physical Safeguards

Section 4 d. of CIHI's *Privacy and Security Framework, 2010,* clearly states that CIHI has in place administrative, technical and physical safeguards to protect the privacy of individuals whose personal health information CIHI receives and to maintain the confidentiality of that personal health information, and references the suite of policies CIHI has implemented to this end. These safeguards include but are not limited to confidentiality agreements, encryption technologies, and physical access controls to CIHI premises in addition to various steps taken to protect personal health information against theft, loss and unauthorized use or disclosure and to protect records of personal health information against unauthorized copying, modification or disposal. Part 2 of this Report, entitled Security Documentation, outlines many of the safeguards implemented by CIHI.

Inquiries, Concerns or Complaints Related to Information Practices

Section 64 of CIHI's *Privacy Policy, 2010*, identifies the Chief Privacy Officer as the contact person to whom individuals can direct inquiries, concerns or complaints relating to CIHI's privacy policies, procedures and practices, as well as CIHI's compliance with the Act and its regulation. Contact information for the Chief Privacy Officer, including the mailing address, telephone number, fax number and email address, are included.

Section 65 of the Policy also specifies that the Chief Privacy Officer may direct an inquiry or complaint to the privacy commissioner of the appropriate jurisdiction, including to the IPC/ON, as the case may be. CIHI has posted on its website information specifically indicating how concerns and complaints are received, who receives them, and that individuals may alternatively contact the privacy commissioner of the jurisdiction in which the person making the

complaint resides to submit a complaint. A link to contact information for the IPC/ON as well as all other provincial/territorial privacy oversight bodies in Canada is included.

Transparency

Section 66 of CIHI's *Privacy Policy, 2010*, identifies that individuals may obtain further information in relation to CIHI's privacy policies, procedures and practices from the Chief Privacy Officer.

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

CIHI is committed to the ongoing review of its privacy policies, procedures and practices in order to determine whether any amendments are needed or whether new privacy policies, procedures and practices are required.

CIHI's *Privacy and Security Framework, 2010*, clearly sets out that the Chief Privacy Officer and the Chief Information Security Officer will assume the responsibility for coordinating the review of all privacy and security policies respectively and for ensuring that the suite of privacy and security policies and procedures is comprehensive, up to date and communicated to staff, the public and other stakeholders. CIHI undertakes to review all privacy policies and procedures at least once prior to their review by the IPC/ON pursuant to section 45(4) of the Act (that is, at least once every three years). As indicated in CIHI's *Privacy and Security Framework, 2010*, the CPO and/or the Chief Information Security Officer will ensure that the required approval process is followed. The Terms of Reference of CIHI's Privacy, Confidentiality and Security Committee include responsibility to review CIHI's privacy policies and protocols and to recommending changes as needed. A review schedule is included as part of the Privacy Policy Review Log. In the case of material changes to the *Privacy Policy, 2010*, approval from CIHI's Board of Directors is required. In other cases, the approval process and the extent of internal and external communication are dependent on the nature of the document and may require approval, for example, by the Executive Committee, Senior Management Committee or other internal committee.

In undertaking the review and determining whether amendments and/or new privacy policies, procedures and practices are necessary, the *Privacy and Security Framework, 2010*, indicates that updates or changes to CIHI's privacy policies, procedures and practices will take into consideration:

- Any orders, guidelines, fact sheets and best practices issued by the IPC/ON under the Act and its regulation;
- Evolving industry privacy standards and best practices;
- Amendments to the Act and its regulation relevant to the prescribed person or prescribed entity;
- Recommendations arising from privacy and security audits, privacy impact assessments and investigations into privacy complaints, privacy and security breaches or incidents;
- Whether the privacy policies, procedures and practices of the prescribed person or 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 Chief Privacy Officer and the Chief Information Security Officer are responsible to ensure that all privacy and security documents available on CIHI's public website (www.cihi.ca) are current and continue to be made available to the public and other stakeholders. As for internal communication to staff, the Chief Privacy Officer and the Chief Information Security Officer ensure that changes to policies, procedures and practices are communicated appropriately and may include targeted mandatory training. This is guided by the *Privacy and Security Training Policy* which clearly stipulates at section 6 that the Chief Privacy Officer and Chief Information Security Officer will be responsible for determining the content of privacy and security training. In addition to formal training, CIHI regularly engages in staff awareness activities such as presentations and email communications.

Compliance, Audit and Enforcement

The *Privacy and Security Framework, 2010*, sets out that CIHI's Code of Business Conduct describes the ethical and professional behaviour related to work relationships, information – including personal health information – and the workplace. The Code requires all employees to comply with the Code and all CIHI's policies, protocols and procedures. Compliance with CIHI's privacy and security program is monitored through CIHI's risk-based privacy audit program and information security audit program. Instances of non-compliance with privacy and security policies are managed through CIHI's *Privacy and Security Incident Management Protocol*. Violations of the Code are referred to Human Resources, as appropriate, and may result in disciplinary action up to and including dismissal.

Transparency

> Regulation 329/04, s. 18 (2) to the Act provides that an entity that is a prescribed entity for the purposes of subsection 45 (1) of the Act shall make publicly available a plain language description of the functions of the entity including a summary of the practices and procedures described in subsection 45 (3) of the Act.

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

CIHI's commitment to transparency and accessibility is prevalent throughout its key policy instruments. For example, section 2 b. of CIHI's *Privacy and Security Framework, 2010*, describes CIHI's commitment to the principle of openness and transparency, and describes the information to be made available to the public and other stakeholders relating to CIHI's privacy policies, practices and procedures, and identifies the means or media by which this information is made available.

The Framework sets out the documentation to be made available, including:

- information related to the privacy and security policies, procedures and practices implemented by CIHI;
- a description of CIHI's data holdings of personal health information;

- PIAs;
- Documentation related to the Information and Privacy Commissioner of Ontario's review of CIHI's privacy and information security practices; and
- Contact information for CIHI's Chief Privacy Officer and Chief Information Security Officer, to whom inquiries, concerns or complaints regarding compliance with the privacy and security policies, procedures practices implemented and regarding compliance with the Act and its regulation may be directed.

Information made available to the public also includes a description of CIHI's status as a prescribed entity under PHIPA, the duties and responsibilities arising from this status and the policies implemented, information related to the collection, use and disclosure of personal health information, and to some of the administrative, technical and physical safeguards implemented to protect the privacy of individuals whose personal health information is received and to maintain the confidentiality of that information.

The Privacy and Security page on CIHI's external website (www.cihi.ca) also contains the contact information of the Chief Privacy Officer for anyone having privacy questions, concerns or complaints. Individuals are also advised that they may direct complaints to the privacy commissioner of the jurisdiction in which they reside – links to the appropriate jurisdictional contact information are available. Specifically, with regard to Ontario, CIHI advises individuals that they may direct complaints regarding CIHI's compliance with Ontario's *Personal Health Information Protection Act* and its regulation to the IPC/ON – IPC/ON coordinates are provided on the Privacy and Security page.

Readers are also informed of CIHI's status as a prescribed entity under section 45(1) of PHIPA and the duties and responsibilities arising from this status, the review by the IPC/ON of our practices and procedures every three years and links to the related documentation.. Information is also made available related to CIHI's collection, use and disclosure of personal health information, and to some of the administrative, technical and physical safeguards implemented to protect the privacy of individuals whose personal health information is received and to maintain the confidentiality of that information. A link to the list of CIHI data holdings of personal health information is also included.

In addition, CIHI's *Privacy Impact Assessment Policy* requires that, once approved, the CPO make privacy impact assessments publicly available, including posting on the CIHI external website (www.cihi.ca) where and when appropriate to do so.

This comprehensive approach ensures that CIHI's status as a prescribed entity under the Act, the duties and responsibilities arising from this status and the privacy policies, procedures and practices implemented in respect of personal health information are accessible and available to the public.

Collection of Personal Health Information

Entities prescribed under section 45 of the Act are permitted to collect personal health information that is disclosed to them by health information 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 or part of the health system, including the delivery of services.

4. Policy and Procedures for the Collection of Personal Health Information

Sections 1 and 2 of CIHI's *Privacy Policy, 2010*, identify the purposes for which CIHI collects personal health information, the nature of the personal health information that is collected, and from whom the personal health information is typically collected.

The related *Privacy Policy Procedures* set out the criteria that must be considered for determining whether to approve the collection of personal health information, including that the collection is permitted by the Act and its regulation and that any and all conditions or restrictions set out in the Act and its regulation have been satisfied; that personal health information will be collected only where a determination has been made that de-identified and/or aggregate data will not serve the identified purpose; and no more personal health information is being requested than is reasonably necessary to meet the identified purpose.

Section 4 d. of CIHI's *Privacy and Security Framework, 2010*, articulates CIHI's commitment to the secure collection of personal health information, which is supported by a comprehensive suite of policies and procedures. More specifically, CIHI has developed a *Health Data Collection Standard* that offers options for the secure transmittal to CIHI of personal health information, based on industry best practices.

Review and Approval Process for Collection

Program area management establish data requirements with their relevant stakeholders, including minimum data sets. In many cases, external Advisory Committees comprising representatives from the data providing organizations and other key stakeholders provide advice and guidance on the development and implementation of the particular program. CIHI is committed at all times, as stated in sections 1 and 2 of CIHI's *Privacy Policy, 2010*, to minimal data collection.

The related *Privacy Policy Procedures* identify who is responsible for reviewing and determining whether to approve the collection of personal health information, the process that must be followed and the requirements that must be satisfied. The Procedures set out the criteria that must be considered for determining whether to approve the collection of personal health information, including that the collection is permitted by the Act and its regulation and that any and all conditions or restrictions set out in the Act and its regulation have been satisfied; that personal health information will be collected only where a determination has been made that de-identified and/or aggregate data will not serve the identified purpose; and no more personal health information is being requested than is reasonably necessary to meet the identified purpose. The Procedures also set out the manner in which the decision approving or denying the collection of personal health information and the reasons for the decision are documented, including any conditions or restrictions, and how the decision is communication and to whom.

Conditions or Retrictions on the Approval

The *Privacy Policy Procedures* related to new collections of personal health information set out the conditions or restrictions that are required to be satisfied prior to collection. This includes consultation with Privacy and Legal Services prior to collectoin to determine if the proposed data collections falls under an existing bilateral or data-sharing agreement or if an amendment to an existing agreement or a new agreement is required. Legal Services will draft the amendment or will lead the development of a new agreement. Decisions approving or denying new collections of personal health information must be communication in writing to the appropriate memaber of Senior Management and document the reasons for the decision, including any conditions or restrictions.

Secure Retention

Section 4 d. of CIHI's *Privacy and Security Framework, 2010*, articulates CIHI's commitment to the secure retention of personal health information, which is supported by a comprehensive suite of policies and procedures. Records of personal health information collected by CIHI are subject to all applicable CIHI privacy and security policies, protocols, standards, procedures and practices including CIHI's *Secure Information Storage Standard* which lays out the specific methods by which records of personal health information are to be securely stored, including records retained on various media.

Secure Transfer

As stated above, CIHI has developed a *Health Data Collection Standard* that offers options for the secure transmittal to CIHI of personal health information, based on best practices. The manner in which records of personal health information are disseminated is detailed in the *Secure Information Transfer Standard*.

Secure Return and Disposal

Section 6 of CIHI's *Privacy Policy, 2010*, states that, consistent with its mandate and core functions, CIHI may retain personal health information for as long as necessary to meet the identified purposes. At such time as personal health information is no longer required for CIHI's purposes, it is disposed of in compliance with CIHI's *Secure Destruction Policy* and the related *Secure Destruction Standard*. The *Secure Destruction Policy* sets out that the Chief Information Security Officer or his/her designate is responsible for developing and maintaining technical standards and processes for the secure destruction of electronic information, media and devices and ensuring that requirements for secure destruction are met. Secure destruction of electronic information, media and device must be completed by, or under the direction of, qualified staff from Information Technology and Services.

Compliance, Audit and Enforcement

The *Privacy Policy, 2010*, sets out that CIHI's Code of Business Conduct describes the ethical and professional behaviour related to work relationships, information – including personal health information – and the workplace. The Code requires all employees to comply with the Code and all CIHI's policies, protocols and procedures, including CIHI's *Privacy Policy, 2010*. Compliance with CIHI's privacy program is monitored through CIHI's risk-based privacy audit

program set out in a multi-year audit plan. Instances of non-compliance with privacy and security policies are managed through CIHI's *Privacy and Security Incident Management Protocol*. Violations of the Code are referred to Human Resources, as appropriate, and may result in disciplinary action up to and including dismissal.

5. List of Data Holdings Containing Personal Health Information

CIHI maintains an up-to date list of and brief description of its data holdings of personal health information. This may be found in the *Products and Services Guide* as well as in other documentation available on CIHI's external website (www.cihi.ca) relating to its collection activities. A more detailed description of the purpose of the data holding, the personal health information contained in the data holding, the sources(s) of the personal health information and the need for the personal health information in relation to the identified purpose is found in the Privacy Impact Assessments which have been completed for all databases containing personal health information.

6. Policy and Procedures for Statements of Purpose for Data Holdings Containing Personal Health Information

Sections 1 and 2 of CIHI's *Privacy Policy, 2010*, state the overall intended purposes of its data holdings, which are consistent with CIHI's pan-Canadian mandate to deliver comparable and actionable information to accelerate improvements in health care, health systems performance and population health across the continuum of care. For Ontario personal health information, CIHI's Data Privacy Agreement with the Ontario Ministry of Health and Long-Term Care acknowledges that CIHI may use the information for the purpose of analysis and compiling of 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, as permitted under section 45(5) of PHIPA. Any change to CIHI's mandate would trigger notification and could impact CIHI's status under the Federal *Not-For-Profit Corporations Act*, and could also impact the current arrangements under which CIHI obtains personal health information from the Ministry. Where CIHI collects personal health information from other organizations in Ontario, the intended purpose is set out in the data-sharing agreement governing the collection of those data and includes any requirements with respect to notice, etc.

The *Products and Services Guide* provides a description of all CIHI's data holdings, including the use(s) to which the data are put and is updated annually and published on CIHI's external website (www.cihi.ca). Data holding-specific purpose statements are clearly articulated in every Privacy Impact Assessment, which are updated regularly and made readily available on CIHI's external website (www.cihi.ca). Each privacy impact assessment has a front section entitled "Quick Facts about this Database". This particular synopsis was developed to give the general public a quick view and understanding of the data holding and its purpose, scope and usefulness. At CIHI, privacy impact assessments are a shared responsibility. Program area staff and Privacy and Legal Services collaborate to develop the PIA. All privacy impact assessments are reviewed and signed-off by both the Chief Privacy Officer and the relevant Vice-President or Executive Director. Directors are responsible for reviewing annually any

existing PIAs for discrepancies between their content and actual practices or processes, and for advising the CPO, and together determining if an update or a new PIA is required.

Compliance, Audit and Enforcement

CIHI's Code of Business Conduct describes the ethical and professional behaviour related to work relationships, information – including personal health information – and the workplace. The Code requires all employees to comply with the Code and all CIHI's policies, protocols and procedures. Compliance with CIHI's privacy program is monitored through CIHI's risk-based privacy audit program set out in a multi-year audit plan. Instances of non-compliance with privacy and security policies are managed through CIHI's *Privacy and Security Incident Management Protocol*. Violations of the Code are referred to Human Resources, as appropriate, and may result in disciplinary action up to and including dismissal.

7. Statements of Purpose for Data Holdings Containing Personal Health Information

Statements of purpose for all CIHI data holdings containing personal health information are routinely made available to the public through CIHI's external website (www.cihi.ca) and are addressed through the application of CIHI's *Privacy Impact Assessment Policy* and in CIHI's *Products and Services Guide*. The Privacy Impact Assessments include a more detailed description of the purpose of the data holding, the personal health information contained in the data holding, the sources(s) of the personal health information and the need for the personal health information in relation to the identified purpose is found in the Privacy Impact Assessments which have been completed for all databases containing personal health information.

Use of Personal Health Information

8. Policy and Procedures for Limiting Agent Access To and Use of Personal Health Information

CIHI ensures that all access to and use of the personal health information in its data holdings is consistent with the Act and its regulation.

Section 3 of CIHI's *Privacy Policy, 2010*, states that CIHI does not use personal health information if other information will serve the purpose and does not use more personal health information than is reasonably necessary to meet the purpose. Section 10 of CIHI's *Privacy Policy, 2010*, clearly sets out that access to personal health information by CIHI's agents is limited to a "need-to-know" basis when required to perform their duties and/or services.

The related *Privacy Policy Procedures* set out the following specific requirements:

(1) prohibit staff from using de-identified and/or aggregate information, either alone or with other information, to identify an individual including attempting to decrypt information that is encrypted, attempting to identify an individual based on unencrypted information and attempting to identify an individual based on prior knowledge (section 3.1);

(2) prohibit staff from accessing and using personal health information, if other levels of information such as de-identified and/or aggregate information will serve the identified purpose (section10.1); and

(3) prohibit staff from accessing and using more personal health information than is reasonably necessary to meet the identified purpose (section 10.2).

Section 7 of CIHI's *Privacy Policy, 2010*, states that CIHI uses personal health information and de-identified data in a manner consistent with its mandate and core functions, and in compliance with all applicable legislation, including privacy legislation. Access to personal health information by CIHI's agents is granted only after they have met the mandatory privacy and security education requirements. This mandatory education requirement extends to certain external consultants and other third-party service providers as set out in section 12 of CIHI's *Privacy Policy, 2010*, where these individuals require access to CIHI data or information systems in order to perform their duties or services. CIHI has segregated the roles and responsibilities of agents, where feasible and possible, based on a need-to-know principle, to avoid a concentration of privileges.

When signing-on to a CIHI information system, agents must confirm, prior to each log-on attempt, their understanding that they may not access or use the computer system without CIHI's express prior authority or in excess of that authority.

Data and Information Governance: Provisioning Access to Privacy Sensitive Variables

In 2019, as part of its internal data and information governance activities, CIHI examined its practices with respect to two privacy-sensitive variables, namely the six-digit postal code and full date of birth, and assessed them as constituting personal health information. In order to be compliant with its privacy policy requirements relating to the need-to-know and data minimization principles, and appropriate authorization approvals, CIHI undertook a review of access to those two privacy sensitive variables by agents.

Many CIHI analysts currently use the six-digit postal code and full date of birth solely to derive age and geographic variables needed for analysis. If those variables are pre-calculated on the analytic datasets, the two privacy-sensitive variables can be removed, minimizing access for most analytic users. This led CIHI to determine that the most feasible approach was to create General Use Data files -- analytical data files developed for use across the organization that meet the requirements for de-identified data by using consistently derived variables for geography and for age.

Work to create General Use Data files for CIHI datasets used for analysis and containing personal health information is underway and is expected to be completed by June 2020, with priority given to the most frequently accessed datasets. As of the end of October 2019, the transition over to General Use Data Files is complete for two datasets; is actively underway for three datasets including our two most highly used datasets -- the Discharge Abstract Database (DAD) and the National Ambulatory Care Reporting System (NACRS) due to be complete in

November 2019; and General Use Data Files for three other datasets are currently in development.

When operational access to privacy-sensitive variables is still required, for example, for purposes of client support, data processing, data quality or error correction, systems development work or testing, returns of own data or disclosures under data-sharing agreements, the required level of approval (i.e., Director-level approval) will be sought. An exceptional access process also exists to allow access to privacy-sensitive variables for analytical purposes (i.e., approval by the Privacy, Confidentiality and Security Committee) in addition to Director-level approval.

Review and Approval

Analysis at CIHI is generally conducted with the use of record-level data. In exceptional instances, Program Area staff will require access to personal health information in the form of original health card numbers or other privacy-sensitive variables such as postal code and date of birth. Section 10 of CIHI's *Privacy Policy Procedures* sets out strict controls to ensure access is approved at the appropriate level and in the appropriate circumstances, and that the principle of data minimization is adhered to at all times. The request and approval processes are documented in sections 10.1 to 10.17 of CIHI's *Privacy Policy Procedures*.

Specifically:

- Where Information Technology and Services (ITS) staff require ongoing access to personal health information, in the form of original health card numbers or other privacy-sensitive variables in order to perform their duties and/or services, approval from their ITS Manager is required.
- Where non-ITS staff require access to personal health information, for example, in the form of original health card numbers or other privacy-sensitive variables to fulfill an operational activity such as client support, data processing, data quality or error correction, systems development work or testing, returns of own data or disclosures under data-sharing agreements, approval is required from both the Director of the staff requesting access and the Director of the data holding/service to which access is being requested .
- For any staff requiring access to personal health information, for example, in the form of original health card numbers or other privacy-sensitive variables for analytical activities, approval from CIHI's Privacy, Confidentiality and Security Committee is also required.

Tracking Approved Access to and Use of Personal Health Information

Once approved, data access requests are documented and forwarded to ITS, whose responsibility it is to log and track access requests, grant agents with the appropriate level of access (i.e., "read-only"), prepare the necessary data files, and at the end of the access period, revoke access. Access is validated yearly as part of CIHI's ITS internal data access audit.

In some limited circumstances, personal health information may also be included in CIHI's secure online applications available to its data providers, and to CIHI agents on a need-to-know basis. In addition, a limited number of CIHI agents require access to initial data submission processes, which include the receipt, data quality verification or error correction, and for returns

of own data to data providers. Online applications/processes where personal health information exists are flagged, and director approvals are sought for staff requiring access to those applications/processes. All access to these online applications/processes is managed through CIHI's Access Management System and validated yearly.

CIHI has implemented a well-structured off-boarding process which is key to ensuring prompt and timely revocation of access privileges to CIHI's premises and networks, including CIHI's data holdings. As later described in Part 3 of this Report, CIHI's Policy and Procedures for Termination or Cessation of the Employment or Contractual Relationship set out exit procedures that ensure Human Resources, Information Technology, Corporate Administration, Finance and Web Services are notified of any agent terminating their relationship with CIHI and that all CIHI property, including security access cards and keys if applicable, and personal health information are securely returned. The *Off-Boarding Checklist* for Managers identifies the necessary steps the Manager must complete before the agent's last day and to whom the property should be returned. The Checklist includes a requirement for the CIHI Manager to retrieve the security access card from the departing agent and return it to the Corporate Administration Department.

In the case of agents who are transferring from one department to another and no longer have a need to access the previously approved data, the previous manager requests removal of all file or folder access for the transferred agents as set out in CIHI's internal employee movement action checklist.

Secure Retention and Destruction of Accessed/Used Records

When access is approved, data files and related reports are managed to the end of their lifecycle in a manner that is consistent with section 4.d of CIHI's *Privacy and Security Framework, 2010*. Section 4.d recognizes that information is only secure if it is secure throughout its entire lifecycle: creation and collection, access, retention and storage, use, disclosure and disposal. Accordingly, CIHI has a comprehensive suite of policies 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 associated standards, guidelines and operating procedures reflect best practices in privacy, information security and records management that are also at par with the requirements of the IPC/ON.

Compliance, Audit and Enforcement

The *Privacy Policy, 2010*, sets out that CIHI's Code of Business Conduct describes the ethical and professional behaviour related to work relationships, information – including personal health information – and the workplace. The Code requires all employees to comply with the Code and all CIHI's policies, protocols and procedures, including CIHI's *Privacy Policy, 2010*. Compliance with CIHI's privacy program is monitored through CIHI's risk-based privacy audit program set out in a multi-year audit plan. Instances of non-compliance with privacy and security policies are managed through CIHI's *Privacy and Security Incident Management Protocol*. Violations of the Code are referred to Human Resources, as appropriate, and may result in disciplinary action up to and including dismissal.

9. Log of Agents Granted Approval to Access and Use Personal Health Information

The log of agents granted approval to access and use personal health information is maintained by the appropriate service team (ITS or Client Engagement and Support) as part of the service fulfillment process. It includes the following fields of information:

- Name of agent;
- Data holdings or applications to which access and use was granted;
- Level or type of access and use; and
- The date access and use was granted.
- The termination date or the date of the next audit of access and use is also captured. For access to a secure CIHI on-line application that may contain personal health information, access is validated upon role change and annually and revoked upon employment termination.

10. Policy and Procedures for the Use of Personal Health Information for Research

Not applicable – CIHI does not use personal health information for research purposes as contemplated by paragraph 37(1)(j) of the Act nor does CIHI use aggregate or de-identified data for research purposes. In keeping with its mandate and core functions, CIHI only uses personal health information, de-identified data and aggregate data for statistical analysis and reporting purposes. Analyses are undertaken to support decision-making for stakeholders such as Health Canada, Statistics Canada and ministries of health and health system managers. Section 7.1 of CIHI's *Privacy Policy Procedures* specifically prohibits the use of personal health information, de-identified and/or aggregate data for research purposes.

11. Log of Approved Uses of Personal Health Information for Research

Not applicable.

Disclosure of Personal Health Information

12. Policy and Procedures for Disclosure of Personal Health Information for Purposes other than Research

Section 37 of CIHI's *Privacy Policy, 2010*, states that CIHI discloses health information and analyses on Canada's health system and the health of Canadians in a manner consistent with its mandate and core functions, including:

37 (a) Disclosures to parties with responsibility for the planning and management of the health care system to enable them to fulfill those functions; and

37 (b) Disclosures to parties with a decision-making role regarding health care system policy to facilitate their work.

Furthermore, section 38 of CIHI's *Privacy Policy, 2010*, states that CIHI reviews the requests to ensure that all disclosures are consistent with section 37, above, and meet the requirements of applicable legislation – including PHIPA and its regulation.

Sections 45 to 47 of CIHI's *Privacy Policy, 2010*, set out CIHI's commitment to disclose non-identifying information before considering the disclosure of personal health information. They read as follows:

45. CIHI data disclosures are made at the highest degree of anonymity possible while still meeting the research and/or analytical purposes. This means that, whenever possible, data are aggregated.

46. Where aggregate data are not sufficiently detailed for the research and/or analytical purposes, data that have been de-identified using various de-identification processes may be disclosed to the recipient on a case-by-case basis, and where the recipient has entered into a data protection agreement or other legally binding instrument with CIHI.

47. Only those data elements necessary to meet the identified research or analytical purposes may be disclosed.

Once it has been determined that aggregate or de-identified data will not serve the intended purpose, the disclosure of personal health information will be contemplated only in limited circumstances and when permissible by law. Section 40 of CIHI's *Privacy Policy, 2010*, reads as follows:

> *40. CIHI will not disclose personal health information if other information will serve the purpose of the disclosure and will not disclose more personal health information than is reasonably necessary to meet the purpose. CIHI does not disclose personal health information except under the following limited circumstances and where the recipients have entered into a data protection agreement or other legally binding instrument(s) with CIHI:*
>
> *(a) The recipient has obtained the consent of the individuals concerned; or*
>
> *(b) The recipient is a prescribed entity under Section 45 of Ontario's Personal Health Information Protection Act, 2004 (PHIPA) 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 requirements of PHIPA and CIHI's internal requirements are met; or*
>
> *(c) The recipient is a prescribed person under Subsection 13(1) O.Reg.329/04 of Ontario's PHIPA for the purposes of facilitating or improving the provision of health care, provided the requirements of PHIPA and CIHI's internal requirements are met; or*
>
> *(d) The disclosure is otherwise authorized by law; or*
>
> *(e) The disclosure is required by law.*

Review and Approval Process

CIHI's *Privacy Policy Procedures* related to sections 40 to 44 of CIHI's *Privacy Policy, 2010*, designate Privacy and Legal Services as responsible for determining if there is lawful authority for the disclosure of personal health information in a manner consistent with the Act and its regulation. The *Privacy Policy Procedures* also set out the process, including what documentation must be completed, provided or executed, who is responsible for same, the content of the documentation and to whom it must be provided prior to the disclosure of personal health information in a manner at par with the IPC/ON's requirements as set out in the IPC/ON Manual.

Further, section 35 of CIHI's *Privacy Policy, 2010*, requires that when returning personal health information to an original data provider, it shall not contain any additional identifying information to that originally provided.

At CIHI, all disclosures of personal health information for purposes other than research must receive approval by the President and Chief Executive Officer.

Conditions and Restrictions on the Approval

Certain conditions and restrictions must be satisfied **prior** to CIHI's disclosure of personal health information. The *Privacy Policy, 2010*, identifies Privacy and Legal Services as responsible for ensuring that these are met. The conditions and restrictions include a requirement for a Data Sharing Agreement or other legally binding instrument to be executed in accordance with section 42 of CIHI's *Privacy Policy, 2010*.

The Data Sharing Agreement or other legally binding instrument must contain the following requirements:

- Prohibits contacting the individuals;
- Prohibits linking the personal health information unless expressly authorized in writing by CIHI;
- Limits the purposes for which the personal health information may be used;
- Requires that the personal health information be safeguarded;
- Limits publication or disclosure to data that do not allow identification of any individual;
- Requires the secure destruction of data, as specified;
- Permits CIHI to conduct on-site privacy audits pursuant to its privacy audit program; and
- Requires the recipient to comply with any other provision that CIHI deems necessary to further safeguard the data.

Secure Transfer

The manner in which records of personal health information will be securely transferred is detailed in the *Secure Information Transfer Standard* and the *Health Data Collection Standard*.

Secure Return or Disposal

CIHI uses standard provisions in data sharing agreements and other legally binding instruments to ensure the secure return or disposal of personal health information disclosed. The agreements make reference to CIHI's standards in this regard, that is, the *Secure Information Transfer Standard* and the *Secure Destruction Standard*, as the case may be, copies of which form part of the agreement.

Where data are to be securely destroyed, CIHI also requires that data recipients complete and submit a Certificate of Destruction to CIHI within 15 days of destruction, setting out the date, time, location and method of secure destruction employed.

CIHI has instituted an ongoing data destruction compliance process whereby all data sets that are disclosed to third parties, whether they contain personal health information or de-identified data, are tracked and monitored by Privacy and Legal Services to ensure that the data destruction requirements are met at the end of their life cycle.

Documentation Related to Approved Disclosures of Personal Health Information

Furthermore, CIHI has adopted a business process management system whereby all disclosures of both personal health information and de-identified data are logged to ensure that documentation related to the receipt, review and approval of requests for disclosure of personal health information are retained and auditable.

Compliance, Audit and Enforcement

The *Privacy Policy, 2010*, sets out that CIHI's Code of Business Conduct describes the ethical and professional behaviour related to work relationships, information – including personal health information – and the workplace. The Code requires all employees to comply with the Code and all CIHI's policies, protocols and procedures, including CIHI's *Privacy Policy, 2010*. Compliance with CIHI's privacy program is monitored through CIHI's risk-based privacy audit program set out in a multi-year audit plan. Instances of non-compliance with privacy and security policies are managed through CIHI's *Privacy and Security Incident Management Protocol*. Violations of the Code are referred to Human Resources, as appropriate, and may result in disciplinary action up to and including dismissal.

Where the Disclosure of Personal Health Information for Purposes other than Research is not Permitted

Not applicable as the disclosure of personal health information for purposes other than research is permitted.

13. Policy and Procedures for Disclosure of Personal Health Information for Research Purposes and the Execution of Research Agreements

Section 37 of CIHI's *Privacy Policy, 2010*, states that CIHI discloses health information and analyses on Canada's health system and the health of Canadians in a manner consistent with its mandate and core functions, including:

37 (c) Disclosures to parties with responsibility for population health research and/or analysis; and

37 (d) Disclosures to third-party data requesters to facilitate health or health services research and/or analysis.

Furthermore, section 38 of CIHI's *Privacy Policy, 2010*, states that CIHI reviews the requests to ensure that all disclosures are consistent with section 37, above, and meet the requirements of applicable legislation – including PHIPA.

Sections 45 to 47 of CIHI's *Privacy Policy, 2010*, set out CIHI's commitment to disclose non-identifying information before considering the disclosure of personal health information. They read as follows:

45. CIHI data disclosures are made at the highest degree of anonymity possible while still meeting the research and/or analytical purposes. This means that, whenever possible, data are aggregated.

46. Where aggregate data are not sufficiently detailed for the research and/or analytical purposes, data that have been de-identified using various de-identification processes may be disclosed to the recipient on a case-by-case basis, and where the recipient has entered into a data protection agreement or other legally binding instrument with CIHI.

47. Only those data elements necessary to meet the identified research or analytical purposes may be disclosed.

Once it has been determined that aggregate or de-identified data will not serve the intended purpose, the disclosure of personal health information will be contemplated only in limited circumstances and when permissible by law. Section 40 of CIHI's *Privacy Policy, 2010*, reads as follows:

40. CIHI will not disclose personal health information if other information will serve the purpose of the disclosure and will not disclose more personal health information than is reasonably necessary to meet the purpose. CIHI does not disclose personal health information except under the following limited circumstances and where the recipients have entered into a data protection agreement or other legally binding instrument(s) with CIHI:

(a) The recipient has obtained the consent of the individuals concerned; or

(b) The recipient is a prescribed entity under Section 45 of Ontario's Personal Health Information Protection Act, 2004 (PHIPA) 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 requirements of PHIPA and CIHI's internal requirements are met; or

(c) The recipient is a prescribed person under Subsection 13(1) O.Reg.329/04 of Ontario's PHIPA for the purposes of facilitating or improving the provision of health care, provided the requirements of PHIPA and CIHI's internal requirements are met; or

(d) The disclosure is otherwise authorized by law; or

(e) The disclosure is required by law.

The related procedures, however, differ from those for disclosure of personal health information for purposes other than research because of the PHIPA requirements. CIHI's procedures are consistent with the Act and its regulation and the IPC/ON Manual and include the following requirements:

- The researcher must submit the following documentation to CIHI:
  - An application in writing;
  - A copy of the research plan submitted to the Research Ethics Board that sets out, at minimum, the affiliation of each person involved in the research, the nature and objectives of the research, and the public or scientific benefit of the research that the researcher anticipates; and
  - A copy of the decision of the research ethics board that approved the research plan.

- The researcher must comply with any conditions and restrictions relating to the use, security, disclosure, return or destruction of the personal health information.

- The program area must ensure:
  - that the personal health information being requested is consistent with the personal health information identified in the written research plan; and
  - that de-identified and/or aggregate information will not serve the research purpose and no more personal health information is being requested than is reasonably necessary to meet the research purpose.

- The program area must retain original documentation relating to the request.

Review and Approval Process for Disclosures of Personal Health Information for Research Purposes

The only distinction between disclosures for research purposes and disclosures for purposes other than research lies in the criteria against which approval will be considered. Specifically, section 43.2 of CIHI's *Privacy Policy Procedures* sets out the criteria against which approval will be considered, having regard to the requirements of the Act and its regulation. These criteria include:

- Does CIHI have a copy of the decision of the research ethics board approving the Research Plan, and does the Research Plan:
  - set out the affiliation of each person involved in the research?
  - set out the nature and objectives of the research and the public or scientific benefit of the research that the researcher anticipates?
  - include a description of the research proposed to be conducted and the duration of the research?
  - include a description of the PHI required and the potential sources?
  - a description of how the PHI will be used in the research, and if it will be linked to other information, a description of the other information as well as how the linkage will be done
  - include an explanation as to why the research cannot reasonably be accomplished without the PHI and, if it is to be linked to other information, an explanation as to why this linkage is required?
  - indicate whether other, de-identified and/or aggregate information serve the research purpose?

- indicate whether more personal health information is being requested than is reasonably necessary to meet the research purpose?
- include a retention period for the personal health information records?
- include an explanation as to why consent to the disclosure of the PHI is not being sought from the individuals to whom the information relates?
- include a description of the reasonably foreseeable harms and benefits that may arise from the use of the PHI and how the researchers intend to address those harms?
- include a description of all persons who will have access to the information, why their access is necessary, their roles in relation to the research, and their related qualifications?
- include a description of the safeguards that the researcher will impose to protect the confidentiality and security of the PHI, including an estimate of how long information will be retained in an identifiable form and why?
- include information as to how and when the PHI will be disposed of or returned to the health information custodian?
- indicate the funding source of the research?
- indicate whether the researcher has applied for the approval of another research ethics board and, if so the response to or status of the application?
- indicate whether the researcher's interest in the disclosure of the PHI or the performance of the research would likely result in an actual or perceived conflict of interest with other duties of the researcher?
- Is the information requested consistent with the information identified in the Research Plan approved by the research ethics board?

Section 42 of CIHI's *Privacy Policy Procedures* require that prior to disclosing personal health information, agents from the program area must consult with Privacy and Legal Services who will review the proposed disclosure and all relevant documentation to ensure there is lawful authority for the disclsoure. Further, all disclosures of personal health information for research purposes must be reviewed and approved by CIHI's Privacy, Confidentiality and Security Committee, in writing, through the submission of a briefing note. Privacy and Legal Services will document the record of decision by amending the briefing note, forward a copy of the briefing note to the agent of the program area that submitted the request and identify, log and track the dates of destruction in a bring-forward system. Internal approval and verification processes and the Secure Information Transfer Standard must also be followed..

Prior to disclosure, the recipient must sign a Research Agreement. All elements listed in the IPC/ON Manual, namely, all items in the General Provisions; Purposes of Collection, Use and Disclosure; Compliance with the Statutory Requirements for the Disclosure for Research Purposes; Secure Transfer; Secure Retention; Secure Return or Disposal; Notification; and Consequences of a Breach and Monitoring Compliance are contained in CIHI's Template Research Agreement for the disclosure of Ontario Personal Health Information.Review and Approval Process for Disclosures of Aggregate and De-identified Information for Research Purposes

CIHI administers a third-party custom data request program for both aggregate and de-identified record-level data. The program falls under the responsibility of the Vice-President, Programs,

and is managed by the Manager, Decision Support Services, for all of Programs. The process for requesting data from CIHI is found on CIHI's external website – Make a Data Request page.

CIHI's custom data request program addresses the requirements of CIHI *Privacy Policy, 2010*, with respect to data disclosures to third parties as set out in sections 37, 38, 45 to 52 and 54 to 56. CIHI discloses health information and analyses on Canada's health system and the health of Canadians in a manner that is consistent with its mandate and core functions, including disclosures to third-party data requesters to facilitate health or health services research and/or analysis. CIHI reviews the requests to ensure that the disclosures are consistent with its mandate and meet the requirements of any applicable legislation. CIHI data disclosures are made at the highest degree of anonymity possible while still meeting the research and/or analytical purposes of the requester. This means that, whenever possible, data are aggregated. Where aggregate data are not sufficiently detailed for the intended purpose, data that have been de-identified may be disclosed to the recipient on a case-by-case basis, and where the recipient has entered into a data protection agreement with CIHI. Only those data elements necessary to meet the intended purpose may be disclosed. For disclosures of de-identified data, the requester will provide CIHI with evidence of Research Ethics Board approval where such approval was obtained. Prior to disclosure, program areas evaluate the data to assess and subsequently minimize privacy risks of re-identification and residual disclosure, and implement the necessary mitigating measures to manage residual risks. The Programs area maintains all documentation related to third-party data requests in its workflow management tool.

Compliance, Audit and Enforcement

The *Privacy Policy, 2010*, sets out that CIHI's Code of Business Conduct describes the ethical and professional behaviour related to work relationships, information – including personal health information – and the workplace. The Code requires all employees to comply with the Code and all CIHI's policies, protocols and procedures, including CIHI's *Privacy Policy, 2010*. Compliance with CIHI's privacy program is monitored through CIHI's risk-based privacy audit program set out in a multi-year audit plan. Instances of non-compliance with privacy and security policies are managed through CIHI's *Privacy and Security Incident Management Protocol*. Violations of the Code are referred to Human Resources, as appropriate, and may result in disciplinary action up to and including dismissal.

CIHI has adopted a complete lifecycle approach to data management for third-party de-identified data requests. As part of that lifecycle, Privacy and Legal Services developed and is responsible for the ongoing compliance monitoring process whereby all de-identified data sets that are disclosed to third-party data recipients are tracked and monitored for secure destruction at the end of their lifecycle. Prior to disclosure, recipients of third-party de-identified data sign a data protection agreement and agree to comply with the conditions and restrictions imposed by CIHI which include secure destruction requirements and CIHI's right to audit.

In addition to the compliance monitoring process with respect to data destruction requirements, Privacy and Legal Services contacts third-party recipients of record-level data (personal health

information and de-identified data) on an annual basis to certify that they continue to comply with their obligations as set out in the data protection agreement signed with CIHI.

In 2018, for the first time, third-party recipients of both personal health information and de-identified data were required to complete a short online survey audit designed to provide more detailed compliance verification in specific areas of concern to CIHI Privacy and Information Security departments.

Secure Access Environment

CIHI is exploring the development of a Secure Access Environment (SAE) where external clients (researchers) would have secure, controlled remote access to CIHI data via a secure and encrypted session. This would eliminate, to a great extent, the residence of personal health information and de-identified data used for research purposes outside of CIHI's secure environment.

Some important features of the SAE would include:

- Multi-factor authentication (no unauthorized access)
- Read-only access to original data
- Only aggregate outputs may leave the SAE, with strict vetting rules to ensure privacy and security principles are applied (no downloading of record-level data from the environment to the requestor's computer)
- Change in the current Information Security and associated processes.
- High availability with secure storage and backup IT infrastructure

Where the Disclosure of Personal Health Information is not Permitted for Research

Disclosure of personal health information is permitted for research; this section, therefore, is not applicable.

14. Template Research Agreement

Section 42 of CIHI's *Privacy Policy, 2010*, requires that, prior to disclosure of personal health information for research purposes, a Research Agreement be executed with the researchers to whom the personal health information will be disclosed. The Research Agreement addresses the matters set out below.

General Provisions

- Describes CIHI's status under the Act and the duties and responsibilities arising from this status.
- Specifies the precise nature of the personal health information that CIHI will disclose for research purposes.
- Provides a definition of personal health information that is consistent with the Act and its regulation.

Purposes of Collection, Use and Disclosure

- Identifies the research purpose for which CIHI is disclosing the personal health information, identifies the purposes for which the personal health information may be used or disclosed by the researcher, and identifies the statutory authority for each collection, use and disclosure identified.

- Only permits the researcher to use the personal health information for the purposes set out in the written research plan approved by the research ethics board and prohibits the use of the personal health information for any other purpose.

- Prohibits the researcher from permitting persons to access and use the personal health information except those persons described in the written research plan approved by the research ethics board.

- In identifying the purposes for which the personal health information may be used, explicitly states whether or not the personal health information may be linked to other information and prohibits the personal health information from being linked except in accordance with the written research plan approved by the research ethics board.

- Requires the researcher to acknowledge that the personal health information that is being disclosed pursuant to the Research Agreement is necessary for the identified research purpose and that other information, namely de-identified and/or aggregate information, will not serve the research purpose.

- Requires the researcher to acknowledge that no more personal health information is being collected and will be used than is reasonably necessary to meet the research purpose.

- Imposes restrictions on the disclosure of personal health information. Requires the researcher to acknowledge and agree not to disclose the personal health information except as required by law and subject to the exceptions and additional requirements prescribed in the regulation to the Act; not to publish the personal health information in a form that could reasonably enable a person to ascertain the identity of the individual; and not to make contact or attempt to make contact with the individual to whom the personal health information relates, directly or indirectly, unless the consent of the individual to being contacted is first obtained in accordance with subsection 44(6) of the Act.

Compliance with the Statutory Requirements for the Disclosure for Research Purposes

- Requires the researcher and CIHI to acknowledge and agree that the researcher has submitted an application in writing, a written research plan that meets the requirements of the Act and its regulation, and a copy of the decision of the research ethics board approving the written research plan.

- Requires the researcher to acknowledge and agree that the researcher will comply with the Research Agreement, with the written research plan approved by the research ethics board and with the conditions, if any, specified by the research ethics board in respect of the written research plan.

Secure Transfer

- Requires the secure transfer of records of personal health information that will be disclosed pursuant to the Research Agreement.

- Sets out the secure manner in which records of personal health information will be transferred, including under what conditions and to whom the records will be transferred, and the procedure that will be followed in ensuring that the records of personal health information are transferred in a secure manner. In identifying the secure manner in which the records of personal health information will be transferred, has regard to the Policy and Procedures for Secure Transfer of Records of Personal Health Information implemented by CIHI.

Secure Retention

- Identifies the retention period for the records of personal health information subject to the Research Agreement, including the length of time that the records of personal health information will be retained in identifiable form. The retention period is consistent with that set out in the written research plan approved by the research ethics board.

- Requires the researcher to ensure that the records of personal health information are retained in a secure manner and identifies the precise manner in which the records of personal health information in paper and electronic format will be securely retained. In identifying the secure manner in which the records of personal health information will be retained, may have regard to the Policy and Procedures for Secure Retention of Records of Personal Health Information and has regard to the written research plan approved by the research ethics board.

- Requires the researcher to take steps that are reasonable in the circumstances to ensure that the personal health information subject to the Research Agreement is protected against theft, loss and unauthorized use or disclosure and to ensure that the records of personal health information subject to the Research Agreement are protected against unauthorized copying, modification or disposal.

- Details the reasonable steps that are required to be taken by the researcher and, at a minimum, includes those set out in the written research plan approved by the research ethics board.

Secure Return or Disposal

- Addresses whether the records of personal health information subject to the Research Agreement will be returned in a secure manner, will be disposed of in a secure manner or will be de-identified and retained by the researcher following the retention period set out in the Research Agreement. In this regard, the provisions in the Research Agreement are consistent with the written research plan approved by the research ethics board.

- If the records of personal health information are required to be returned in a secure manner, stipulate the time frame following the retention period within which the records must be securely returned, the secure manner in which the records must be returned and the agent of the prescribed person or prescribed entity to whom the records must be securely returned. In identifying the secure manner in which the records of personal

health information will be returned, regard may be had to the Policy and Procedures for Secure Transfer of Records of Personal Health Information implemented by CIHI.

- If the records of personal health information are required to be disposed of in a secure manner, provides a definition of secure disposal that is consistent with the Act and its regulation and identifies the precise manner in which the records of personal health information subject to the Research Agreement must be securely disposed of.

- Stipulates the time frame following the retention period set out in the Research Agreement within which the records of personal health information must be securely disposed of and within which a certificate of destruction must be provided.

- In identifying the secure manner in which the records of personal health information will be disposed of, ensures that the method of secure disposal identified is consistent with the Act and its regulation; with orders issued by the Information and Privacy Commissioner of Ontario under the Act and its regulation, including Order HO-001 and Order HO-006; and with guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner of Ontario pursuant to the Act and its regulation, including Fact Sheet 10: Secure Destruction of Personal Information. In addition, regard may be had to the Policy and Procedures for Secure Disposal of Records of Personal Health Information implemented by CIHI.

- Identifies the agent of CIHI to whom the certificate of destruction must be provided, the time frame following secure disposal within which the certificate of destruction must be provided and the required content of the certificate of destruction. At a minimum, the certificate of destruction identifies the records of personal health information securely disposed of; stipulates the date, time, location and method of secure disposal employed; and bears the name and signature of the person who performed the secure disposal. If the records of personal health information are required to be de-identified and retained by the researcher rather than being securely returned or disposed of, the manner and process for de-identification is set out in the Research Agreement. In identifying the manner and process for de-identification, regard may be had to the Policy and Procedures with Respect to De-Identification and Aggregation implemented by CIHI. The Research Agreement also requires the researcher to submit written confirmation that the records were de-identified and stipulates the time frame following the retention period set out in the Research Agreement within which the written confirmation must be provided and the agent of CIHI to whom the written confirmation must be provided.

Notification

- Requires the researcher to notify the prescribed person or prescribed entity immediately, in writing, if the researcher becomes aware of a breach or suspected breach of the Research Agreement, a breach or suspected of subsection 44(6) of the Act or if personal health information subject to the Research Agreement is stolen, lost or accessed by unauthorized persons or is believed to have been stolen, lost or accessed by unauthorized persons.

- Identifies the agent of CIHI to whom notification must be provided and requires the researcher to take steps that are reasonable in the circumstances to contain the breach and to contain the theft, loss or access by unauthorized persons.

Consequences of Breach and Monitoring Compliance

- Outlines the consequences of breach of the agreement and indicates whether compliance with the Research Agreement will be audited by CIHI and, if so, the manner in which compliance will be audited and the notice, if any, that will be provided of the audit.

- Requires the researcher to ensure that all persons who will have access to the personal health information, as identified in the written research plan approved by the research ethics board, are aware of and agree to comply with the terms and conditions of the Research Agreement prior to being given access to the personal health information. Sets out the method by which this will be ensured by the researcher, such as requiring the persons identified in the written research plan to sign an acknowledgement prior to being granted access, indicating that they are aware of and agree to comply with the terms and conditions of the Research Agreement.

15. Log of Research Agreements

CIHI maintains a business process management system workflow tool that tracks all executed third-party data requests, including requests for disclosure of personal health information and de-identified data and the resulting data protection agreements (i.e., Research Agreements for the Disclosure of Ontario Personal Health Information in the case of disclosures of personal health information, and Non-Disclosure/Confidentiality Agreements in the case of disclosures of de-identified record-level data). The following data elements are contained in the workflow tool and/or the associated documentation:

- The name of the research study;
- The name of the principal researcher to whom the personal health information was disclosed pursuant to the data protection agreement;
- The date(s) of receipt of the written application, the written research plan and the written decision of the research ethics board approving the research plan;
- The date that the approval to disclose the personal health information for research purposes was granted;
- The date that the data protection agreement was executed;
- The date that the personal health information was disclosed;
- The nature of the personal health information disclosed;
- The retention period for the records of personal health information as set out in the data protection agreement;
- The date by which the records of personal health information must be securely destroyed; and
- The certificate of destruction and the date it was received.

Data Sharing Agreements

16. Policy and Procedures for the Execution of Data Sharing Agreements

Section 40 of CIHI's *Privacy Policy, 2010*, requires that, prior to disclosure of personal health information, including for non-research purposes, a Data Sharing Agreement or other legally binding instrument be executed with the person or organization to whom the personal health information will be disclosed. Sections 42.1 and 42.2 of the *Privacy Policy Procedures* require that, prior to disclosing personal health information, program area staff must consult with Privacy and Legal Services. Privacy and Legal Services will review all relevant documentation to ensure there is lawful authority for the proposed disclosure and must be satisfied that the disclosure is in accordance with CIHI's *Privacy Policy, 2010*. Ultimately, all Data Sharing Agreements are signed by CIHI's President and Chief Executive Officer or his delegate.

At CIHI, Privacy and Legal Services is responsible for maintaining a log and repository of Data Sharing Agreements and for all documentation relating to the execution of the Data Sharing Agreements. The requirement for a log and responsibility for maintaining the log is set out in the *Privacy Policy Procedures*.

For CIHI, Data Sharing Agreements for the disclosure of personal health information for non-research purposes are generally limited to other prescribed entities or prescribed persons in Ontario. As such, the disclosures are for purposes of their mandate and are in compliance with the respective obligations under PHIPA of CIHI and the prescribed entity/prescribed person. All agreements between CIHI and other prescribed entities or prescribed persons are in keeping with the templates described in section 17, below.

Any new collection of personal health information must be reviewed by Privacy and Legal Services to determine if the proposed data collection falls under an existing agreement, or if an amendment to an existing agreement or a new agreement is required. This is set out in section 1 of CIHI's *Privacy Policy Procedures*.

Compliance, Audit and Enforcement

The *Privacy Policy, 2010*, sets out that CIHI's Code of Business Conduct describes the ethical and professional behaviour related to work relationships, information – including personal health information – and the workplace. The Code requires all employees to comply with the Code and all CIHI's policies, protocols and procedures, including CIHI's *Privacy Policy, 2010*. Compliance with CIHI's privacy program is monitored through CIHI's risk-based privacy audit program set out in a multi-year audit plan. Instances of non-compliance with privacy and security policies are managed through CIHI's *Privacy and Security Incident Management Protocol*. Violations of the Code are referred to Human Resources, as appropriate, and may result in disciplinary action up to and including dismissal.

17. Template Data Sharing Agreement

CIHI has developed two template data sharing agreements:

- Template Data Sharing Agreement for the Collection of Personal Health Information for Non-Research Purposes; and
- Template Data Sharing Agreement for the Disclosure of Personal Health Information for Non-Research Purposes.

The template Data Sharing Agreements address the matters set out below:

General Provisions

- Describes the status of CIHI under the Act and the duties and responsibilities arising from this status. Species the precise nature of the personal health information subject to the Data Sharing Agreement and provides a definition of personal health information that is consistent with the Act and its regulation.
- Identifies the person or organization that is collecting personal health information and the person or organization that is disclosing personal health information pursuant to the Data Sharing Agreement.

Purposes of Collection, Use and Disclosure

- Identifies the purposes for which the personal health information subject to the Data Sharing Agreement is being collected and for which the personal health information will be used.
- In identifying these purposes, explicitly states whether or not the personal health information collected pursuant to the Data Sharing Agreement will be linked to other information. If the personal health information will be linked to other information, the Data Sharing Agreement identifies the nature of the information to which the personal health information will be linked, the source of the information to which the personal health information will be linked, how the linkage will be conducted and why the linkage is required for the identified purposes.
- Contains an acknowledgement that the personal health information collected pursuant to the Data Sharing Agreement is necessary for the purpose for which it was collected and that other information, namely de-identified and/or aggregate information, will not serve the purpose and that no more personal health information is being collected and will be used than is reasonably necessary to meet the purpose.
- Identifies the purposes, if any, for which the personal health information subject to the Data Sharing Agreement may be disclosed and any limitations, conditions or restrictions imposed thereon.
- Requires the collection, use and disclosure of personal health information subject to the Data Sharing Agreement to comply with the Act and its regulation and sets out the specific statutory authority for each collection, use and disclosure contemplated in the Data Sharing Agreement.

Secure Transfer

- Requires the secure transfer of the records of personal health information subject to the Data Sharing Agreement. Sets out the secure manner in which the records of personal health information will be transferred, including under what conditions and to whom the records will be transferred, and the procedure that must be followed in ensuring that the records are transferred in a secure manner. In identifying the secure manner in which the records of personal health information will be transferred, regard may be had to the

Policy and Procedures for Secure Transfer of Records of Personal Health Information implemented by CIHI.

Secure Retention

- Specifies the retention period for the records of personal health information subject to the Data Sharing Agreement. In identifying the relevant retention period, ensures that the records of personal health information are retained only for as long as necessary to fulfill the purposes for which the records of personal health information were collected.
- Requires the records of personal health information to be retained in a secure manner and identifies the precise manner in which the records of personal health information in paper and electronic format will be securely retained, including whether the records will be retained in identifiable form. In identifying the secure manner in which the records of personal health information will be retained, the Data Sharing Agreement may have regard to the Policy and Procedures for Secure Retention of Records of Personal Health Information implemented by CIHI.
- Requires reasonable steps to be taken to ensure that the personal health information subject to the Data Sharing Agreement is protected against theft, loss and unauthorized use or disclosure and to ensure that the records of personal health information are protected against unauthorized copying, modification or disposal. The reasonable steps that are required to be taken are also detailed in the Data Sharing Agreement.

Secure Return or Disposal

- Addresses whether the records of personal health information subject to the Data Sharing Agreement will be returned in a secure manner or will be disposed of in a secure manner following the retention period set out in the Data Sharing Agreement or following the date of termination of the Data Sharing Agreement, as the case may be.
- If the records of personal health information are required to be returned in a secure manner, stipulates the time frame following the retention period or following the date of termination of the Data Sharing Agreement within which the records of personal health information must be securely returned, the secure manner in which the records must be returned and the person to whom the records must be securely returned. In identifying the secure manner in which the records of personal health information will be returned, regard may be had to the Policy and Procedures for Secure Transfer of Records of Personal Health Information implemented by the prescribed person or prescribed entity.
- If the records of personal health information are required to be disposed of in a secure manner, provides a definition of secure disposal that is consistent with the Act and its regulation and identifies the precise manner in which the records of personal health information subject to the Data Sharing Agreement must be securely disposed of. Stipulates the time frame following the retention period or following the date of termination of the Data Sharing Agreement within which the records of personal health information must be securely disposed of and within which a certificate of destruction must be provided.
- In identifying the secure manner in which the records of personal health information will be disposed of, ensures that the method of secure disposal identified is consistent with the Act and its regulation; with orders issued by the Information and Privacy Commissioner of Ontario under the Act and its regulation, including Order HO-001 and Order HO-006; and with guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner of Ontario pursuant to the Act and its regulation,

including Fact Sheet 10: Secure Destruction of Personal Information. In addition, regard may be had to the Policy and Procedures for Secure Disposal of Records of Personal Health Information implemented by CIHI.

- Identifies the person to whom the certificate of destruction must be provided, the time frame following secure disposal within which the certificate of destruction must be provided and the required content of the certificate of destruction. At a minimum, the certificate of destruction identifies the records of personal health information securely disposed of; stipulates the date, time, location and method of secure disposal employed; and bears the name and signature of the person who performed the secure disposal.

Notification

- Requires that notification be provided at the first reasonable opportunity if the Data Sharing Agreement has been breached or is suspected to have been breached or if the personal health information subject to the Data Sharing Agreement is stolen, lost or accessed by unauthorized persons or is believed to have been stolen, lost or accessed by unauthorized persons. Identifies whether the notification must be verbal and/or in writing and to whom the notification must be provided. Requires that reasonable steps be taken to contain the breach of the Data Sharing Agreement and to contain the theft, loss or access by unauthorized persons.

Consequences of Breach and Monitoring Compliance

- Outlines the consequences of breach of the agreement and indicates whether compliance with the Data Sharing Agreement will be audited and, if so, the manner in which compliance will be audited and the notice, if any, that will be provided of the audit.
- Requires that all persons who will have access to the personal health information are aware of and agree to comply with the terms and conditions of the Data Sharing Agreement prior to being given access to the personal health information. Sets out the method by which this will be ensured. This may include requiring the persons that will have access to the personal health information to sign an acknowledgement, prior to being granted access, indicating that they are aware of and agree to comply with the terms and conditions of the Data Sharing Agreement.

18. Log of Data Sharing Agreements

CIHI's Privacy and Legal Services maintains a log of all executed Data Sharing Agreements. The following data elements are contained in the log:

- The name of the person or organization from whom the personal health information was collected or to whom the personal health information was disclosed;
- The date that the collection or disclosure of personal health information was approved;
- The date that the Data Sharing Agreement was executed or effective;
- The nature of the personal health information subject to the Data Sharing Agreement;
- The retention period for the records of personal health information set out in the Data Sharing Agreement or the date of termination of the Data Sharing Agreement;
- Whether the records of personal health information will be securely returned or will be securely disposed of following the retention period set out in the Data Sharing Agreement or the date of termination of the Data Sharing Agreement; and

- The date the records of personal health information were securely returned or a certificate of destruction was provided or the date by which they must be returned or disposed of.

The data-sharing agreements for both the collection and disclosure of personal health information typically apply on an on-going basis, with no set termination date, with data submissions or disclosures occurring on a daily, weekly, quarterly or annual basis, depending on the arrangements in place. In the case of data disclosures, CIHI maintains a business process management system workflow tool that tracks all disclosures of data under data-sharing agreements, including the dates data are disclosed. For data collections, data flow to CIHI through CIHI's secure web-based or server-to-server applications. These applications use industry standard, encrypted, secure socket layer sessions. Logging of receipt of data occurs within this environment identifying the data supplier, what data were submitted and when the data were submitted.

Agreements with Third Party Service Providers

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

CIHI's Procurement Program *(Accountability Framework, policy and procedures)* sets the guidelines that govern the acquisition of all goods and services by CIHI in meeting its goals and objectives. CIHI has developed various template agreements for the acquisition of goods and services pertaining to personal health information. These templates include a CIHI Services Agreement, a Master Services Agreement, as well as a Standing Offer Agreement and a Services Agreement template (used for contractors providing secure retention and destruction services only), all of which are consistent with the requirements of the *Template Agreement for All Third Party Service Providers* described in section 20, below.

Further, section 11 of CIHI's *Privacy Policy, 2010*, requires that prior to permitting third party service providers to access and use the personal health information held by CIHI, they also must enter into a Confidentiality Agreement with CIHI.

In keeping with section 10 of CIHI's *Privacy Policy, 2010*, CIHI allows, in some circumstances, third party service providers to access and use specific data on a need-to know basis, that is, when required to perform their services. CIHI will not provide any personal health information to a third party service provider if other information, namely de-identified and/or aggregate information, will serve the purpose and CIHI will not provide more personal health information than is reasonably necessary to meet the purpose. Program Area Managers are responsible for making this determination. Section 10 of the *Privacy Policy Procedures* sets out the position responsible for approving access to personal health information.

The Manager, Procurement executes a copy of the final supply agreement and forwards a copy to the third-party for signing. In the absence of the Manager, Procurement, the Director, Strategy and Operations or Vice-President, Corporate Services will assume this responsibility.

Prior to signing, the contract is reviewed against a checklist to ensure that all PHIPA and other contractual requirements have been addressed.

Section 6 of the *Competitive and Non-Competitive Procurement Procedure* states that CIHI's Procurement department will retain all fully executed supply agreements for future reference and audit. In addition, the Procurement department maintains a log of all executed supply agreements. The Procurement department captures all relevant and necessary information from third-party service provider agreements in a database.

CIHI utilizes automated alerts that are sent out from its enterprise resource planning tool. This tool notifies the Program Manager 30 days and 15 days prior to the external professional services staff member's last day of work that Human Resources will initiate the offboarding process if there is no extension in the external professional services staff member's contract through Procurement. Human Resources utilizes an automated task-based process in its business process management workflow tool that initiates the off-boarding workflow for external professional services staff. Once HR initiates the offboarding of the external professional services staff member, the Program Manager receives a link to the Off-Boarding Checklist. The Checklist includes a requirement for the Program Manager to ensure the secure return of any confidential information held by external professional services staff.

The business process management workflow tool issues a task through the off-boarding process to the relevant Program Manager to confirm that the external professional services staff member has returned IT assets, their security card, and any confidential information. Completion of the task is tracked in the workflow tool and in associated processes such as the Service Request for Employee Departure. If the task is not completed within the 24-hour period following the external professional services staff member's last day of work, an escalation notice is sent immediately to the Chief Privacy Officer and to the Chief Information Security Officer for follow-up with the Program Manager to ensure completion of the task. Should CIHI property not be duly returned, the Program Manager is to contact the Chief Privacy Officer/General Counsel.

Secure destruction of confidential information, including personal health information, requires prior approval from the Chief Information Security Officer or the Chief Privacy Officer. A Certificate of Destruction must also be completed. Given that the work of external professional services staff involving personal health information is carried out on CIHI premises and/or over its secure network using CIHI-issued equipment, all personal health information remains under the control of CIHI and the requirement for secure destruction and the related Certificate of Destruction has not yet arisen.

Compliance, Audit and Enforcement

The *Privacy Policy, 2010*, sets out that CIHI's Code of Business Conduct describes the ethical and professional behaviour related to work relationships, information – including personal health information – and the workplace. The Code requires all employees to comply with the Code and all CIHI's policies, protocols and procedures, including CIHI's *Privacy Policy, 2010*. Compliance with CIHI's privacy program is monitored through CIHI's risk-based privacy audit program set out in a multi-year audit plan. Instances of non-compliance with privacy and security policies are managed through CIHI's *Privacy and Security Incident Management Protocol*. Violations of the Code are referred to Human Resources, as appropriate, and may result in disciplinary action up to and including dismissal.

20. Template Agreement for All Third Party Service Providers

CIHI's *Procurement Policy* requires that all purchase orders or contracts 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 the work. The above requirements also apply to third parties who are contracted to retain, transfer, or dispose of personal health information and electronic service providers, where applicable. With respect to the latter, CIHI does not currently contract with electronic service providers for the purpose of enabling CIHI to use electronic means to collect, use, modify, disclose, retain or dispose of PHI Should this change, CIHI would enter into a written agreement with the provider.

CIHI has developed the following template agreements for third party service providers:

- CIHI Services Agreement
- Master Services Agreement
- Standing Offer Agreement
- Services Agreement (used for contractors providing secure retention and destruction services only)

The template agreements for third party service providers address the matters set out below:

General Provisions

- Describes the status of CIHI under the Act and the duties and responsibilities arising from this status. States whether or not the third party service provider is an agent of CIHI in providing services pursuant to the agreement.

- Specifies that all third party service providers that are permitted to access and use personal health information in the course of providing services to CIHI shall be considered agents of CIHI, with the possible exception of electronic service providers. Agreements with electronic service providers explicitly state whether or not the third party service provider is an agent of CIHI in providing services pursuant to the agreement.

- If the third party service provider is an agent of CIHI, the agreement requires the third party service provider to comply with the provisions of the Act and its regulation relating to prescribed entities and to comply with the privacy and security policies and procedures implemented by CIHI in providing services pursuant to the agreement.

- Provides a definition of personal health information which is consistent with the Act and its regulation. Where appropriate, the agreement also specifies the precise nature of the personal health information that the third party service provider will be permitted to access and use in the course of providing services pursuant to the agreement.

- Requires that the services provided by the third party service provider pursuant to the agreement be performed in a professional manner, in accordance with industry standards and practices, and by properly trained agents of the third party service provider.

Obligations with Respect to Access and Use

- Identifies the purposes for which the third party service provider is permitted to access and use the personal health information of CIHI and any limitations, conditions or restrictions imposed thereon.

- In identifying the purposes for which the third party service provider is permitted to use personal health information, CIHI ensures that each use identified in the agreement is consistent with the uses of personal health information permitted by the Act and its regulation. The agreement also prohibits the third party service provider from using personal health information except as permitted in the agreement.

- In the case of an electronic service provider that is not an agent of CIHI, the agreement explicitly prohibits the electronic service provider from using personal health information except as necessary in the course of providing services pursuant to the agreement.

- Further, the agreement prohibits the third party service provider from using personal health information if other information will serve the purpose and from using more personal health information than is reasonably necessary to meet the purpose.

Obligations with Respect to Disclosure

- The agreement identifies the purposes, if any, for which the third party service provider is permitted to disclose the personal health information of the prescribed entity or prescribed person and any limitations, conditions or restrictions imposed thereon.

- In identifying the purposes for which the third party service provider is permitted to disclose personal health information, CIHI ensures that each disclosure identified in the agreement is consistent with the disclosures of personal health information permitted by the Act and its regulation. In this regard, the agreement prohibits the third party service provider from disclosing personal health information except as permitted in the agreement or as required by law, from disclosing personal health information if other information will serve the purpose and from disclosing more personal health information than is reasonably necessary to meet the purpose.

- In the case of an electronic service provider that is not an agent of the prescribed entity or prescribed person, the agreement prohibits the electronic service provider from disclosing personal health information to which it has access in the course of providing services except as required by law.

Secure Transfer

- Where it is necessary to transfer records of personal health information to or from CIHI, the agreement requires the third party service provider to securely transfer the records of personal health information and sets out the responsibilities of the third party service provider in this regard. In particular, the agreement specifies the secure manner in which the records will be transferred by the third party service provider, the conditions pursuant to which the records will be transferred by the third party service provider, to whom the records will be transferred and the procedure that must be followed by the third party service provider in ensuring that the records are transferred in a secure manner.

- In identifying the secure manner in which records of personal health information must be transferred, the agreement has regard to the Policy and Procedures for Secure Transfer of Records of Personal Health Information implemented by CIHI.

- In addition, where the retention of records of personal health information or where the disposal of records of personal health information outside the premises of CIHI is the primary service provided to CIHI, the agreement requires the third party service provider to provide documentation to CIHI setting out the date, time and mode of transfer of the records of personal health information and confirming receipt of the records of personal health information by the third party service provider. In these circumstances, the agreement obligates the third party service provider to maintain a detailed inventory of the records of personal health information transferred.

Secure Retention

- The agreement requires the third party service provider to retain the records of personal health information, where applicable, in a secure manner and identifies the precise methods by which records of personal health information in paper and electronic format will be securely retained by the third party service provider, including records of personal health information retained on various media.

- The agreement further outlines the responsibilities of the third party service provider in securely retaining the records of personal health information. In identifying the secure manner in which the records of personal health information will be retained, and the methods by which the records of personal health information will be securely retained, the agreement has regard to the Policy and Procedures for Secure Retention of Records of Personal Health Information implemented by CIHI.

- Where the retention of records of personal health information is the primary service provided to CIHI by the third party service provider, the agreement also obligates the third party service provider to maintain a detailed inventory of the records of personal health information being retained on behalf of CIHI as well as a method to track the records being retained.

Secure Return or Disposal Following Termination of the Agreement

- The agreement addresses, where applicable, whether records of personal health information will be securely returned to CIHI or will be disposed of in a secure manner following the termination of the agreement.

- If the records of personal health information are required to be returned in a secure manner, the agreement stipulates the time frame following the date of termination of the

agreement within which the records of personal health information must be securely returned, the secure manner in which the records must be returned and the agent of CIHI to whom the records must be securely returned. In identifying the secure manner in which the records of personal health information will be returned, the agreement has regard to the Policy and Procedures for Secure Transfer of Records of Personal Health Information implemented by CIHI.

- If the records of personal health information are required to be disposed of in a secure manner, the agreement provides a definition of secure disposal that is consistent with the Act and its regulation and identifies the precise manner in which the records of personal health information are to be securely disposed of.

- In identifying the secure manner in which the records of personal health information will be disposed of, it is ensured that the method of secure disposal identified is consistent with the Act and its regulation; with orders issued by the Information and Privacy Commissioner of Ontario under the Act and its regulation, including Order HO-001 and Order HO-006; with guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner of Ontario pursuant to the Act and its regulation, including Fact Sheet 10: Secure Destruction of Personal Information; and with the Policy and Procedures for Secure Disposal of Records of Personal Health Information implemented by CIHI.

- The agreement stipulates the time frame following termination of the agreement within which the records of personal health information must be securely disposed of and within which a certificate of destruction must be provided to CIHI. The agreement further identifies the agent of CIHI to whom the certificate of destruction must be provided and identifies the required content of the certificate of destruction. At a minimum, the certificate of destruction identifies the records of personal health information securely disposed of; to stipulate the date, time and method of secure disposal employed; and to bear the name and signature of the person who performed the secure disposal.

Secure Disposal as a Contracted Service

- Where the disposal of records of personal health information is the primary service provided to CIHI by the third party service provider, in addition to the requirements set out above in relation to secure disposal, the agreement further sets out the responsibilities of the third party service provider in securely disposing of the records of personal health information, including:
- The time frame within which the records are required to be securely disposed of;
- The precise method by which records in paper and/or electronic format must be securely disposed of, including records retained on various media;
- The conditions pursuant to which the records will be securely disposed of; and
- The person(s) responsible for ensuring the secure disposal of the records.
- The agreement also enables CIHI, at its discretion, to witness the secure disposal of the records of personal health information subject to such reasonable terms or conditions as may be required in the circumstances.

Implementation of Safeguards

- The agreement requires the third party service provider to take steps that are reasonable in the circumstances to ensure that the personal health information accessed and used in the course of providing services pursuant to the agreement is protected against theft, loss and unauthorized use or disclosure and to ensure that the records of personal health information subject to the agreement are protected against unauthorized copying, modification or disposal. The reasonable steps that are required to be implemented by the third party service provider are detailed in the agreement.

Training of Agents of the Third Party Service Provider

- The agreement requires the third party service provider to provide training to its agents on the importance of protecting the privacy of individuals whose personal health information is accessed and used in the course of providing services pursuant to the agreement and on the consequences that may arise in the event of a breach of these obligations.

- The agreement also requires the third party service provider to ensure that its agents who will have access to the records of personal health information are aware of and agree to comply with the terms and conditions of the agreement prior to being given access to the personal health information. The agreement sets out the method by which this will be ensured. This may include requiring agents to sign an acknowledgement, prior to being granted access to the personal health information, indicating that they are aware of and agree to comply with the terms and conditions of the agreement.

Subcontracting of the Services

- In the event that the agreement permits the third party service provider to subcontract the services provided under the agreement, the third party service provider is required to acknowledge and agree that it will provide CIHI with advance notice of its intention to do so, that the third party service provider will enter into a written agreement with the subcontractor on terms consistent with its obligations to CIHI and that a copy of the written agreement will be provided to CIHI.

Notification

- At a minimum, the agreement requires the third party service provider to notify CIHI at the first reasonable opportunity if there has been a breach or suspected breach of the agreement or if personal health information handled by the third party service provider on behalf of CIHI is stolen, lost or accessed by unauthorized persons or is believed to have been stolen, lost or accessed by unauthorized persons. The agreement also identifies whether the notification must be verbal, written or both and to whom the notification must be provided. The third party service provider is also be required to take steps that are reasonable in the circumstances to contain the breach and to contain the theft, loss or access by unauthorized persons.

Consequences of Breach and Monitoring Compliance

- The agreement outlines the consequences of breach of the agreement and indicates whether CIHI will be auditing compliance with the agreement and, if so, the manner in which compliance will be audited and the notice, if any, that will be provided to the third party service provider of the audit.

21. Log of Agreements with Third Party Service Providers

CIHI's Procurement department maintains a log of all Third Party Service Provider Agreements, which captures the following data elements:

- The name of the third party service provider;
- A description of the services provided by the third party service provider that require access to and use of personal health 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.

Access to and use of records of personal health information by third party service providers in performing their duties or services is provided on a need-to-know basis and is requested by the appropriate Program Manager. No access to data files is granted until the mandatory privacy and security training requirements have been met. All access requests are logged in CIHI's Service Desk, including the date the records of personal health information or access to the records of personal health information was provided and the nature of the PHI .

All confidential information, including personal health information, must be returned to CIHI as specified in the agreement. Secure destruction of personal health information requires prior approval from the Chief Information Security Officer or the Chief Privacy Officer. A Certificate of Destruction must also be completed. The decision for a third-party to securely destroy personal health information is at CIHI's discretion. Given that the work of external professional services staff involving personal health information is carried out on CIHI premises and/or over its secure network using CIHI-issued equipment, all personal health information remains under the control of CIHI and the requirement for secure destruction and the related Certificate of Destruction has not yet arisen.

The date the records of personal health information were securely returned (or a certificate of destruction was provided should that scenario arise) are tracked in the documentation associated with the business process management workflow tool.

Data Linkage and Data De-Identification

22. Policy and Procedures for the Linkage of Records of Personal Health Information

Sections 14 to 31 of CIHI's *Privacy Policy, 2010*, govern linkage of records of personal health information. Pursuant to this *Policy*, CIHI permits the linkage of personal health information under certain circumstances. CIHI also establishes limited purposes for data linkage, having regard to the source of the records and the identity of the person or organization that will ultimately make use of the linked records.

Specifically:

- The linkage of records of personal health information solely in the custody of CIHI for the exclusive use of the linked records of personal health information by CIHI is addressed in sections 18 and 19 of the *Policy*;
- CIHI does not carry out the linkage of records of personal health information in the custody of CIHI with records of personal health information to be collected from another person or organization for the exclusive use of the linked records by CIHI;
- The linkage of records of personal health information solely in CIHI's custody for purposes of disclosure of the linked records of personal health information to another person or organization is addressed in section 20 of the Policy;
- The linkage of records of personal health information in the custody of CIHI with records of personal health information to be collected from another person or organization for purposes of disclosure of the linked records of personal health information to that person or organization is addressed in section 21 of the Policy.

In the case of a new collection of data, such linkages could occur only after the required approval process for a new collection of personal health information was approved under the procedures set out in section 1 of CIHI's Privacy Policy. Use of the linked dataset is governed by section 3 of the Policy which articulates CIHI's commitment not to use personal health information if other information, such as de-identified and/or aggregate information, will serve the purpose and not to use more personal health information than is reasonably necessary to meet the purpose.

Sections 22 to 27 of CIHI's *Privacy Policy, 2010*, describe the approval requirements for data linkage, including the criteria against which approval will be considered, having regard to the requirements of the Act and its regulation.

Criteria for approval pursuant to sections 19 to 21 include:

23. The individuals whose personal health information is used for data linkage have consented to the data linkage; or

24. All of the following criteria are met:

    (a) The purpose of the data linkage is consistent with CIHI's mandate;

    (b) The public benefits of the linkage significantly offset any risks to the privacy of individuals (see section 26);

    (c) The results of the data linkage will not be used for any purpose that would be detrimental to the individuals that the personal health information concerns (see section 27);

    (d) The data linkage is for a time-limited specific project and the linked data will be subsequently destroyed in a manner consistent with sections 28 and 29; or

    (e) The data linkage is for purposes of an approved CIHI ongoing program of work where the linked data will be retained for as long as necessary to meet the

identified purposes and, when no longer required, will be destroyed in a manner consistent with sections 28 and 29; and

(f) The data linkage has demonstrable savings over other alternatives or is the only practical alternative.

Review and Approval Process for Data Linkage

Section 18 of CIHI's *Privacy Policy, 2010*, states that data linkage within a single data holding for CIHI's own purposes is generally permitted. Section 19 states that data linkage across data holdings for CIHI's own purposes will be submitted to CIHI's Privacy, Confidentiality & Security Committee for approval when the requisite criteria set out in sections 22 to 27 of the *Policy* are met. Data linkage requests for or by external third parties are also submitted to CIHI's Privacy, Confidentiality & Security Committee for approval pursuant to sections 20 and 21 of CIHI's *Privacy Policy, 2010*. The *Privacy Policy Procedures* related to the above sections set out the process, including what documentation must be completed, provided or executed, who is responsible for same, the content of the documentation and to whom it must be provided.

Sections 22 to 27 of CIHI's *Privacy Policy, 2010*, describe the approval requirements for data linkage, including the criteria against which approval will be considered, having regard to the requirements of the Act and its regulation.

Criteria for approval pursuant to sections 19 to 21 include:

23. The individuals whose personal health information is used for data linkage have consented to the data linkage; or

24. All of the following criteria are met:

(a) The purpose of the data linkage is consistent with CIHI's mandate;

(b) The public benefits of the linkage significantly offset any risks to the privacy of individuals (see section 26);

(c) The results of the data linkage will not be used for any purpose that would be detrimental to the individuals that the personal health information concerns (see section 27);

(d) The data linkage is for a time-limited specific project and the linked data will be subsequently destroyed in a manner consistent with sections 28 and 29; or

(e) The data linkage is for purposes of an approved CIHI ongoing program of work where the linked data will be retained for as long as necessary to meet the identified purposes and, when no longer required, will be destroyed in a manner consistent with sections 28 and 29; and

(f) The data linkage has demonstrable savings over other alternatives or is the only practical alternative.

As an additional measure, section 25 of CIHI's *Privacy Policy, 2010*, provides that any request for data linkage that is unusual, sensitive or precedent-setting is to be referred by the Privacy, Confidentiality & Security Committee to the President and CEO for approval.

The *Privacy Policy Procedures* related to sections 19-21 describe the manner in which the decision approving or denying the request to link records of personal health information and the reasons for the decision are documented; the method by which and the form in which the decision will be communicated; and to whom the decision will be communicated.

Conditions or Restrictions on the Approval

Section 17 of CIHI's *Privacy Policy, 2010*, requires that in addition to satisfying the requirements and requisite circumstances for data linkage, the linked data remain subject to the use and disclosure provisions in the *Privacy Policy, 2010*. Specifically, Section 3 of CIHI's *Privacy Policy, 2010*, states that CIHI does not use personal health information if other information will serve the purpose and does not use more personal health information than is reasonably necessary to meet the purpose. Section 10 of CIHI's *Privacy Policy, 2010*, clearly sets out that access to personal health information by CIHI's agents (employees) is limited to a "need-to-know" basis when required to perform their duties and/or services.

The related *Privacy Policy Procedures* set out the following specific requirements:

(1) prohibit staff from using de-identified and/or aggregate information, either alone or with other information, to identify an individual including attempting to decrypt information that is encrypted, attempting to identify an individual based on unencrypted information and attempting to identify an individual based on prior knowledge (section 3.1);

(2) prohibit staff from accessing and using personal health information, if other levels of information such as de-identified and/or aggregate information will serve the identified purpose (section10.1); and

(3) prohibit staff from accessing and using more personal health information than is reasonably necessary to meet the identified purpose (section 10.2).

Section 7 of CIHI's *Privacy Policy, 2010*, states that CIHI uses personal health information and de-identified data in a manner consistent with its mandate and core functions, and in compliance with all applicable legislation, including privacy legislation.

Section 14.3 of CIHI's *Privacy Policy Procedures* states that linked records of personal health information are to be de-identified and/or aggregated as soon as practicable and, to the extent possible, only de-identified and/or aggregate information is to be used by CIHI agents.

Process for the Linkage of Records of Personal Health Information

Section 14 of CIHI's *Privacy Policy, 2010*, states that when carrying out data linkage, CIHI will generally do so without using names or original health card numbers. At CIHI, data linkages are typically performed or facilitated by using the Client Linkage Standard. The Standard consists of linking clients based on the combination of the encrypted Health Card Number (HCN) and the jurisdiction issuing the HCN. As set out in the procedures related to section 14, prior approval to conduct data linkages must be obtained as per sections 22 – 27, described above. The briefing notes submitted by the program areas identify the agents who are responsible for

undertaking the linkage. The actual work may be conducted by other agents in the program area in keeping with the requirements of their position.

Moreover, where the data linkage is conducted by CIHI on behalf of a third party, the resulting linked data are de-identified prior to disclosure. Section 51 of CIHI's *Privacy Policy, 2010*, requires that program areas evaluate the de-identified data to assess and subsequently minimize privacy risks of re-identification and residual disclosure, and to implement the necessary mitigating measures to manage residual risks. That said, there may be instances where the data requester is legally authorized to obtain personal health information in linked form, for example, to a researcher under section 44 or to a prescribed entity under section 45 of PHIPA or with the informed consent of the individuals concerned. In such cases, the linked data remain subject to the use and disclosure provisions in the *Privacy Policy, 2010*.

Retention of Linked Records of Personal Health Information

Section 4.d of CIHI's *Privacy and Security Framework, 2010,* addresses, at a high level, the secure retention of records in both paper and electronic form, including linked data sets. It recognizes that information is only secure if it is secure throughout its entire lifecycle: creation and collection, access, retention and storage, use, disclosure and disposal. Accordingly, CIHI has a comprehensive suite of policies and the associated standards, guidelines and operating procedures that reflect best practices in privacy, information security and records management for the protection of the confidentiality, integrity and availability of CIHI's information assets.

Secure Disposal of Linked Records of Personal Health Information

Section 29 of CIHI's *Privacy Policy, 2010*, further requires that for linked data, secure destruction will occur within one year after publication of the resulting analysis, or three years after the linkage, whichever is sooner, in a manner consistent with CIHI's *Secure Destruction Standard*. For linked data resulting from a CIHI ongoing program of work, secure destruction will occur when the linked data are no longer required to meet the identified purposes, in a manner consistent with CIHI's *Secure Destruction Standard.*

Tracking Approved Linkages of Records of Personal Health Information

Section 21.4 of CIHI's *Privacy Policy Procedures* requires Privacy and Legal Services to maintain a log of approved linkages of records of personal health information and de-identified data and maintain all documentation relating to the requests for data linkage.

Compliance, Audit and Enforcement

The *Privacy Policy, 2010*, sets out that CIHI's Code of Business Conduct describes the ethical and professional behaviour related to work relationships, information – including personal health information – and the workplace. The Code requires all employees to comply with the Code and all CIHI's policies, protocols and procedures, including CIHI's *Privacy Policy, 2010*. Compliance with CIHI's privacy program is monitored through CIHI's risk-based privacy audit program set out in a multi-year audit plan. Instances of non-compliance with privacy and security policies are managed through CIHI's *Privacy and Security Incident Management*

Protocol. Violations of the Code are referred to Human Resources, as appropriate, and may result in disciplinary action up to and including dismissal.

23. Log of Approved Linkages of Records of Personal Health Information

As stated above, CIHI maintains a log of *all* approved linkages of personal health information *and de-identified data*. The following data elements are contained in the log:

- The name of the third party or the CIHI department that requested the linkage
- The date that the linkage was approved
- The nature of the records linked
- The scheduled date of data destruction

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

Prescribed entities are required to have a policy and procedures to ensure that personal health information will not be used or disclosed if other information, namely de-identified and/or aggregate information, will serve the identified purpose.

CIHI's *Privacy Policy, 2010*, states this as its starting point. Specifically, section 3 of CIHI's *Privacy Policy, 2010*, states that CIHI data disclosures are made at the highest degree of anonymity possible while still meeting the research and/or analytical purposes. This means that, whenever possible, data are aggregated. Where aggregate data are not sufficiently detailed for the purposes, CIHI de-identifies personal health information using the appropriate methodologies to reduce the risks of re-identification and residual disclosure. Definitions of "aggregate data" and "de-identified data" are included in the *Privacy Policy, 2010*, taking into account the meaning of "identifying information" in subsection 4(2) of the Act.

Section 33 of CIHI's *Privacy Policy, 2010*, articulates CIHI's position with respect to aggregate data and cell sizes of less than five. It states that in general, CIHI makes publicly available aggregate data with units of observation no less than five. Furthermore, CIHI imposes that rule through the use of data sharing/data protection agreements and other legally binding instruments, so as to ensure that CIHI's data recipients perform cell suppression in their publications.

Sections 45 to 47 of CIHI's *Privacy Policy, 2010*, relate specifically to the disclosure of de-identified data. They read as follows:

> *45. CIHI data disclosures are made at the highest degree of anonymity possible while still meeting the research and/or analytical purposes. This means that, whenever possible, data are aggregated.*
>
> *46. Where aggregate data are not sufficiently detailed for the research and/or analytical purposes, data that have been de-identified using various de-identification processes may be disclosed to the recipient on a case-by-case basis and where the recipient has entered into a data protection agreement or other legally binding instrument with CIHI.*

47. *Only those data elements necessary to meet the identified research or analytical purposes may be disclosed.*

Section 51 of CIHI's *Privacy Policy, 2010*, and the accompanying procedures specifically designate program areas as responsible for de-identifying or aggregating information. In cases of uncertainty about de-identification processes, program area staff must consult with CIHI methodologists within the Clinical Data Standards, Quality & Methodology Unit. A key control is the requirement that program areas follow a prescribed process to review all de-identified and/or aggregate information, including cell-sizes of less than five, prior to its use or 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 an individual.

CIHI may publish from time-to-time units of observation less than five in those instances where it is deemed necessary to the value of the findings – and this determination is made on a case-by-case basis, where CIHI is satisfied that, as stated above, it is not reasonably foreseeable in the circumstances that the information could be utilized, either alone or with other information, to identify an individual.

The following de-identification processes are set out in the Definitions section of CIHI's *Privacy Policy, 2010*:

De-identification processes

Such processes include but are not limited to:

- *Removal of name and address, if present; and*
- *Removal or encryption of identifying numbers, such as personal health number and chart number;*

and may also involve:

- *Truncating postal code to the first three characters (forward sortation area);*
- *Converting date of birth to month and year of birth, age or age group; or*
- *Converting date of admission and date of discharge to month and year only;*

and then:

Reviewing the remaining data elements to ensure that they do not permit identification of the individual by a reasonably foreseeable method.

Methodologies, standards and best practices, in addition to those listed above, may evolve and be developed from time to time and followed, as appropriate, to de-identify personal health information.

CIHI's Employee Confidentiality Agreement and the related annual Renewal Agreement have been updated to include an undertaking whereby agents expressly recognize and agree not to use de-identified or aggregated information, including information in cell sizes less than five, either alone or with other information, including prior knowledge, to identify an individual. This prohibition includes attempting to decrypt encrypted information.

Compliance, Audit and Enforcement

The *Privacy Policy, 2010*, sets out that CIHI's Code of Business Conduct describes the ethical and professional behaviour related to work relationships, information – including personal health information – and the workplace. The Code requires all employees to comply with the Code and all CIHI's policies, protocols and procedures, including CIHI's *Privacy Policy, 2010*. Compliance with CIHI's privacy program is monitored through CIHI's risk-based privacy audit program set out in a multi-year audit plan. Instances of non-compliance with privacy and security policies are managed through CIHI's *Privacy and Security Incident Management Protocol*. Violations of the Code are referred to Human Resources, as appropriate, and may result in disciplinary action up to and including dismissal.

Modernizing CIHI's approach to data de-identification

In September 2018, CIHI approved the purchase of a risk-based de-identification software solution for custom third-party record-level data requests and that can be used as well for internal analytical files. The software tool will measure the de-identification risks of both linked and unlinked data sets while preserving analytic content. Implementation of the software and the associated work to classify variables is ongoing during 2019-20 and it is expected that the tool will be implemented for record-level data files accessed via CIHI's new Secure Access Environment.

Privacy Impact Assessments

25. Privacy Impact Assessment Policy and Procedures

CIHI conducts a privacy impact assessment on every one of its data holdings. In order to keep these assessments current, CIHI adopted and implemented a *Privacy Impact Assessment Policy* as its governing document on privacy impact assessments. The *Privacy Impact Assessment Policy* clearly stipulates that the CPO is the custodian of the Policy and has the authority and responsibility for its day-to-day implementation. The Policy further stipulates that final sign-off prior to publication and external dissemination resides with both the Vice President of the relevant program area and the CPO.

Pursuant to section 1 of the *Policy*, CIHI requires that privacy impact assessments be conducted in the following circumstances:

- On existing programs, initiatives, processes and systems where significant changes relating to the collection, access, use or disclosure of personal information are being implemented.
- In the design of new programs, initiatives, processes and systems that involve the collection, access, use or disclosure of personal information or otherwise raise privacy issues. PIAs will be reviewed and amended as necessary during the design and implementation stage.
- On any other programs, initiatives, processes and systems with privacy implications as recommended by the CPO in consultation with program area or project management.

Specifically, PIAs will be conducted at the conceptual design stage and will be reviewed and amended, if necessary, during the detailed design and implementation stage. This concept, Privacy and Security by Design, is endorsed and well respected at CIHI.

The Chief Privacy Officer is the custodian of the *Policy* and has the authority and responsibility for its implementation. Part of the implementation includes the development of a timetable for the update or renewal of existing PIAs.

Under CIHI's *Privacy Impact Assessment Policy*, Directors in the Program Areas are responsible for reviewing Privacy Impact Assessments annually for discrepancies between their content and actual practices or processes, and for advising the CPO, and together they will determine if an update or a new PIA is required. The Policy requires PIAs to be updated in the following circumstances:

- significant changes occur to functionality, purposes, data collection, uses, disclosures, relevant agreements or authorities for a program, initiative, process or system that are not reflected in its PIA;
- other changes that may potentially affect the privacy and security of those programs, initiatives, processes and systems;
- the CPO determines that an update of a PIA or a new PIA is required and recommends same; or
- every five years at a minimum.

The Policy requires that CIHI's Privacy Impact Assessments must, at a minimum, describe the following:

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

- The risks to the privacy of individuals whose personal health information 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 personal health information.

Section 4 of the Policy addresses recommendation implementation. CIHI's Privacy and Legal Services maintains a log of all privacy-related recommendations including recommendations resulting from PIAs. It is in this general recommendation log that the following elements are tracked:

- the recommendations arising from the privacy impact assessment;
- the agent(s) responsible for addressing, monitoring and ensuring the implementation of the recommendations;
- the date that each recommendation was or is expected to be addressed; and
- prioritized action plans, including the manner in which each recommendation was or is expected to be addressed.

Privacy and Legal Services feeds this information into CIHI's Master Log of Action Plans where it will be monitored and reported on at the corporate level. The owner of the individual action plan (Vice President or Director) is responsible for documenting the recommendations and the actions taken (or planned) to address these. Furthermore, each owner of the action plan is required to provide regular updates/presentations to CIHI's Senior Management Committee. Regular updates will continue to be provided until such time as the recommendations are fully implemented.

Sections 9, 10 and 11 of the Policy address the requirements for non-compliance and audit monitoring. Specifically, the Policy sets out that CIHI's Code of Business Conduct describes the ethical and professional behaviour related to work relationships, information – including personal health information – and the workplace. The Code requires all employees to comply with the Code and all CIHI's policies, protocols and procedures, including CIHI's *Privacy Policy, 2010*. Compliance with CIHI's privacy program is monitored through CIHI's risk-based privacy audit program set out in a multi-year audit plan. Instances of non-compliance with privacy and security policies are managed through CIHI's *Privacy and Security Incident Management Protocol*. Violations of the Code are referred to Human Resources, as appropriate, and may result in disciplinary action up to and including dismissal.

In developing the Policy, CIHI had regard to the *Privacy Impact Assessment Guidelines for the Ontario Personal Health Information Protectoin Act*, published by the IPC/ON.

26. Log of Privacy Impact Assessments

CIHI's *Privacy Impact Assessment Policy* states that Privacy and Legal Services is responsible for maintaining a scheduling log of all privacy impact assessments completed, undertaken but not complete, and others that are scheduled. The following elements are contained in the log:

- the data holding, information system, technology or program involving personal health information that is at issue;
- the date that the privacy impact assessment was completed or is expected to be completed;
- the agent(s) responsible for completing or ensuring the completion of the privacy impact assessment.

CIHI's Privacy and Legal Services maintains a log of all privacy-related recommendations including recommendations resulting from PIAs. It is in this general recommendation log that the following elements are tracked:

- the recommendations arising from the privacy impact assessment;
- the agent(s) responsible for addressing each recommendation;
- the date that each recommendation was or is expected to be addressed; and
- the manner in which each recommendation was or is expected to be addressed.

This information is subsequently fed into CIHI's Master Log of Action Plans that must be monitored and reported on at the corporate level. The owner of the individual action plan is responsible for documenting the recommendations and the actions taken (or planned) to address these. Furthermore, each owner of the action plan is required to provide regular updates/presentations to the CIHI's Senior Management Committee. Regular updates will continue to be provided until such time as the recommendations are fully implemented.

Privacy Audit Program

27. Policy and Procedures in Respect of Privacy Audits

Privacy Audits are a key component of CIHI's overall privacy program. As described in section 5 of CIHI's *Privacy and Security Framework, 2010*, and more specifically in the Terms of Reference for CIHI's Privacy Audit and Compliance Monitoring Program, CIHI carries out two types of of privacy audits:

1. *Internal Privacy Audits* **–** These audits assess internal staff compliance with CIHI's privacy policies, procedures and privacy best practices. Internal privacy audits are initiated as the need arises, and often occur within the context of CIHI internal incident and breach response processes. Internal privacy audits may also be performed in response to external factors such as an investigation, recommendation or order from a privacy commissioner/ombudsman.
2. *Third-Party Audits* – These audits focus on external recipients of CIHI data. The audits evaluate compliance with terms of the agreement governing the use of

CIHI data. The audits also make recommendations to address any issues identified.

Audits of agents permitted to access and use personal health information are carried out as part of Information Security's ongoing regular audits (see Indicators: Appendix F – CIHI's Security Audit Program).

These audits demonstrate CIHI's due diligence in evaluating all aspects of its Privacy Program.

CIHI's privacy audit program is risk-based and includes a multi-year plan. Consistent with best practices, it monitors compliance with legislative and regulatory requirements, internal policy and procedure, and any other contractual obligations pertaining to privacy and security, and is at par with the requirements of the IPC/ON.

In addition to the above, the Terms of Reference for CIHI's Privacy Audit and Compliance Monitoring Program detail the process for conducting the audit, including criteria for selecting the subject matter, when notification occurs, the content of the notification, and all documentation required at the outset and conclusion of the audit and to whom it must be provided.

CIHI's Privacy Audit Program and Multi-Year Privacy Audit Plan is approved on an annual basis by the Governance and Privacy Committee of CIHI's Board of Directors. The Chief Privacy Officer reports regularly on all auditing activities, including findings and recommendations, to CIHI's Senior Management team and CIHI's Board of Directors. Summaries of audit activities are also published in CIHI's annual privacy report which receives Board approval. Privacy and Legal Services maintains a log of all privacy-related recommendations. It is in this general recommendation log that the following elements are tracked:

- The recommendations arising from internal privacy audits
- The agent(s) responsible for addressing each recommendation
- The date each recommendation was or is expected to be addressed
- The manner in which each recommendation was or is expected to be addressed.

This information is subsequently fed into CIHI's Master Log of Action Plans that must be monitored and reported on at the corporate level. The owner of the individual action plan is responsible for documenting the recommendations and the actions taken (or planned) to address these. Furthermore, each owner of the action plan is required to provide regular updates/presentations to the CIHI's Senior Management Committee. Regular updates will continue to be provided until such time as the recommendations are fully implemented.

Recommendations resulting from external data recipient audits are monitored by Privacy and Legal Services until such time as the recommendations have been implemented by the external data recipient.

All material relating to the audit is retained by Privacy and Legal Services.

28. Log of Privacy Audits

CIHI's Privacy and Legal Services maintains a schedule of privacy audits that have been approved, that are underway, and subsequently completed. The log contains the following elements:

- The nature and type of audit conducted (i.e., internal privacy audit, third-party audit)
- The status of the audit and subsequently, the date the audit was completed
- The agents(s) responsible for completing the audit.

Privacy and Legal Services maintains a log of all privacy-related recommendations, for both internal and external privacy audits. It is in this general recommendation log that the following elements are tracked:

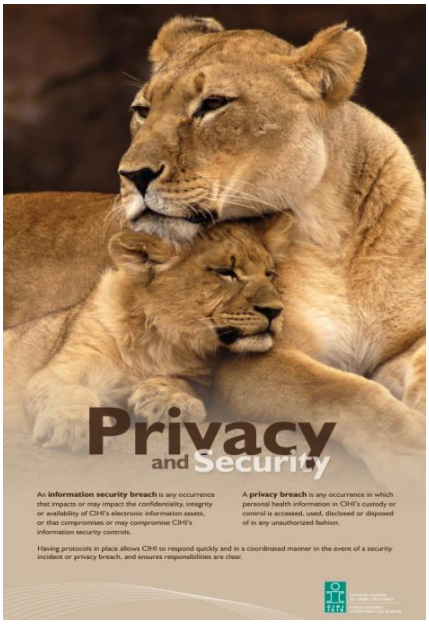
- The recommendations arising from program area or topic audits
- The agent(s) responsible for addressing each recommendation
- The date each recommendation was or is expected to be addressed
- The manner in which each recommendation was or is expected to be addressed.

For internal privacy audits, this information is subsequently fed into CIHI's Master Log of Action Plans that must be monitored and reported on at the corporate level. The owner of the individual action plan is responsible for documenting the recommendations and the actions taken (or planned) to address these. Furthermore, each owner of the action plan is required to provide regular updates/presentations to the CIHI's Senior Management Committee. Regular updates will continue to be provided until such time as the recommendations are fully implemented.

Recommendations resulting from external data recipient audits are monitored by Privacy and Legal Services until such time as the recommendations have been implemented by the external data recipient and noted in the log. Results of external data receipient audits are also reported to the Governance and Privacy Committee of CIHI's Board of Directors.

Privacy Breaches, Inquiries and Complaints

29. Policy and Procedures for Privacy and Security Breach Management



CIHI's *Privacy and Security Incident Management Protocol* is an internal management tool which is intended to enable CIHI to respond to and resolve both privacy and security incidents and breaches promptly and effectively. It addresses incident reporting, containment and preliminary assessment, communcation/notification and investigation/remediation/ prevention of future incidents.The Protocol makes it mandatory for CIHI agents to immediately report all privacy and security breaches or incidents. To make it easy for agents to do so, CIHI has established a centralized mailbox (Incident@cihi.ca) to which agents are directed to report real or suspected privacy and security incidents or breaches. This ensures that both the Chief Privacy Officer and the Chief Information Security Officer are informed immediately of any such incident or breach.

The *Privacy and Security Incident Management Protocol* defines a breach as any event that

- results in CIHI's information assets that contain personal health information being accessed, used, copied, modified, disclosed or disposed of in an unauthorized fashion, either deliberately or inadvertently (privacy breach); or
- compromises CIHI's information security controls (security breach).

An incident is any event that

- Affects or has the potential to affect the confidentiality, integrity or availability of CIHI's information assets;
- Compromises or has the potential to compromise CIHI's information security controls;
- May result in unauthorized use, access, copying, modification, disclosure or disposal of CIHI's information assets; or
- Is a suspected privacy or security breach.

When reporting incidents and breaches to incident@cihi.ca, the Protocol reminds agents to include the following information: when the incident was discovered; how it was discovered; its location, its cause (if known); the individuals involved; and any other relevant information, including any immediate steps taken to contain it.

Upon being notified of an incident, the Incident Response Team is assembled and starts managing the incident. CIHI's Core Incident Response Team consists of the Chief Privacy Officer and the Chief Information Security Officer, or delegate, who have authority to manage the privacy program and the security program, respectively.

The Core Incident Response Team will assess the nature of the incident and determine if it is classed as major or minor. Minor Incidents can be dealt with by the Core Incident Response Team with involvement of others at their discretion. Major Incidents require a formal Incident management response and additional representation on the Incident Response Team. The specific composition of the Incident Response Team beyond the core team will depend on the nature of each Incident; however, at minimum, the following staff members (or their delegates) must be included:

- Management / Senior Management representation from all affected program areas within CIHI, even if not directly required for Incident management activities;
- Management / Senior Management representation from all affected ITS departments or branches; and
- A representative from Service Desk (for Incidents involving CIHI's applications or technologies).

The IRT will determine the scope of the Incident and identify the following:

- The Incident Owner;
- Composition of the IRT beyond the initially identified team;
- Containment measures that may be required, including the need to shut down systems or services;
- Communication requirements, both internally and externally;
- Potential or actual harm as a result of the Incident;
- Any other requirements as dictated by the nature of the Incident; and
- A schedule for further calls or meetings as required.

The IRT performs a preliminary assessment of the Incident and ensures all necessary containment measures are taken.

The purpose of the preliminary assessment is to determine the immediate scope of the Incident – the affected data, systems, users and stakeholders.

Containment measures are addressed in CIHI's *Privacy and Security Incident Management Protocol*, including the responsibilities of agents under the Protocol to immediately report incidents, including any immediate steps taken to contain the incident, and the documentation that must be provided.

Containment measures may include activities such as:

- Secure retrieval or destruction of affected data or copies of data;
- Shutting down applications or services;
- Removing access to applications or services for specific individuals or groups of individuals;
- A temporary or permanent work-around to contain/avoid the Incident;
- Temporary or permanent changes to processes;
- A temporary freeze on application releases or production activities.

The Incident Response Team must notify the President and CEO at the earliest opportunity of a suspected privacy or security breach. The President and CEO, in consultation with the Incident Response Team, determines whether a privacy or security breach has occurred. Consideration is given to any legislative requirements or contractual arrangements to which the information may be subject.

In the event of a privacy or security breach, the notification process (i.e., when to notify, how to notify, who should notify, and what should be included in the notification) will be determined by the President and Chief Executive Officer, in consultation with the Incident Response Team. This determination will be made on a case-by-case basis, with consideration of guidelines or other material published by privacy commissioners or other regulators, and in keeping with any specific requirements for notification that may be found in legislation or agreements with data providers.

The Incident Response Team will direct internal and external communication as required, consulting with Communications and others as deemed necessary.

Privacy and security breaches will be reported to the Governance and Privacy Committee of CIHI's Board of Directors.

The Incident Response Team is responsible for investigation of the incident and determining, where possible, the root cause of the Incident, as well as any remediation activities required to minimize the likelihood of a recurrence. These remediation activities may be in the form of formal recommendations in an Incident Report. An Incident Report must be produced for all major Incidents, or when the Incident Response Team deems it necessary. Incident Reports must be produced in a timely manner. The Protocol contains an Incident Management Checklist identifying who is responsible for each activity, including any documentation requirements.

Incident reports containing recommendations will be submitted to the Privacy, Confidentiality and Security Committee for review prior to final submission to CIHI's Senior Management Committee for inclusion in the Master Log of Action Plans. The owners of the individual recommendations are responsible for documenting the actions taken (or planned) to address the recommendations. Furthermore, each recommendation owner is required to provide regular updates/presentations to the CIHI's Senior Management Committee. Regular updates will continue to be provided until such time as the recommendations are fully implemented.

With respect to third-party data recipients and data-sharing partners who obtain data from CIHI, they are required to notify CIHI at the earliest opportunity of real or suspected breaches through contractual obligations in data protection agreements, data sharing agreements or other legally-binding instruments. CIHI has an unfettered right to audit recipients. CIHI, therefore, monitors compliance by conducting privacy audits of external recipients.

The *Privacy and Security Incident Management Protocol* identifies Privacy and Legal Services as being responsible to maintain a log of privacy breaches and Information Security as being resposnible to maintain a log of security breaches. Compliance with the *Privacy and Security*

Incident Management Protocol is addressed in the Protocol itself, as well as in the Code of Business Conduct.

30. Log of Privacy Breaches

Privacy and Legal Services maintains a log of privacy breaches. The log and/or the accompanying breach management report contain the following elements:

- The date of the breach
- The date that the privacy breach was identified or suspected;
- Whether the privacy breach was internal or external;
- The nature of the personal health information that was the subject matter of the privacy breach and the nature and extent of the privacy breach;
- The date that the privacy breach was contained and the nature of the containment measures;
- Where applicable, the date that the health information custodian or other Organization that disclosed the personal health information to CIHI was notified;
- The date that the investigation of the privacy breach was completed;
- The agent(s) responsible for conducting the investigation.

As well, Privacy and Legal Services maintains a log of all privacy-related recommendations. It is in this general recommendation log that the following elements are tracked:

- 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 Inquiries, Concerns or Complaints

Sections 64 to 66 of *CIHI's Privacy Policy, 2010*, and related *Privacy Policy Procedures*, address the receiving, documenting, tracking, investigating, remediating and responding to privacy inquiries, concerns or complaints. As defined in section 64.1 of the *Privacy Policy* Procedures, a privacy inquiry is an inquiry relating to the privacy policies, procedures and practices implemented by CIHI and related to the compliance of CIHI with the *Act* and its regulation. A privacy complaint includes concerns or complaints relating to the privacy policies, procedures and practices implemented by CIHI and related to the compliance of CIHI with the *Act* and its regulation

Section 64.2 of the *Privacy Policy Procedures* sets out that inquiries, concerns or complaints related to the privacy policies, procedures and practices implemented by CIHI or to CIHI's compliance with the Act and its regulation are to be addressed to CIHI's Chief Privacy Officer, whose contact information is included in the *Policy* itself (section 64). Furthermore, as stated in section 65 of CIHI's *Privacy Policy, 2010*, the Chief Privacy Officer may direct an inquiry or complaint to the privacy commissioner of the individual's jurisdiction.

Section 64.3 of the *Privacy Policy Procedures* require that the following information must be communicated to the public:

- The title, mailing address and contact information of the agent to whom concerns or complaints may be directed;
- Information relating to the manner in which and format in which privacy concerns or complaints may be directed to CIHI;
- That individuals be advised that they make a complaint regarding compliance with the Act and its regulation to the Information and Privacy Commissioner of Ontario; and
- That the mailing address and contact information for the Information and Privacy Commissioner of Ontario be provided.

All of this information is made available on CIHI' external website.

Upon receipt of a privacy complaint, section 64.5 of the *Privacy Policy Procedures* sets out that the Chief Privacy Officer or designate is responsible to determine whether or not the privacy complaint will be investigated based on the definition set out in section 64.1. The timeframe within which this determination must be made is 15 days from receipt of the complaint.

Section 64.5 of the *Privacy Policy Procedures* sets out the process as follows:

- An individual may make a written inquiry or complaint to the Chief Privacy Officer about CIHI's compliance with its privacy principles, policies, procedures or practices or with the Act and its regulation.

- The written inquiry or complaint must provide:
  - Contact information for communication with the complainant, such as full name, full address, phone number, fax number and e-mail address; and
  - Sufficient detail to permit investigation.

- The Chief Privacy Officer or designate will send an acknowledgement that:
  - The inquiry or complaint has been received; and
  - Explains the process and timeframe.

- Where required, the Chief Privacy Officer or designate will contact the individual to:
  - Clarify the nature and extent of the inquiry or complaint; and
  - Obtain more details, if needed, to accurately locate the complainant's personal health information in CIHI's data holdings, when required to investigate the inquiry or complaint.

  The Chief Privacy Officer or designate investigates and responds to the inquiry or complaint by providing a written response to the individual that summarizes the nature and findings of the investigation and, when appropriate, outlines the measures that CIHI is taking in response to the complaint.

Section 64.6 of the *Privacy Policy Procedures* also sets out that, in the event that it is determined that an investigation will not be undertaken, a letter be provided to the individual making the privacy complaint acknowledging receipt of the privacy complaint; providing a response to the privacy complaint; advising that an investigation of the privacy complaint will not be undertaken; advising the individual that he or she may make a complaint to the Information and Privacy Commissioner of Ontario if there are reasonable grounds to believe that CIHI has

contravened or is about to contravene the *Act* or its regulation; and for providing contact information for the Information and Privacy Commissioner of Ontario.

Where an investigation of a privacy complaint will be undertaken, section 64.7 of the *Privacy Policy Procedures* set out the following responsibilities and requirements:

- The Chief Privacy Officer or designate is responsible for investigating the privacy complaint;
- The nature and scope of the investigation is to include, as appropriate, document reviews, interviews, site visits, inspections;
- The process that must be followed in investigating the privacy complaint is dependent on the nature and scope of the investigation, including the documentation that must be completed, provided and/or executed in undertaking the investigation; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation;
- The Chief Privacy Officer is delegated day-to-day authority to manage the privacy program;
- Privacy and Legal Services maintains a consolidated log of privacy recommendations, including recommendations arising from the investigation of privacy complaints; the recommendations are subsequently fed into CIHI's Master Log of Corporate Action Plans, are monitored and reported on at the corporate level. The owner of the individual action plan (i.e., recommendation) is responsible for documenting the recommendations and the actions taken (or planned) to address them. Furthermore, each owner of the action plan related to a recommendation is required to provide regular updates / presentations to the Senior Management Committee. Regular updates will continue to be provided to the Senior Management Committee until such time as the recommendations are addressed. Review of the Corporate Action Plans is included in the Terms of Reference for the Senior Management Committee.
- The Chief Privacy Officer or designate is responsible to determine, on a case-by-case basis, the nature of the documentation that will be completed, provided and/or executed at the conclusion of the investigation of the privacy complaint, the agent(s) in Privacy and Legal Services responsible for completing, preparing and/or executing the documentation; the agent(s) to whom the documentation must be provided; and the required content of the documentation.
- The Chief Privacy Officer is responsible to determine, on a case-by-case basis, the manner and format in which the findings of the investigation of the privacy complaint, including recommendations arising from the investigation and the status of implementation of the recommendations, are communicated; the agent(s) responsible for communicating the findings of the investigation; the mechanism and format for communicating the findings of the investigation; the time frame within which the findings of the investigation must be communicated; and to whom the findings must be communicated, including the Chief Executive Officer.
- The Chief Privacy Officer or designate is required, within 30 days from the date the determination was made to conduct the investigation to notify the individual making the privacy complaint, in writing, of the nature and findings of the investigation and of the measures taken, if any, in response to the privacy complaint; that he or she may make a

complaint to the Information and Privacy Commissioner of Ontario if there are reasonable grounds to believe that the Act or its regulation has been or is about to be contravened; contact information for the Information and Privacy Commissioner of Ontario shall also be provided;

- The Chief Privacy Officer or designate is responsible to determine on a case-by-case basis if notification is required to any other person or organization of privacy complaints and the results of the investigation of privacy complaints and, if required, will be provided in writing and as soon as practicable;
- The Chief Privacy Officer or designate is responsible for providing the notification;
- Privacy and Legal Services is responsible to maintain a log of privacy complaints and to track whether the recommendations arising from the investigation of privacy complaints are addressed within the identified timelines;
- Privacy and Legal Services is responsible to retain documentation related to the receipt, investigation, notification and remediation of privacy complaints.

Compliance, Audit and Enforcement

The *Privacy Policy, 2010*, sets out that CIHI's Code of Business Conduct describes the ethical and professional behaviour related to work relationships, information – including personal health information – and the workplace. The Code requires all employees to comply with the Code and all CIHI's policies, protocols and procedures, including CIHI's *Privacy Policy, 2010*. Compliance with CIHI's privacy program is monitored through CIHI's risk-based privacy audit program set out in a multi-year audit plan. Instances of non-compliance with privacy and security policies are managed through CIHI's *Privacy and Security Incident Management Protocol*. Violations of the Code are referred to Human Resources, as appropriate, and may result in disciplinary action up to and including dismissal.

32. Log of Privacy Complaints

CIHI has set up a log of privacy complaints containing the following information:

- The date that the privacy complaint was received and the nature of the privacy complaint;
- The determination as to whether or not the privacy complaint will be investigated and the date that the determination was made;
- The date that the individual making the complaint was advised that the complaint will not be investigated and was provided a response to the complaint;
- The date that the individual making the complaint was advised that the complaint will be investigated;
- The agent(s) 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 each recommendation;
- The date each recommendation was or is expected to be addressed;
- The manner in which each recommendation was or is expected to be addressed; and
- The date that the individual making the privacy complaint was advised of the findings of the investigation and the measures taken, if any, in response to the privacy complaint.

Part 2 - Security Documentation

General Security Policies and Procedures

1. Information Security Policy

CIHI's *Privacy and Security Framework, 2010*, is the backbone of CIHI's overall privacy and security programs which also includes security specific policies, procedures and protocols. CIHI also has developed an overarching *Information Security Policy* that sets out its commitment to secure the personal health information under its control. Of equal importance is the commitment that CIHI take reasonable steps to ensure that personal health information is protected against loss or theft as well as unauthorized access, disclosure, copying, use, modification and disposal, in a manner that is at par with the requirements of the IPC/ON.

Accountability must start at the top of an organization and therefore CIHI's *Privacy and Security Framework, 2010*, clearly indicates that the President and Chief Executive Officer is ultimately accountable for privacy and security. The Framework also clearly indicates that day-to-day authority to manage the security program has been delegated to the Chief Information Security Officer. The structure, duties and functions of the key security roles are clearly articulated in section 2 of CIHI's *Privacy and Security Framework, 2010*.

CIHI's *Information Security Policy* mandates a comprehensive Information Security Program that consists of industry standard administrative, technical and physical safeguards to protect personal health information and that is subject to independent verification. CIHI has implemented a security governance structure to ensure compliance with its security policies, practices and procedures.

CIHI's *Information Security Policy* sets out the requirements of CIHI's Information Security Program as follows:

- A security governance model;
- Ongoing review of the security policies, procedures and practices implemented;
- An Information Security awareness and training program for all staff;
- Policies, standards and/or procedures that ensure:
  - The physical security of the premises;
  - The security of the information processing facilities;
  - The protection of information throughout its lifecycle – creation, acquisition, retention and storage, use, disclosure and disposal;
  - The protection of information in transit, including requirements related to mobile devices;
  - The protection of information accessed remotely;
  - Access controls and authorizations for information and information processing facilities;

- The acquisition, development and maintenance of information systems, correct processing in applications, cryptographic controls, security of system files, security in development and support procedures and technical vulnerability management;
- Security audits including monitoring, maintaining and reviewing system control and audit logs;
- Network security management, including patch management and change management;
- The acceptable use of information technology;
- Back-up and recovery;
- Information security incident management; and
- Protection against malicious and mobile code.

In addition, CIHI has implemented an information security audit program that measures the effectiveness of the administrative, logical and physical information security controls in place.

CIHI has implemented through its Information Security Program a security infrastructure that addresses the following:

- The transmission of personal health information over authenticated, encrypted and secure connections;
- 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.

CIHI has implemented an Information Security Management System (ISMS) that covers its IT infrastructure, platform services and data centres. The ISMS provides for the ongoing management of information security based on legislative, regulatory and business requirements. As part of the ISMS, regular Threat-Risk-Assessments are performed to facilitate the ongoing management and improvement of CIHI's information security controls.

In addition to the ISMS risk assessments, CIHI assesses and addresses information security risks through its information security audit program. This program measures the effectiveness of the administrative, logical and physical information security controls that have been implemented. Specifically, audits will be used to assess the following:

- Compliance with information security policies, standards, guidelines and procedures;
- Technical compliance of information processing systems with best practices and published architectural and security standards;
- Inappropriate use of information processing systems;
- Inappropriate access to information or information processing systems;

- Security posture of CIHI's technical infrastructure, including networks, servers, firewalls, software and applications; and
- CIHI's ability to safeguard against threats to its information and information processing systems.

Compliance, Audit and Enforcement

The *Information Security Policy* sets out that CIHI's Code of Business Conduct describes the ethical and professional behaviour related to work relationships, information – including personal health information – and the workplace. The Code requires all employees to comply with the Code and all CIHI's policies, protocols and procedures. Compliance with CIHI's security program is monitored through CIHI's Information Security Audit Program and instances of non-compliance with security policies are managed through CIHI's *Privacy and Security Incident Management Protocol*. Violations of the Code, including violation of privacy and security policies, procedures and protocols, are referred to Human Resources, as appropriate, and may result in disciplinary action up to and including dismissal.

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

CIHI's *Privacy and Security Framework, 2010* clearly sets out that the Chief Privacy Officer and the Chief Information Security Officer will assume the responsibility for coordinating the review of all privacy and security policies respectively and for ensuring that the suite of privacy and security policies and procedures is comprehensive, up to date and communicated to staff, the public and other stakeholders..

All approved ISMS documentation must be reviewed on an annual basis, as per the Document Review procedure described in the ISMS Manual. The next review date is recorded on each document. All security documentation made available on CIHI's intranet must be reviewed on an annual basis by the CISO or Manager, Information Security (depending on the document up for review). The next review date is recorded on each document as well. The Coordinator, Information Security, is responsible to monitor the review dates and book meetings to review the document.

The ISMS procedures require that a designated approval authority and, where appropriate, designated consultation authorities, be named for all information security documents. Approval authorities are selected commensurate with document scope and impact to the organization. Consultation authorities are subject-matter experts who must be consulted for the particular document.

In undertaking the review and determining whether amendments are necessary, the Document Owner, in consultation with Privacy and Legal Services or others as necessary, considers the following:

- Any orders, guidelines, fact sheets and best practices issued by the federal and provincial privacy commissioners;
- Evolving industry security standards and best practices;

- Technological advancements;
- CIHI's legislative and contractual obligations, including having regard to amendments to the Act and its regulation;
- Recommendations arising from privacy and information security audits, investigations, etc.;
- Whether CIHI's actual practices continue to be consistent with its security policies, standards, guidelines, protocols and procedures;
- Whether there is consistency between and among the privacy and security policies, procedures and practices implemented; and
- Whether it is necessary to involve designated consultation authorities.

Document Owners are responsible for amending policies, procedures or practices if deemed necessary after the review. These individuals are also responsible for obtaining approval of any such amendments from the designated approval authority. The Chief Information Security Officer is responsible for identifying any required additions to the policy suite. The Chief Information Security Officer is responsible to ensure that all documents available on its external website are current and continue to be made available to the public and other stakeholders. As for internal communication to staff, the Chief Privacy Officer and the Chief Information Security Officer ensure that changes to policies, procedures and practices are communicated appropriately and may include targeted mandatory training. The latter is guided by the *Privacy and Security Training Policy* which clearly stipulates at section 6 that the Chief Privacy Officer and Chief Information Security Officer will be responsible for determining the content of privacy and security training. In addition to formal training, CIHI regularly engages in staff awareness activities such as presentations and email communications.

CIHI maintains a complete inventory of all active and inactive Information Security documentation in its Information Security Library, under the Chief Information Security Officer.

The ISMS Manual has been updated to require agents to comply with the policy and its procedures and to address how and by whom compliance will be enforced and the consequences of breach. It also stipulates that compliance will be audited in accordance with CIHI's ISMS Audit Manual.

Physical Security

3. Policy and Procedures for Ensuring Physical Security of Personal Health Information

As indicated in the introduction to this report, CIHI has offices located throughout Canada including two offices in Ontario (one in Ottawa and one in Toronto), one in British Columbia and one in Quebec. CIHI's *Security and Access Policy* governs, amongst other things, CIHI's physical safeguards to protect personal health information against theft, loss and unauthorized use or disclosure and to protect same from unauthorized copying, modification or disposal.

Compliance, Audit and Enforcement

The *Security and Access Policy* sets out that CIHI's Code of Business Conduct describes the ethical and professional behaviour related to work relationships, information – including personal health information – and the workplace. The Code requires all employees to comply with the Code and all CIHI's policies, protocols and procedures. Compliance with CIHI's privacy program is monitored through CIHI's risk-based privacy audit program set out in a multi-year audit plan. Instances of non-compliance with privacy and security policies are managed through CIHI's *Privacy and Security Incident Management Protocol*. Violations of the Code are referred to Human Resources, as appropriate, and may result in disciplinary action up to and including dismissal.

Generally, security guards are not used at entrances to CIHI offices. However, in the case of the building where the CIHI office in Toronto is located, security guards are present at the entrance to the builidng. CIHI has controlled access to its premises through a photographic card access system together with a personal identification number. CIHI agents must visibly display their security access card at all times. Doors with direct access to CIHI offices are locked at all times and alarmed and monitored after hours, on weekends and on statutory holidays. Elevator access is either limited to card access and/or locked down outside of business hours. Building locations are equipped with surveillance cameras at various points of entry. Further restrictions are imposed within CIHI premises to its server rooms/data centres where personal health information is stored in electronic format to ensure access is only provided to agents who routinely require such access for their employment, contractual or other responsibilities.

Policy, Procedures and Practices with Respect to Access by Agents

The Manager of the Corporate Administration Department is responsible for granting and revoking access to CIHI premises and to restricted areas within CIHI premises. Departmental Managers are responsible for requesting and authorizing access for their agents, including consultants and students, through CIHI's onboarding process. The onboarding process documents the process for approving access to the premises, including the level of access granted, who approves, and any required documentation. The criteria for granting access are based on the "need to know" principle and ensure that access is only provided to agents who routinely require such access for their employment, contractual or other responsibilities. Full access (24/7) to CIHI offices is granted to CIHI agents, consultants and students.

The CIHI receptionist is responsible for ensuring access to contractors (e.g., building maintenance, vendors) and delivery personnel. Contractors and delivery personnel requiring access to CIHI facilities during the hours of 8:30 a.m. to 4:30 p.m. will be provided with a contractor security access card at Reception. Contractors are required to sign a document entitled "*CIHI On-site Privacy and Security Requirements*" which sets out the rules contractors must follow while on CIHI premises.

Contactors requiring access to CIHI facilities after normal business hours will be provided with a contractor security access card by the Office Administrator upon approval by the Manager,

Corporate Administration. Contractors are required to sign a document entitled "CIHI On-site Privacy and Security Requirements" which sets out the rules contractors must follow while on CIHI premises.

The process to be followed in managing security access cards, including required documentation, is set out in the *Security and Access Policy* and related procedures, and the Manager of the Corporate Administration Department is designated as responsible for the process.

Theft, Loss and Misplacement of Security Access Cards

CIHI's *Security and Access Policy* defines the specific process to manage security access cards in the event of loss, theft, or misplacement, including to whom the notification must be provided; the nature and format of the notification; the documentation that must be completed, provided and/or executed; the agent(s) responsible for completing, providing and/or executing the documentation; the agent to whom the documentation must be provided; and the required content of the documentation. Agents who have lost their security access card must notify the Corporate Administration Department immediately via facilities@cihi.ca or by calling the local Receptionist or designated agent. Notification must indicate whether the card is lost/stolen, damaged, or defective. The Office Administrator in Corporate Administration will request a new security access card for the agent using the "Request for Security Card Access" form. The lost/stolen security access card is deactivated immediately upon receipt of the notification.

The Procedures related to the *Security and Access Policy* set out the following:

- Temporary security access cards and PINs are issued by Receptionists or other designated personnel as required (i.e. lost, stolen or damaged card) to employees only;
- When a temporary security access card is issued, the Receptionist suspends the employee's permanent access card until the temporary security access card is returned;
- One piece of government issued photo identification (e.g., driver's license, etc.) or two pieces of non-photo identification must be shown if the Receptionist does not know the employee requesting the temporary security access card;
- Alternately the employee's supervisor/manager is asked to come to reception to validate the request for a temporary security access card;
- Temporary security access cards must be returned to the Receptionist no later than 4:30 p.m.;
- In the event that temporary access cards are not returned to the Receptionist as required, the Receptionist will email the CIHI staff responsible for the card issued
- Issuing and return of the temporary access card is logged in cards log.

Termination of the Employment, Contractual or Other Relationship

The Procedures relating to the *Security and Access Policy* require agents, as well as their supervisors, to notify CIHI of the termination of their employment, contractual or other relationship with CIHI. CIHI has well established exit procedures that ensure Human Resources, Information Technology, Corporate Administration, Finance, Web Services and the business process management workflow tool team are notified of any agent terminating their relationship with CIHI and that all CIHI property, including access cards and keys, if applicable, and personal health information are securely returned. The importance of having a well-structured off-boarding process is key to ensuring prompt and timely revocation of access privileges to CIHI's premises and networks. The Senior Human Resources Assistant is responsible for initiating the off-boarding workflow in the business process management workflow tool which generates a last day email to the above-mentioned teams to notify them that an agent is leaving CIHI, as well as creating an alert to Service Desk to inform the Information Technology team of the agent's last day in the office.

The *Off-Boarding Checklist* for Managers identifies the necessary steps the Manager must complete before the agent's last day and to whom the property should be returned. The Checklist includes a requirement for the CIHI Manager to retrieve the security access card from the departing agent and return it to the Corporate Administration Department.

The Procedures associated with the *Security and Access Policy* state that security access cards assigned to students, contract agents and consultants are programmed to deactivate on the last day of the employment or contractual arrangement with CIHI.

Audits of Agents with Access to the Premises

In accordance with CIHI's *Security and Access Policy*, three types of audits are conducted by the Corporate Administration Department:

1. A weekly audit to compare the repository of active temporary security access cards against the log where the use of such cards is documented, to ensure that all cards are accounted for and to ensure that agents granted access continue to have an employment, contractual or other relationship with CIHI and continue to require the same level of access;
2. A quarterly audit of cards with access to restricted areas (Finance, Human Resources, IT), confirmed with the respective managers; and
3. Annually, every April, a visual verification is carried out by the Corporate Administration Department to ensure that agents display their security access card, that the card is in good repair and that the photographic identification is reasonable.

Tracking and Retention of Documentation Related to Access to the Premises

CIHI's *Security and Access Policy* requires that the Manager of the Corporate Administration Department is responsible for maintaining a log of agents granted approval to access CIHI premises and for all documentation related to the receipt, review, approval and termination of such access.

Notification When Access is No Longer Required

The Procedures associated with the Security and Access Policy set out the process to be followed when access is requested to restricted areas where personal health information may be retained (e.g., the Data Centres).

Access is reviewed on a quarterly basis. Managers responsible for restricted areas receive a report from Corporate Administration outlining which CIHI agents have access to their respective restricted area, validate the report, and notify Corporate Administration via email if changes to access are required.

Access may also be removed for agents:

- Who are identified as requiring access to be removed through HR off-boarding/internal movement workflows; or
- At the request of their manager.

The process to be followed in managing security access cards generally, including required documentation, is set out in the Security and Access Policy and related Procedures, and the Manager of the Corporate Administration Department is designated as responsible for the process.

Policy, Procedures and Practices with Respect to Access by Visitors

CIHI's *Security and Access Policy* sets out a comprehensive process for screening and supervising visitors to CIHI premises. Visitors are required to:

- Record their name, date, time of arrival
- Record their time of departure
- Record the name of the agent whom they are meeting
- Wear a CIHI Guest ID card at all times on the premises
- Be escorted by a CIHI agent at all times while on CIHI premises
- Return their Guest ID card upon their departure

The Guest ID card is issued for identification purposes only and does not grant access to the premises. The CIHI agent responsible for the visitor must ensure that the visitor visibly displays the Guest ID card and then returns it to the receptionist at the end of the appointment. Upon departure, the CIHI agent is responsible for signing-out the visitor and for return of the Guest ID Card. Each time a Guest ID card is issued, it is logged. These logs are reviewed daily to ensure all cards issued have been returned. In the event a card is not returned, an email is sent to the CIHI agent responsible for the card issued. Documentation relating to access by visitors is stored on the Department's SharePoint site.

4. Log of Agents with Access to the Premises of the Prescribed Person or Prescribed Entity

CIHI maintains a log of all agents granted approval to access CIHI premises. General access to CIHI premises is granted to all agents except for restricted areas such as data centers/server rooms. Access to the restricted areas is granted only to those agents who require such access for their employment, contractual or other responsibilities. The log includes the following elements:

- The name of the agent granted approval to access the premises;
- The name of the agent granted specific approval to access data centers/server rooms, IT hub rooms and Human Resources file room;
- The date that the access was granted;
- The date(s) that the secure access card was provided to the agent;
- The identification numbers on the secure access cards, if any; and
- The date that the secure access cards were returned or deactivated, if applicable.

The log is audited on an annual basis, at the same time as the physical audit of access cards, which takes place in April of every year.

Retention, Transfer and Disposal

5. Policy and Procedures for Secure Retention/Storage of Records of Personal Health Information

The secure retention of paper and electronic records of personal health information is central to CIHI's privacy and security programs. Section 4.d of CIHI's *Privacy and Security Framework, 2010*, articulates CIHI's commitment to a secure information lifecycle whereby CIHI has implemented administrative, technical and physical safeguards to protect personal health information under its control.

Section 6 of CIHI's *Privacy Policy, 2010*, states that, consistent with its mandate and core functions, CIHI may retain personal health information for as long as necessary to meet the identified purposes. At such time as personal health information is no longer required for CIHI's purposes, it is disposed of in compliance with CIHI's *Secure Destruction Policy* and the related *Secure Destruction Standard*.

CIHI's *Secure Information Storage Standard* lays out the specific methods by which records of personal health information in paper and electronic format are to be securely stored, including records retained on various media. The Standard requires that staff ensure that when storing PHI, that the following safeguards are met and provides specific guidance:

- The information must be protected against theft, loss, unauthorized use or disclosure, unauthorized copying, modification or disposal;

- The information must be stored only as long as authorized and must be securely disposed of at the end of its life (refer to CIHI's Secure Destruction Policy and Information Destruction Standard).

Staff is defined in the *Secure Information Storage Standard* to specify those CIHI agents whose role includes responsibility for the secure storage of personal health information.

The information may be stored only in authorized locations.

As well, as part of its *Security and Access Policy*, CIHI has implemented "clean desk" measures as an administrative safeguard for the protection of personal health information.

As stated in CIHI's *Privacy Policy, 2010* and its *Information Security Policy*, CIHI is committed to safeguarding its IT ecosystem, to securing its data holdings and to protecting health information with administrative, physical and technical security safeguards appropriate to the sensitivity of the information. These safeguards protect CIHI's data holdings against theft, loss, unauthorized use or disclosure, unauthorized copying, modification or disposal.

CIHI contracts with a third party service provider to retain personal health information records on its behalf for secure off-site storage of back-up media. As described in Part 1 of this Report[1], CIHI's *Procurement Policy* sets the guidelines that govern the acquisition of all goods and services by CIHI. The contractual arrangements for this service follow the requirements set out in CIHI's *Procurement Policy* and the template Services Agreement that is used for contractors providing secure retention and destruction services only.. Responsibility for ensuring that the Services Agreement with the third party providing secure retention and destruction services has been executed prior to transferring the records of personal health information for secure retention rests with the Manager responsible for the Corporate Administration Department.

CIHI's *Secure Information Transfer Standard* provides that records are transferred and retrieved in a documented and secure manner when records of personnal health information are being transferred to the third party service provider for secure retention or retrieving the records from the third party service provider, including the secure manner in which the records will be transferred and trieved, the agent(s) responsible for ensuring the secure transfer and retrieval of the records. The requirements for secure transfer are detailed in section 7, below. Infrastructure and Technology Services maintains a detailed inventory of all electronic information media that are retained by and retrieved from a third party service provider.

Paper records containing personal health information are not to be stored outside of CIHI's secure premises.

Compliance, Audit and Enforcement

The *Secure Information Storage Standard* sets out that CIHI's Code of Business Conduct describes the ethical and professional behaviour related to work relationships, information – including personal health information – and the workplace. The Code requires all employees to

1. In particular, see sections 19 and 20 – *Agreements with Third Party Service Providers*.

comply with the Code and all CIHI's policies, protocols and procedures. Compliance with CIHI's security program is monitored through CIHI's Information Security Audit Program and instances of non-compliance with security policies are managed through CIHI's *Privacy and Security Incident Management Protocol*. Violations of the Code, including violation of privacy and security policies, procedures and protocols, are referred to Human Resources, as appropriate, and may result in disciplinary action up to and including dismissal.

6. Policy and Procedures for Secure Retention of Records of Personal Health Information on Mobile Devices

The *Policy on the Security of Confidential Information and Use of Mobile Devices / Removable Media* requires:

- that agents are to perform work either on CIHI's premises or over its secure networks, using CIHI-issued computing devices/media and in keeping with CIHI's privacy and security policies, procedures, standards and guidelines; and
- that Confidential Information shall not be stored on CIHI's mobile devices or removable media except in specific and exceptional circumstances on a temporary basis where a Privacy and Security Risk Management assessment has been undertaken and where prior approval has been given by the relevant vice president.
- If approval is required, the policy and procedures must identify the process that must be followed and the agent(s) responsible for receiving, reviewing and determining whether to approve or deny a request for the retention of personal health information on a mobile device. This shall include a discussion of any documentation that must be completed, provided and/or executed; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation.
- The policy and procedures must further address the requirements that must be satisfied and the criteria that must be considered by the agent(s) responsible for determining whether to approve or deny a request for the retention of personal health information on a mobile device.
- At a minimum, prior to any approval of a request to retain personal health information on a mobile device, the policy and procedures must require the agent(s) responsible for determining whether to approve or deny the request to ensure that other information, namely de-identified and/or aggregate information, will not serve the identified purpose and that no more personal health information will be retained on the mobile device than is reasonably necessary to meet the identified purpose. The policy and procedures must also require the agent(s) responsible for determining whether to approve or deny the request to ensure that the use of the personal health information has been approved pursuant to the *Policy and Procedures for Limiting Agent Access to Personal Health Information*.
- The policy and procedures should also set out the manner in which the decision approving or denying the request is documented; the method by which and the format in which the decision will be communicated; and to whom the decision will be communicated.

The definition of Confidential Information, for purposes of this policy, includes Personal Health Information.

The *Policy on the Security of Confidential Information and Use of Mobile Devices / Removable Media* is consistent with orders issued under the Act and its regulation, as well as with the various guidelines, fact sheets and best practices issued by the IPC/ON and others in Canada[2] and with the requirements set out in the *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities*. Specifically, the Policy, Procedures or other related documents:

- Identify in what circumstances CIHI permits personal health information to be retained on a mobile device /removable media;
- Provide a definition of mobile device/removable media;
- Require agents to comply with the policy and its procedures and address how and by whom compliance will be enforced and the consequences of breach;
- Require agents to notify CIHI at the first reasonable opportunity in accordance with the *Privacy and Security Incident Management Protocol*, if an agent breaches or believes there may have been a breach of this policy or its procedures;
- Address the requirements that must be satisfied and the criteria that must be considered by the agent(s) responsible for determining whether to approve or deny a request for the retention of personal health information on a mobile device / removable media;
- Require agent(s) responsible for determining whether to approve or deny the request to ensure that the use of the personal health information has been approved in accordance with section 10 of CIHI's *Privacy Policy, 2010*;
- Set out the manner in which the decision approving or denying the request is documented, the method by which and the format in which the decision will be communicated, and to whom the decision will be communicated;
- Where mobile devices / removable media have display screens, require a mandatory standardized password-protected screen saver be enabled after a defined period of inactivity;
- Ensure that the strong and complex password for the mobile device / removable media is different from the strong and complex passwords for the files containing personal health information and that the password is supported by "defence in depth" measures;
- Detail the steps that must be taken by agents to protect the personal health information retained on a mobile device against theft, loss, and unauthorized use or disclosure and to protect the personal health information retained against unauthorized copying, modification, or disposal.

CIHI audits compliance with its privacy and security policies in accordance with its privacy and security audit programs as described in Part 1, section 27 and Part 2, section 15 of this document.

In recent years, the health sector has come to know and understand the increased risks associated with personal health information on electronic media and, in particular, the risks associated with mobile computing devices. One of the ways to mitigate risks to privacy is to

[2] See "Protecting Personal Information Away from the Office", January 2015, Office of the Information and Privacy Commissioner for British Columbia

ensure appropriate safeguards such as encryption for mobile computing devices. In Order HO-004, for example, the IPC/ON stated as follows on this issue:

> "The *Act* requires custodians to notify an individual at the first reasonable opportunity if PHI is stolen, lost or accessed by unauthorized persons. If the case can be made that the PHI was not stolen, lost or accessed by unauthorized persons as a result of the loss or theft of a mobile computing device because the data were encrypted (and encrypted data does not relate to identifiable individuals), the custodian would not be required to notify individuals under the *Act*."[3] [Emphasis added]

Where Personal Health Information is Permitted to be Retained on a Mobile Device

CIHI's *Policy on the Security of Confidential Information and Use of Mobile Devices / Removable Media* sets out as a general rule that work performed by agents is to be done on CIHI premises or over its secure networks, using CIHI-issued computing devices/media and in keeping with CIHI's privacy and security policies, procedures, standards and guidelines. Specifically, personal health information:

- Shall not be removed from CIHI premises in paper form;
- Shall not be sent by email, either internally or externally, unless authorized and with appropriate safeguards, as set out in the Secure Information Transfer Standard; and
- Shall not be stored on mobile devices or removable media except in specific and exceptional circumstances on a temporary basis where a Privacy and Security Risk Management Assessment has been undertaken and where prior approval has been given by the relevant Vice-President.

Conditions or Restrictions on the Retention of Personal Health Information on a Mobile Device

CIHI's *Policy on the Security of Confidential Information and Use of Mobile Devices / Removable Media* sets out conditions or restrictions on the retention of personal health information on a mobile device / removable media.

CIHI staff are prohibited from retaining personal health information on a mobile device or removable media if other information, such as de-identified and/or aggregate information will serve the purpose. When using mobile devices or removable media and the requisite approval has been obtained:

1. Only the minimum amount of personal health information required for the identified purpose may be stored on mobile devices and removable media on a temporary basis;
2. Once the identified purpose for temporarily storing the personal health information on mobile devices and removable media is accomplished, the personal health information shall be removed or destroyed, where possible, within 5 days of completion by following CIHI's Secure Destruction Standard; and
3. Personal health information temporarily stored on mobile devices and removable media will be:
    a. stored on CIHI-issued equipment;
    b. de-identified to the fullest extent possible; and

[3] IPC/ON, Order HO-004, March 2007 at page 20

c. encrypted and password protected in keeping with CIHI's current encryption and password standards. Mobile devices must be password protected.

Once the intended purpose for temporarily storing personal health information on mobile devices / removable media is accomplished, the personal health information must be removed or destroyed, where possible, within 5 days of completion in accordance with CIHI's Secure Destruction Standard.

In accordance with the *Policy on the Security of Confidential Information and Use of Mobile Devices / Removable Media*, agents in the Infrastructure and Business Operations team within Infrastructure and Technology Services are responsible for ensuring that all mobile devices / removable media that will contain personal health information are encrypted in compliance with CIHI's encryption standard and password protected with a password in compliance with the Infrastructure Security Standard.

Remote Network Access

CIHI's workforce is made up of agents in four offices across the country in addition to Location Independent Workers who work from a home office with an encrypted workstation. CIHI allows its staff to work remotely over its virtual private network (VPN) using CIHI-provided encrypted laptop computers. CIHI has implemented two-factor authentication for remote access to its systems. No specific approval processes are required. CIHI agents working remotely over its VPN are subject to all privacy and security policies and procedures, the same as if they were working on CIHI premises. This includes the prohibition against accessing personal health information if other information, such as de-identified and/or aggregate information, will serve the purpose and from remotely accessing more personal health information than is reasonably necessary for the identified purpose.

Conditions or Restrictions on the Remote Access to Personal Health Information

Only authorized CIHI-owned devices are allowed to connect to CIHI's networks over VPN. The following conditions and restrictions are imposed on all agents who have been granted remote access to CIHI's networks over VPN:

- The user must safeguard the device's physical security;
- The device may be used for CIHI related work only and may not be used by anyone other than the authorized user;
- Systems connected to CIHI's network over VPN are locked after 10 minutes of idle time by policy;
- .Storage of data on CIHI-issued laptops and workstations is prohibited.

Additionally, all laptops and workstations capable of accessing CIHI's networks over VPN employ whole disk encryption in addition to all information security controls employed for on-site devices.

7. Policy and Procedures for Secure Transfer of Records of Personal Health Information

CIHI's *Secure Information Transfer Standard* ensures appropriate safeguards are implemented for the secure transfer of records of personal health information in electronic format. The *Standard* takes into account any applicable Orders, guidelines, fact sheets and best practices issued by the IPC/ON under the Act and its regulation and are consistent with evolving privacy and security standards and best practices. This includes Order HO-004 and Order HO-007.

The *Standard* requires safeguards to protect personal health information from theft, loss, unauthorized use or disclosure, unauthorized copying, modification or disposal be implemented for all transfers. It sets out the conditions under which such transfers are permitted and defines the nature and content of the required documentation. Specifically:

- All electronic transfers of personal health information must
  - ensure personal health information is disseminated via one of CIHI's three approved methods, which require data files to be encrypted before and during transmission; and
  - receive prior approval by a CIHI Program Area Manager or Director, in compliance with CIHI's *Privacy Policy Procedures* (Internal Approval and Verification), or prior approval from the relevant authority, where the return of own data involving personal health information is being disseminated by encrypted email.
- CIHI agents performing the transfer of personal health information must document the following:
  - Date, time and method of transfer;
  - Recipient;
  - Nature of the records; and
  - Confirmation of receipt.

  Confirmation of receipt must be obtained and retained by the agents performing the transfer.

CIHI does not permit personal health information to be transmitted by facsimile.

CIHI has achieved 100% electronic data submission across the country and no longer collects personal health information in paper form from data submitters. Electronic data submission has a number of advantages over paper submissions, including:

- Improved security for both the data submitter and CIHI, meaning fewer risks to patient privacy and confidentiality;
- Improved data quality, as there is less manual processing; and
- Faster and more efficient submissions because no shipping is needed, thereby improving the timeliness of the data.

Compliance, Audit and Enforcement

The *Secure Information Transfer Standard* sets out that CIHI's Code of Business Conduct describes the ethical and professional behaviour related to work relationships, information – including personal health information – and the workplace. The Code requires all employees to comply with the Code and all CIHI's policies, protocols and procedures. Compliance with CIHI's security program is monitored through CIHI's Information Security Audit Program and instances of non-compliance with security policies are managed through CIHI's *Privacy and Security Incident Management Protocol*. Violations of the Code, including violation of privacy and security policies, procedures and protocols, are referred to Human Resources, as appropriate, and may result in disciplinary action up to and including dismissal.

8. Policy and Procedures for Secure Disposal of Records of Personal Health Information

CIHI ensures that the reconstruction of records of personal health information that have been disposed of is not reasonably foreseeable. To that end, CIHI has developed and operationalized its *Secure Destruction Policy* and the related *Secure Destruction Standard*. As with secure transfer, this Policy is consistent with the requirements of the Act and its regulation, as well as with factsheets, guidelines, best practices and orders issued by the IPC/ON.

The *Secure Destruction Policy* requires that information in any format, including paper or electronic, must be securely destroyed in the following circumstances:

- When the decision has been made to not retain or archive the information;
- At the end of its useful lifespan;
- In the case of electronic information, prior to repair or resale of the device upon which the information resides;
- Where otherwise required by legislation, agreements or CIHI policies and procedures.

Electronic media is securely destroyed at the end of its useful life and may not be sold or provided to any third party for reuse. That said, computing devices such as laptops and desktop computers may be disposed of by any means, provided that the information contained in the device has been securely destroyed in accordance with CIHI's *Secure Destruction Standard*.

Further, the *Secure Destruction Policy* states that individuals responsible for secure destruction must be properly trained in methods that correspond to the format, media or device, in accordance with industry best practices and CIHI standards. The *Secure Destruction Standard* requires that all media destined for destruction be kept secure. Paper must be stored in approved locked paper destruction consoles and electronic media must be stored in one of CIHI's computing centers in clearly marked and locked containers until such time as they are securely destroyed by CIHI staff or transferred to a third party for secure destruction. Secure shredding bins are available throughout CIHI's secure premises and the contents are inaccessible to staff.

The Corporate Administration Department is responsible for ensuring the secure retention of personal health information paper records pending their secure destruction by a third party service provider. The *Secure Destruction Standard* lists the approved methods of paper destruction as incineration and shredding. For shredding, the following standards must be met:

- A cross-cut or confetti-shredder must be used to destroy the document;
- The size of the material once it is shredded must be no larger than 5/8 inch.

The *Secure Destruction Standard* outlines the approved electronic information destruction methods in order of preference:

- Physical Destruction
- Degaussing
- Complete secure data wipe of hard drive
- Selected secure data wipe of individual files and folders

Destruction by a Designated Agent, Not a Third Party Service Provider

In certain circumstances, destruction of electronic information is performed by qualified ITS staff. These circumstances include the following:

- Degauss of hard drives
- Physical destruction of removable media such as CDs, DVDs
- Complete wipe of desktop or laptop hard drive prior to resale or repair
- Selective wipe of hard drive upon request for destruction of specific electronic files

The destruction process is initiated with a request to Service Desk and is tracked within the Information Technology Service Management (ITSM) tool. The destruction process with ITSM reflects the timeframe within which the destruction must be completed where this requirement exists. The process also reflects the following:

- Identification of the records of personal health information to be securely destroyed, where specifics are known (e.g. DVDs, CDs);
- Confirmation of the secure disposal of the records of personal health information;
- The method of secure disposal employed;
- The date and time the request was fulfilled; and
- The name of the agent) who performed the secure destruction.

When requested or required by data providers to securely destroy data and where a Certificate of Destruction is requested, CIHI ITS staff produce a Certificate of Destruction containing the following information and provide it within the time frame specified by the data provider:

- A description of the information that was securely disposed of;
- Confirmation that the information was securely destroyed such that reconstruction is not reasonably foreseeable;
- The date, time, location and method of secure destruction;

- The name and signature of the person who performed the secure destruction.

Destruction of Paper by a Third Party Service Provider

At CIHI, paper records are securely destroyed by a third party service provider in accordance with the contractual agreement. This agreement is based on CIHI's *Secure Destruction Standard*.

Locked paper destruction consoles are located throughout the CIHI premises. Paper records destined for destruction are placed in the locked consoles, which are clearly marked. The third party securely destroys these documents on-site every two weeks and provides a certificate of destruction to CIHI immediately upon completion. Where a third party service provider does not provide the certificate of destruction following destruction, the Corporate Administration Department follows up to ensure the certificate is provided by calling the company to have the required document sent by email.

The Certificate of Destruction contains the following information:

- Confirmation of the secure destruction of the records;
- The date, time, location and method of secure destruction employed; and
- The name and signature of the agents who performed the secure destruction.

Certificates of destruction are treated as a business record under CIHI's Records and Information Management Policy and are retained according to the corporate retention guidelines.

In instances of data destruction by third-party data requesters, tracking of secure destruction is carried out by Privacy and Legal Services – see Part 1, section 12.

Destruction of Electronic Information by a Third Party Service Provider

Where the physical destruction of electronic media is performed by a qualified third party service provider, destruction may be performed either on-site or off-site. All such arrangements are governed by written, executed agreements with the third party service providers using the Services Agreement template created by CIHI for contractors providing secure retention and destruction services only. The Services Agreement template contains all elements listed at pages 51 to 57 in the IPC/ON 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 of Safeguards; Training of Agents of the Third Party Service Provider; Subcontracting of the Services; Notification; Consequences of Breach and Monitoring Compliance and are, therefore, consistent with the requirements of the *Template Agreement for All Third Party Service Providers*. Where the work is done onsite at CIHI, certificates of destruction are provided by the third-party service provider as soon as the work is done. Where the work is done offsite, a certificate of destruction is available online. If no certificate of destruction is issued as required, follow-up occurs. To date, this has never happened. All certificates of destruction are stored, either in physical or electronic folders, as evidence of destruction for the ISO audit.

In cases where the third party performs the destruction off-site, media is first degaussed by CIHI in accordance with the *Secure Destruction Standard*.

Compliance, Audit and Enforcement

Both the *Secure Destruction Policy* and the *Secure Destruction Standard* set out that CIHI's Code of Business Conduct describes the ethical and professional behaviour related to work relationships, information – including personal health information – and the workplace. The Code requires all employees to comply with the Code and all CIHI's policies, protocols and procedures. Compliance with CIHI's security program is monitored through CIHI's Information Security Audit Program and instances of non-compliance with security policies are managed through CIHI's *Privacy and Security Incident Management Protocol*. Violations of the Code, including violation of privacy and security policies, procedures and protocols, are referred to Human Resources, as appropriate, and may result in disciplinary action up to and including dismissal.

Information Security

9. Policy and Procedures Relating to Passwords

CIHI recognizes that a rigorous approach to passwords is essential to protecting the privacy of personal health information. The CIHI *User Password Guidelines* govern the passwords used for both authentication and access to information systems whether they are owned, leased or operated by CIHI. The *Guidelines* have been developed with regard to and is consistent with orders, fact sheets, guidelines and best practices issued by the IPC/ON and also with regard to current best practices.

The *Guidelines* lay out the requirements of CIHI's default password schema which includes, for example, passwords of a minimum length and containing characters from at least four different categories (English upper case characters, English lower case characters, numeric digits and non-alphanumeric characters). The Guidelines also establish requirements for password expiration, reuse, inactivity timeouts and lockouts after failed login attempts. CIHI systems will automatically reject passwords that do not comply with the Guidelines where technology permits, that is, compliance with password requirements is enforced through group policies which is a technical control that ensures that passwords meet our complexity requirements. The User Password Guidelines impose more rigorous restrictions on administrative passwords and requires highly complex passwords up to 20 characters in length in certain circumstances. Where possible, user credentials are specific to an individual and traceable to that individual.

The *Guidelines* mandate the following administrative, technical and physical safeguards to be implemented by agents:

- Passwords may not be written down;

- Passwords may not be shared with anyone under any circumstances – and agents must change their passwords immediately if they suspect it has become known to any other individual;
- Passwords must remain hidden from view of others when being entered; and
- The use of patterns, common words, phrases, birthdays, names of places, people, pets, etc. is forbidden.

Compliance, Audit and Enforcement

The User Password Guidelines sets out that CIHI's Code of Business Conduct describes the ethical and professional behaviour related to work relationships, information – including personal health information – and the workplace. The Code requires all employees to comply with the Code and all CIHI's policies, protocols and procedures. Compliance with CIHI's security program is monitored through CIHI's Information Security Audit Program and instances of non-compliance with security policies are managed through CIHI's *Privacy and Security Incident Management Protocol*. Violations of the Code, including violation of privacy and security policies, procedures and protocols, are referred to Human Resources, as appropriate, and may result in disciplinary action up to and including dismissal.

CIHI's *Privacy and Security Incident Management Protocol* indicates that a suspected or actual compromised password is a serious information security incident and requires that the protocol be initiated in such a circumstance.

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

CIHI's *Policy on the Maintenance of System Control and Audit Logs* requires that all information systems, technologies, applications and programs involving personal health information at CIHI must contain functionality to log access, use, modification and disclosure of personal health information where technology permits.

Information to be logged shall include, where possible and appropriate, the following:

- Computer or network identification from which the connection is made
- Date/Time
- Username
- Nature of the event (creation, modification, deletion)

Information Technology & Services asset owners are responsible for ensuring that the types of events that are required to be audited are audited for all assets under their control.

Audit logs shall be available for review when required for incident management or investigation, for forensic purposes. Information Security is responsible for maintaining standards specifying the length of time that system control and audit logs are required to be retained, the agent responsible for retaining the system control and audit logs and where the system control and audit logs will be retained.

CIHI's *Policy on the Maintenance of System Control and Audit Logs* requires that CIHI must maintain practices and procedures to ensure that audit logs are protected from unauthorized access or modification.

Audit logs shall be available for review when required for incident management or investigation, for forensic purposes, or at the request of the CISO/CPO. The CISO is responsible for overseeing such reviews. Such reviews would typically be in the context of an incident investigation. Agent(s) responsible for reviewing system control and audit logs are to report to incident@cihi.ca at the first reasonable opportunity a privacy or an information security breach or suspected privacy or information security breach in accordance with the *Privacy and Security Incident Management Protocol*. Identification of agent(s) responsible for assigning other agent(s) to address the findings arising from the review of system control and audit logs, establishing timelines to address the findings, for addressing the findings and for monitoring and ensuring that the findings have been addressed will be addressed as part of the incident response.

Documentation requirements including nature, format, communication, etc., are subject to the requirements set out in CIHI's *Privacy and Security Incident Management Protocol*.

CIHI's *Policy on the Maintenance of System Control and Audit Logs* and related documents are consistent with evolving industry standards and are commensurate with the amount and sensitivity of the personal health information maintained, with the number and nature of agents with access to personal health information and with the threats and risks associated with the personal health information.

Compliance, Audit and Enforcement

The *Policy on the Maintenance of System Control and Audit Logs* sets out that CIHI's Code of Business Conduct describes the ethical and professional behaviour related to work relationships, information – including personal health information – and the workplace. The Code requires all employees to comply with the Code and all CIHI's policies, protocols and procedures. Compliance with CIHI's security program is monitored through CIHI's Information Security Audit Program and instances of non-compliance with security policies are managed through CIHI's *Privacy and Security Incident Management Protocol*. Violations of the Code, including violation of privacy and security policies, procedures and protocols, are referred to Human Resources, as appropriate, and may result in disciplinary action up to and including dismissal.

11. Policy and Procedures for Patch Management

As set out in CIHI's Data Centre Operations Guidelines, patch and vulnerability management procedures require designated owners of information processing assets to monitor the availability of patches on behalf of CIHI and to maintain patch management procedures for each asset under their control. CIHI's patch management procedures contain the following information:

- A list of all sources to be monitored for patches and vulnerabilities and the frequency with which sources should be monitored;
- Criteria for determining if a patch should be implemented;
- The maximum timeframe for categorizing a patch once its availability is known;
- If appropriate, the *Standard Operating Procedures* for patch deployment for the asset in question;
- The circumstances in which patches must be tested;
- The timeframe within which patches must be tested;
- Testing procedures;
- The agent responsible for testing;
- Documentation that must be completed for testing.

At CIHI, asset owners analyze all security patches to determine whether or not the patch should be implemented. In cases where a vendor releases a patch as a non-security update, but where the patch protects against a security vulnerability, the asset owner treats the patch as a security patch. Once a determination has been made to implement a patch, the patch is classified based on risk, where risk is determined by the severity of the vulnerability being addressed, the probability of compromise, the current mitigations in place that reduce the overall risk, and the value of the asset to the organization. At CIHI, asset owners categorize security patches within a reasonable time after notification of patch availability.

CIHI uses the following classifications for probability of compromise:

- Low – Little or no effect on the ability to facilitate an attack, not easily exploited
- Medium – Increased effect on the ability to exploit an attack, some knowledge or skill required to exploit
- High – Serious increased effect on the ability to exploit an attack, little or no knowledge required to exploit

CIHI uses the following classifications for severity of vulnerability:

- Low – Little or no impact on the confidentiality, integrity or availability of information or information processing systems and/or low value to the organization
- Medium – Moderate impact on the confidentiality, integrity or availability of information or information processing systems and/or moderate value to the organization
- High – Major impact on the confidentiality, integrity or availability of information or information processing systems and/or high value to the organization

At CIHI, risk categorization is determined by a combination of probability of compromise and severity of vulnerability. For example, a low severity and low probability would produce a very low risk, a high severity and low probability would produce a medium risk, etc., thereby informing the required course of action. Timeframes for security patch deployment depend upon the risk categorization:

- Critical – within 24 hours
- High – deploy at earliest opportunity within the next 5 business days
- Medium – Scheduled in next available maintenance window
- Low – Schedule for a maintenance window within the next three months or, with justification, within the next 12 months or, with justification, dropped altogether if the affected system/software will be upgraded or replaced within the next 12 months.

All security patch deployments are subject to current change management standards. For patches that have been implemented, all change management records are required to be maintained. The records include the following information:

- a description of the patch;
- the date that the patch became available;
- the date that the patch was tested;\The agents(s) responsible for testing the patch;
- Whether or not the testing was successful;
- the severity level and priority of the patch;
- the information system, technology, equipment, resource, application or program to which the patch relates;
- the date that the patch was implemented;
- the agent(s) responsible for implementing the patch.

Testing of patches occurs where the environment permits.

Where a decision has been made that the patch should not be implemented, the asset owner documents the following:

- A description of the patch;
- The published security level of the patch;
- The date the patch became available;
- The asset to which the patch applies; and
- The rationale for the determination that the patch should not be implemented.

Compliance, Audit and Enforcement

The Data Centre Operations Guidelines set out that CIHI's Code of Business Conduct describes the ethical and professional behaviour related to work relationships, information – including personal health information – and the workplace. The Code requires all employees to comply with the Code and all CIHI's policies, protocols and procedures. Compliance with CIHI's security program is monitored through CIHI's Information Security Audit Program and instances of non-compliance with security policies are managed through CIHI's *Privacy and Security Incident Management Protocol*. Violations of the Code, including violation of privacy and security policies, procedures and protocols, are referred to Human Resources, as appropriate, and may result in disciplinary action up to and including dismissal.

12. Policy and Procedures Related to Change Management

CIHI's Change Advisory Board (CAB) Charter governs authorization or denial of a request for a change to the operational environment at CIHI in accordance with the ITSM international standard for IT Service Management. It designates Change Managers as responsible for receiving and reviewing such requests and for determining whether to approve or deny them. Significant changes, including changes with a privacy or security impact, must be approved by the Change Advisory Board (CAB) or Emergency Change Advisory Board (eCAB).

Change Managers and the CAB follow a detailed, documented process to approve or deny a request for a change. All change requests contain the following information:

- A description of the requested change;
- The rationale for the change;
- Why the change is necessary;
- The impact and risk of executing or not executing the change to the operational environment;
- Interdependencies;
- Effort and resources required;
- Back-out possibilities;
- Deployment environments; and
- Change Manager (approver).

The final decision to approve or deny the request for a change is documented in the Request for Change (RFC) and communicated to the requestor via the IT Service Management Tool. The impact of, the urgency and the rationale for the requested change are to be considered when determining whether to approve or deny a request for change.

Where appropriate, changes must be tested in a test environment prior to production deployment, as well as post-production release testing. All of this must occur before the operational system is made available for use.

Where a request for a change to the operational environment is denied, the Change Manager or CAB member documents the rationale for denying the request. Where a request for a change to the operational environment is approved, the identified Change Analyst is responsible for determining the timeframe for implementation and the priority assigned to the change, based on CIHI's Change Categorization and Change Prioritization Models. The Change Analyst is also responsible for ensuring that all required documentation is completed.

CIHI keeps records of all changes implemented and documents the following:

- 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.

Compliance, Audit and Enforcement

The CAB Charter sets out that CIHI's Code of Business Conduct describes the ethical and professional behaviour related to work relationships, information – including personal health information – and the workplace. The Code requires all employees to comply with the Code and all CIHI's policies, protocols and procedures. Compliance with CIHI's security program is monitored through CIHI's Information Security Audit Program and instances of non-compliance with security policies are managed through CIHI's *Privacy and Security Incident Management Protocol*. Violations of the Code, including violation of privacy and security policies, procedures and protocols, are referred to Human Resources, as appropriate, and may result in disciplinary action up to and including dismissal.

13. Policy and Procedures for Back-Up and Recovery of Records of Personal Health Information

As set out in CIHI's Data Centre Operations Guidelines, secure information backup procedures cover the requirements for the back-up and recovery of records of personal health information and specify the frequency with which records of personal health information are backed-up – backups are carried out daily.

The backups are tested in the following ways:

- A monthly restore report is produced by ITS which shows all the failures of user requests to restore data from backup. ITS investigates and opens up incident tickets where required.
- Critical backup restores are tested during annual disaster recovery test exercise which occurs annually in May.

CIHI's secure information backup procedures identify the nature of CIHI's back-up devices and require that records of personal health information be backed up according to the source and nature of the information. The Manager of Infrastructure and Technology Services is responsible for all processes and procedures for the backup and recovery of information. Back-up storage devices are encrypted and are stored and transported securely. All transfers and retrievals of backed-up records are carried out in the documented secure manner as set out in CIHI's *Secure Information Transfer Standard* as described in section 7, above, and authorized staff document the date, time and mode of transfer and that written receipts of the records are provided by the third party. In addition, in accordance with the procedures, authorized staff

maintain a detailed inventory of all backed-up records that are stored with a third party service provider and of all records retrieved from same.

The information backup and recovery procedures outline the process for back-up and recovery, including requirements that must be satisfied and the required documentation. Pursuant to CIHI's information security audit procedures, the Manager of Infrastructure and Technology Services is responsible for auditing backup tape validity and integrity on an ongoing basis.

The Data Centre Operations Guidelines identify the frequency of back-ups and the length of time that back-ups are required to be retained (i.e., the retention policy). The Data Centre Operations Manual describes the location of back-ups. Backed-up records are required to be made available as required, for purposes of data restoration.

CIHI contracts with a third party service provider to retain backup media including records of personal health information. The contractual arrangements for this service follow the guidelines set out in CIHI's *Procurement Policy* and are consistent with the requirements of the *Template Agreement for All Third Party Service Providers* described at Part 1, section 20.

Compliance, Audit and Enforcement

The Data Centre Operations Guidelines set out that CIHI's Code of Business Conduct describes the ethical and professional behaviour related to work relationships, information – including personal health information – and the workplace. The Code requires all employees to comply with the Code and all CIHI's policies, protocols and procedures. Compliance with CIHI's security program is monitored through CIHI's Information Security Audit Program and instances of non-compliance with security policies are managed through CIHI's *Privacy and Security Incident Management Protocol*. Violations of the Code, including violation of privacy and security policies, procedures and protocols, are referred to Human Resources, as appropriate, and may result in disciplinary action up to and including dismissal.

14. Policy and Procedures on the Acceptable Use of Technology

A key underpinning of CIHI's privacy and security program is CIHI's *Acceptable Use of Information Systems Policy*. It outlines for all agents the acceptable use of information systems, computing devices, email, internet and networks, whether they are owned, leased or operated by CIHI. It spells out those activities that constitute authorized, unauthorized, illegal and unlawful uses of CIHI's information processing assets.

Agents may access CIHI's electronic networks, systems and computing devices in order to carry out the business of CIHI, for professional activities and reasonable personal use, and must refrain from any unauthorized, illegal or unlawful purposes. Among other things, while accessing CIHI's electronic networks, systems and computing devices, agents must adhere to *all* of CIHI's published privacy and security policies, procedures, standards and guidelines, not attempt to defeat information technology security features and not communicate CIHI confidential information, except where authorized or as required by law.

Compliance, Audit and Enforcement

The *Acceptable Use of Information Systems Policy* sets out that CIHI's Code of Business Conduct describes the ethical and professional behaviour related to work relationships, information – including personal health information – and the workplace. The Code requires all employees to comply with the Code and all CIHI's policies, protocols and procedures. Compliance with CIHI's security program is monitored through CIHI's Information Security Audit Program and instances of non-compliance with security policies are managed through CIHI's *Privacy and Security Incident Management Protocol*. Violations of the Code, including violation of privacy and security policies, procedures and protocols, are referred to Human Resources, as appropriate, and may result in disciplinary action up to and including dismissal.

Security Audit Program

15. Policy and Procedures in Respect of Security Audits

CIHI's ISMS Audit Manual requires the following audits:

- ISO/IEC 27001:2013 Certification / Recertification audit
  - Assess compliance with ISO/IEC 27001:2013
- Annual ISMS internal audit

    - Assess compliance with security policies, procedures and practices as well as ongoing compliance with ISO/IEC 27001:2013
- Annual technical vulnerability assessment and penetration testing (ethical hacks)
    - Assess the security posture of CIHI's technology and application infrastructure
- Reviews of system control and audit logs
- Ad hoc information security policy compliance audits
    - Assess staff compliance with CIHI's information security policies, procedures, standards, guidelines, protocols and best practices.
    - Performed on an as-needed basis as defined by the CISO, the CPO or the ISMS Steering Committee in consideration of risk
    - Scope and approach will be defined based on the specific requirements of each audit.

CIHI performs threat and risk assessments as part of the ISMS Risk Management program as set out in the ISMS Manual.

In addition to the prescribed audits, the Chief Information Security Officer, the ISMS Steering Committee, or CIHI Senior Management may request, at their discretion, additional audits of any components of CIHI's ISMS or security posture. All such audits shall be subject to the principles and requirements described in ISMS Audit Program. This request may be as a result of the following:

- Order/ruling from a privacy commissioner;
- Privacy or security incident or breach;
- Request from CIHI's Board of Directors, Chief Privacy Officer or Chief Information Security Officer.

CIHI's ISMS Audit policies and procedures specify the prescribed audits that must be performed and contain the following requirements:

- A description and the frequency of the audit;
- The person responsible for the audit including the documentation to be completed, provided and/or executed at the conclusion of the security audit;
- The event that triggers the audit;
- The procedures for performing the audit;
- Audit reporting;
- All recommendations are logged and tracked, action plans are developed within 30 days.

Security audits that are commissioned and conducted by external third parties are reported to CIHI's Senior Management Committee, in addition to the Finance and Audit Committee of CIHI's Board of Directors.

The Chief Information Security Officer is responsible for providing oversight to the auditing and monitoring activities specified by the ISMS. Results of all auditing and monitoring activities are reported to the ISMS Steering Committee which is chaired by the Vice President and Chief Information Officer. Recommendations contained in audit reports are tracked in the ISMS Action Log.

The ISMS Audit Manual sets out the agent(s) responsible for communicating the findings of the security audit; the mechanism and format for communicating the findings of the security audit; the time frame within which the findings of the security audit must be communicated; and to whom the findings of the security audit will be communicated, including the Chief Executive Officer or the Executive Director.

CIHI, from time to time, will commission external parties to conduct information security audits such as vulnerability assessments and ethical hacks. Recommendations arising from these audits are tracked in CIHI's Master Log of Action Plans that is monitored and reported on at the corporate level to CIHI's Senior Management Committee. The Chief Information Security Officer is responsible for documenting the recommendations and the actions taken (or planned) to address each recommendation and to provide regular updates to the Senior Management Committee.

Compliance, Audit and Enforcement

The ISMS Audit Manual sets out that CIHI's Code of Business Conduct describes the ethical and professional behaviour related to work relationships, information – including personal health information – and the workplace. The Code requires all employees to comply with the Code and all CIHI's policies, protocols and procedures. Compliance with CIHI's security program is monitored through CIHI's Information Security Audit Program and instances of non-compliance with security policies are managed through CIHI's *Privacy and Security Incident Management Protocol*. Violations of the Code, including violation of privacy and security policies, procedures and protocols, are referred to Human Resources, as appropriate, and may result in disciplinary action up to and including dismissal.

16. Log of Security Audits

CIHI's Manager, Information Security maintains a log of security audits that have been completed. The log contains the following elements:

- The nature and type of audit conducted;
- The date the audit was completed;
- The agent(s) responsible for completing the audit; and
- The recommendations arising from the audit.

The CISO maintains a log of all recommendations stemming from security audits that includes:

- The agent(s) responsible for addressing each recommendation;
- The date each recommendation was or is expected to be addressed;
- The manner in which each recommendation was or is expected to be addressed; and
- Ongoing and regular status reports on the progress of the work.

Information Security Breaches

17. Policy and Procedures for Privacy and Security Breach Management

Refer to Part I, Section 29.

18. Log of Information Security Breaches

A log of Information Security Breaches has been set up containing the following elements:

- The date of the information security breach;
- The date that the information security breach was identified or suspected;
- The nature of the personal health information, if any, that was the subject matter of the information security breach and the nature and extent of the information security breach;
- The date that the information security breach was contained and the nature of the containment measures;
- The date that the health information custodian or other organization that disclosed the personal health information to CIHI was notified, if applicable;
- The date that the investigation of the information security breach was completed;
- The agent(s) involved in conducting the investigation.

As well, Information Security maintains a log of all security-related recommendations. It is in this general recommendation log that the following elements are tracked:

- 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.

Recommendations resulting from an information security breach will be included in CIHI's Master Log of Action Plans. The owners of the individual recommendations are responsible for documenting the actions taken (or planned) to address the recommendations. Furthermore, each recommendation owner is required to provide regular updates/presentations to CIHI's Senior Management Committee. Regular updates will continue to be provided until such time as the recommendations are fully implemented.

Part 3 - Human Resources Documentation

Privacy and Security Training and Awareness

1. Policy and Procedures for Privacy and Security Training and Awareness

CIHI's *Privacy and Security Training Policy* sets out the requirements for traceable, mandatory privacy and security training for all CIHI staff. Pursuant to the *Policy*, new agents are required to complete initial privacy and security orientation training within 15 days of commencement of employment and prior to gaining access to any personal health information. The initial privacy and security orientation training is required for all individuals who are commencing an employment, contractual or other working relationship with CIHI that will require them to access CIHI data, including personal health information, or information systems as defined in CIHI's *Acceptable Use of Information Systems Policy*. CIHI's mandatory Privacy and Security Core Learning Series includes training on privacy and security fundamentals, acceptable use of information systems at CIHI, risks associated with social engineering/phishing and incident management. Moreover, every January, all CIHI staff must successfully complete CIHI's mandatory privacy and security annual renewal training, prior to January 31st.

The *Privacy and Security Training Policy* designates the Chief Privacy Officer as being responsible for determining the content of privacy training, and the Chief Information Security Officer as being responsible for determining the content of security training. The mandatory training modules are delivered electronically through CIHI's Learning and Professional Development Program's eLearning Portal.

Initial privacy and security orientation training is delivered to every new-hire[1]. The Human Resources Generalist provides orientation to all new agents on their first day of employment. The mandatory privacy and security training is referenced and explained within this session and agents) are provided a checklist in their orientation package which includes the requirement to complete the privacy and security orientation training. Generally, completion of the training occurs on the first day of employment or as soon as possible thereafter, but within 15 days of commencement of employment, as stipulated in the *Privacy and Security Training Policy*. Once completed, the agent is required to indicate completion of training by completing the task in the business process management workflow tool. Completion of mandatory privacy and security training is monitored via a web-based tracking tool linked to CIHI's Learning Management System.

[1] New-hires include all full-time, part-time and contract agents of CIHI, individuals working at CIHI on secondment and students.

CIHI's on-boarding process for all new hires as well as for external professional services consultants, who must also meet mandatory training requirements, ensures that the training is completed within the timeframe set out in CIHI's *Privacy and Security Training Policy*.

The privacy and security orientation training is updated and adjusted periodically. The *Privacy and Security Training Policy* sets out the following required elements of CIHI's privacy and security training program to ensure its accuracy and relevancy:

- CIHI's status under the Act and the duties and responsibilities that arise as a result of this status;
- The nature of the personal health information collected and from whom this information is typically collected;
- The purposes for which personal health information is collected and used and how this collection and use is permitted by the Act and its regulation;
- Limitations placed on access to and use of personal health information by agents;
- The procedure that must be followed in the event that an agent is requested to disclose personal health information;
- An overview of CIHI's privacy and security policies, procedures and practices and the obligations arising from these policies, procedures and practices;
- The consequences of breach of the privacy and security policies, procedures and practices implemented;
- An explanation of the privacy program, including the key activities of the program and the Chief Privacy Officer;
- An explanation of the security program, including the key activities of the program and of the Chief Information Security Officer
- The administrative, technical and physical safeguards implemented by CIHI to protect personal health information against theft, loss and unauthorized use or disclosure and to protect records of personal health information against unauthorized copying, modification or disposal;
- The duties and responsibilities of agents in implementing the administrative, technical and physical safeguards put in place by CIHI;
- A discussion of the nature and purpose of the Confidentiality Agreement that agents must execute and the key provisions of the Confidentiality Agreement; and
- An explanation of the *Privacy and Security Incident Management Protocol* and the duties and responsibilities imposed on agents in identifying, reporting, containing and participating in the investigation and remediation of privacy and security incidents.

As set out in section 7 of CIHI's *Privacy and Security Training Policy*, in addition to mandatory privacy and security orientation and renewal training, all CIHI staff are required to successfully complete additional training as identified by the Chief Privacy Officer and the Chief Information Security Officer. For example, this additional training may be in response to a privacy breach or security incident, the release of findings from a privacy or security audit, or the adoption and implementation of new policies and procedures. In addition to the mandatory privacy and security training described above, other role-based training is provided to staff, as needed and

as determined by the CPO for privacy training or the CISO for security training. In these instances as well, completion of the training is tracked. Privacy and Legal Services is responsible for tracking the completion of annual renewal training, including completion of the form *Annual Renewal of CIHI Employee Agreement Respecting Confidential Information and Privacy,* as well as any other additional mandatory privacy and security training that may be identified by the CPO and/or the CISO.

In order to ensure compliance with the mandatory training requirements, and in accordance with its *Privacy and Security Training Policy*, CIHI logs completion of all mandatory privacy and security training. Privacy and Legal Services is responsible for ensuring compliance across the organization. CIHI's on-boarding process addresses the role of Managers as it relates to the initial mandatory training. It states that Managers are also responsible for confirming completion by completing the On-Boarding Checklist and submitting confirmation via the business process management workflow tool.

As described in CIHI's *Privacy and Security Training Policy*, the mandatory privacy and security training requirements imposed by CIHI must be met prior to gaining initial access to data and on an annual basis thereafter in order to retain access privileges. Failure to complete mandatory privacy and security training will result in denial or revocation of access to data or other components of CIHI's network. In addition to denial or revocation of access, failure to complete mandatory training may result in disciplinary action, including the termination of employment or other relationship with CIHI.

CIHI's *Privacy and Security Training Policy* identifies that agents are required to comply with the Policy, informs them of the consequences of non-compliance and that compliance is monitored and that instances of non-compliance are managed through CIHI's *Privacy and Security Incident Management Protocol*.

CIHI is committed to ensuring a culture of privacy and security at CIHI through an ongoing awareness program in addition to its formal training program, and has consequently adopted a multi-pronged approach to raising awareness. This includes:

- articles on *CIHighway* (CIHI's intranet-based communication mechanism);
- staff presentations and special presentations at departmental meetings;
- "*January is Privacy Awareness Month at CIHI*" campaign;
- "*September is Information Security Awareness Month at CIHI*" campaign;
- SmallTalks (lunch and learns);
- privacy and security awareness posters and mouse pads;
- summary of investigations completed by privacy commissioners and ombudsmen across Canada, where orders have been issued, that are health care related and could have implications for CIHI with respect to managing its privacy and security program;
- Incident Management desk-top tool provided to all staff;
- all-staff emails; and

- technical training for specific positions.

As set out in CIHI's *Privacy and Security Training Policy*, the CPO and the CISO are responsible to determine the frequency and the method and the nature of the above communications.

2. Log of Attendance at Initial Privacy and Security Orientation and Ongoing Privacy and Security Training

CIHI's Learning Management System logs the completion dates for all agents' mandatory privacy and security training.

3. Policy and Procedures for Security Training and Awareness

Refer to section 1, above.

4. Log of Attendance at Initial Security Orientation and Ongoing Security Training

Refer to section 2, above.

Confidentiality Agreements

5. Policy and Procedures for the Execution of Confidentiality Agreements by Agents

CIHI requires all agents who enter into an employment, contractual or other relationship with CIHI to execute a Confidentiality Agreement in accordance with the *Template for Confidentiality Agreements* – prior to being given access to personal health information. This requirement, in addition to a yearly renewal, is set out in CIHI's *Code of Business Conduct*. Renewal takes place in January as part of CIHI's "*January is Privacy Awareness Month*" campaign and is recorded electronically. Privacy and Legal Services is responsible for tracking the completion of annual renewal training, including completion of the form *Annual Renewal of CIHI Employee Agreement Respecting Confidential Information and Privacy*, One hundred per cent completion is required and is ensured by monitoring and direct follow-up with agents. Amongst other things, the renewal states that agents are prohibited from using de-identified or aggregate information, either alone or with other information, to identify an individual. This obligation also extends to external consultants and other third-party service providers who may be granted access to CIHI data.

At CIHI, the employment contract states that all agents must review and sign the *Agreement Respecting Confidential Information, Privacy and Intellectual Property Rights* (Confidentiality Agreement). Human Resources and Administration has processes in place to ensure that the Confidentiality Agreement is executed for each new agent. The Confidentiality Agreement is included in the employment offer package and new agents are required to sign and return the Agreement prior to starting their employment at CIHI. The Senior Human Resources Assistant updates the New Hire tracking sheet indicating they received the Confidentiality Agreement as well as the employment contract. The Confidentiality Agreement is stored in the agent file.

Human Resources and Administration also has set up a log of executed Confidentiality Agreements. The Manager, Human Resources, is responsible for ensuring that the log is maintained and the appropriate processes are in place to ensure that the Confidentiality Agreement is executed for each new agent.

6. Template Confidentiality Agreement with Agents

CIHI's Confidentiality Agreement with agents addresses all elements listed in the *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities*, issued by the IPC/ON, namely, all items in the General Provisions; Obligations with Respect to Collection, Use, and Disclosure of Personal Health Information; Termination of the Contractual, Employment or Other Relationship; Notification; and Consequences of a Breach and Monitoring Compliance. For example, and without limitation, key provisions include:

- A definition of personal health information that is consistent with the definition that is contained in PHIPA;
- Statement that the employee is an agent of CIHI in respect of personal health information;
- A description of CIHI's status as a prescribed entity under PHIPA including its duties and responsibilities arising from this status;
- Requirement for the employee to comply with PHIPA and its regulation as it relates to prescribed entities;
- Requirement that the employee has familiarized him or herself with, and agrees to comply with, CIHI's privacy and security policies and procedures, including those implemented following execution of the Confidentiality Agreement;
- Requirement that the employee complies with the Confidentiality Agreement as may be amended from time to time.
- Indication of the purposes for which agents are permitted to collect, use and disclose personal health information on behalf of CIHI, and any related conditions.
- A prohibition against collecting and using personal health information except as permitted in the Confidentiality Agreement, and from disclosing such information except as permitted in the Confidentiality Agreement or as required by law.
- A prohibition against collecting, using or disclosing personal health information if other information will serve the purpose, and from collecting, using or disclosing more personal health information than is reasonably necessary to meet the purpose.
- A requirement that the employee return all personal health information to CIHI on or before the termination of employment.

- Stipulation of the time frame and method regarding which the personal health information must be securely returned to CIHI.

- A requirement that the employee notify CIHI, in accordance with the relevant procedures, of a breach/potential breach of the Confidentiality Agreement or one of CIHI's policies or procedures.

- Stipulation of the consequences of breach of the agreement, and stipulation of how compliance with the Confidentiality Agreement will be audited.

7. Log of Executed Confidentiality Agreements with Agents

The log of confidentiality agreements with agents includes the name of the agent, the date of commencement of employment and the date that the Confidentiality Agreement was executed.

With respect to the annual renewal of Confidentiality Agreements, tracking is recorded electronically and 100% completion ensured by monitoring and direct follow-up with agents, in a manner at par with the requirements of the IPC/ON.

Responsibility for Privacy and Security

8. Job Description for the Chief Privacy Officer

At CIHI, the Chief Privacy Officer has been delegated day-to-day authority to manage the privacy program. The Chief Privacy Officer reports directly to the Vice President, Corporate Services, who reports to CIHI's President and CEO.

The job description for the Chief Privacy Officer identifies the key responsibilities and obligations for the role and includes the minimum obligations set out in the *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities*, issued by the IPC/ON, namely:

- Developing, implementing, reviewing and amending privacy policies, procedures and practices;
- Ensuring compliance with the privacy policies, procedures and practices implemented;
- Ensuring transparency of the privacy policies, procedures and practices implemented;
- Facilitating compliance with the Act and its regulation;
- Ensuring agents are aware of the Act and its regulation and their duties thereunder;
- Ensuring agents are aware of CIHI's privacy policies, procedures and practices and are appropriately informed of their duties and obligations thereunder;
- 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 privacy impact assessments;

- Receiving, documenting, tracking, investigating, remediating and responding to privacy complaints pursuant to CIHI's *Privacy Policy, 2010*, and related *Privacy Policy Procedures*;
- Receiving and responding to privacy inquiries pursuant to CIHI's *Privacy Policy, 2010*, and related *Privacy Policy Procedures*;
- Receiving, documenting, tracking, investigating and remediating privacy breaches or suspected privacy breaches pursuant to the *Privacy and Security Incident Management Protocol*; and
- Conducting privacy audits pursuant to the Privacy Audit Program – Terms of Reference.

9. Job Description for the Chief Information Security Officer

At CIHI, the Chief Information Security Officer is responsible and accountable for leading CIHI's Information Security program. The Chief Information Security Officer reports directly to the Vice President and Chief Information Officer, who reports to CIHI's President and CEO.

The job description for the Chief Information Security Officer identifies the key responsibilities and obligations for the role and includes the minimum obligations set out in the *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities*, issued by the IPC/ON, namely:

- Developing, implementing, reviewing and amending security policies, procedures and practices;
- Ensuring compliance with the security policies, procedures and practices implemented;
- Ensuring agents are aware of CIHI's security policies, procedures and practices and are appropriately informed of their duties and obligations thereunder;
- 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 *Privacy and Security Incident Management Protocol*; and
- Conducting security audits pursuant to CIHI's audit program.

Termination of Relationship

10. Policy and Procedures for Termination or Cessation of the Employment or Contractual Relationship

The Procedures relating to the *Security and Access Policy* require agents, as well as their supervisors, to notify CIHI of the termination of their employment, contractual or other relationship with CIHI .CIHI has well established exit procedures that ensure Human Resources, Information Technology, Corporate Administration, Finance, Web Services and the business process management workflow tool team are notified of any agent terminating their relationship with CIHI and that all CIHI property, including access cards and keys, if applicable, and personal health information are securely returned. The importance of having a well-structured off-

boarding process is key to ensuring prompt and timely revocation of access privileges to CIHI's premises and networks. The Senior Human Resources Assistant is responsible for initiating the off-boarding workflow in the business process management workflow tool which generates a last day email to the above-mentioned teams to notify them that an agent is leaving CIHI, as well as creating an alert to Service Desk to inform the Information Technology team of the agent's last day in the office.

Once the Information Technology team receives the alert and creates a Service Request, the Senior Technical Support Specialist disables the departing agent's account, changes the expiration date on the user account, and sends the Employee Departure Information Technology Checklist to the departing agent's Manager. As per the Information Technology Checklist, the user account is disabled at the end of the termination day.

The off-boarding process sets out the Manager's roles and responsibilities to ensure the effective termination of their agent. An *Off-boarding Checklist* for Managers forms part of the business process management workflow tool and sets out the necessary steps that the Manager must complete before the agent's last day. Should CIHI property not be duly returned by the departing agent the Director of Human Resources and Administration[2] or the Manager, Human Resources will contact CIHI's General Counsel and/or lawful authorities.

In the case of involuntary terminations, the Manager, along with a representative from Human Resources, informs the agent of the termination, walks the person back to their work station to collect their personal items, collects the security access card and keys, CIHI-issued credit card, if applicable, and escorts the agent out of the building. The off-boarding process described above is initiated at the time of departure.

Compliance, Audit and Enforcement

CIHI's Code of Business Conduct describes the ethical and professional behaviour related to work relationships, information – including personal health information – and the workplace. The Code requires all employees to comply with the Code and all CIHI's policies, protocols and procedures. Compliance with CIHI's privacy program is monitored through CIHI's risk-based privacy audit program set out in a multi-year audit plan. Instances of non-compliance with privacy and security policies are managed through CIHI's *Privacy and Security Incident Management Protocol*. Violations of the Code are referred to Human Resources, as appropriate, and may result in disciplinary action up to and including dismissal.

Discipline

11. Policy and Procedures for Discipline and Corrective Action

Protecting the privacy of the individuals whose information CIHI holds and safeguarding all personal health information in CIHI's control is core to what CIHI does. As a result, all policies

[2] At times, this particular function may be assumed by the Manager of Human Resources.

relating to the privacy program and the security program require mandatory compliance and instances of non-compliance can be met with disciplinary actions up to and including termination.

Human Resources and Administration has the responsibility for managing all disciplinary and corrective actions involving agents. This Branch has a set of policies and procedures that ensure such employment-related issues within the organization are dealt with effectively. Together, the Respectful Workplace Policy, the related Procedure, the CIHI Employee Discipline Guidelines and the Code of Business Conduct address the following:

1. the person(s) responsible for conducting an investigation of disciplinary matters;

2. the procedure that must be followed in undertaking the investigation;

3. any documentation that must be completed, provided and/or executed in undertaking the investigation;

4. the agent(s) responsible for completing, providing and/or executing the documentation;

5. the required content of the documentation;

6. and the agent(s) to whom the results of the investigation must be reported.

7. the types of discipline that may be imposed and the factors that must be considered in determining the appropriate discipline and corrective action;

8. the agent(s) responsible for determining the appropriate discipline and corrective action;

9. the procedure to be followed in making this determination;

10. the agent(s) that must be consulted in making this determination; and

11. the documentation that must be completed, provided and/or executed, shall also be identified.

12. the retention of documentation related to the discipline and corrective action taken, including where this documentation will be retained and the agent(s) responsible for retaining the documentation.

Part 4 - Organizational and Other Documentation

Governance

1. Privacy Governance and Accountability Framework

CIHI's *Privacy and Security Framework, 2010*, describes its privacy and security governance and accountability model. It sets out that the President and CEO is ultimately accountable for CIHI and for CIHI's ultimate compliance with the Act and its regulation, as well as with all privacy and security policies, procedures and practices at CIHI.

CIHI's *Privacy and Security Framework, 2010*, sets out that the Chief Privacy Officer, who reports to the Vice President of Corporate Services, has been delegated day-to-day authority to manage the privacy program and describes the responsibilities and obligations of the Chief Privacy Officer. The Framework also sets out that the Chief Information Security Officer, who reports to the Vice President and Chief Information Officer, has been delegated day-to-day authority to manage the security program and describes the responsibilities and obligations of the Chief Information Security Officer. This includes responsibility for ensuring that the suite of privacy and security policies and procedures is comprehensive, up to date and communicated to staff, the public and other stakeholders. The Framework illustrates that both CIHI's Chief Privacy Officer and Chief Information Security Officer are supported in managing their respective program by various individuals, teams and committees.

CIHI's Board of Directors recognizes the importance of CIHI's privacy and security obligations and, therefore, established the Governance and Privacy Committee and a Finance and Audit Committee. These committees represent accountability at the highest possible level.

The Governance and Privacy Committee oversees the privacy program and reviews privacy breaches and audit reports, any substantive policy changes and any other issue deemed relevant by the President and CEO and/or the Chief Privacy Officer and Chief Information Security Officer. The Finance and Audit Committee reviews all security audits conducted by third parties as well as any internal security audits as deemed appropriate by the VP& CIO. Security breaches are also reported to the Finance and Audit Committee.

The Governance and Privacy Committee meets at least two times each year, generally just prior to the Board of Directors meetings. As well, an Annual Privacy Report is submitted to the Board of Directors. The Annual Privacy Report describes initiatives undertaken by the privacy program including privacy and security training, the development and implementation of new policies, and a discussion of privacy audits and privacy impact assessments conducted, the results of and recommendations arising from them, and the status of implementation of the recommendations. The Board of Directors is also advised of any privacy or security breaches.

Substantive security audits, for example, results of Threat Risk Assessments or vulnerability assessments, are submitted to the Finance and Audit Committee and ultimately to the Board of Directors.

Key supporting committees for privacy and information security include the following:

- Executive Committee
  - Chaired by the President and CEO and comprising the President and CEO, Vice-Presidents and Executive Directors and the Chief Privacy Officer/General Counsel
- Senior Management Committee
  - Chaired by the Vice-President, Corporate Services, and comprising Vice-Presidents and Executive Directors and all Directors including the Chief Privacy Officer and the Chief Information Security Officer
- IT Leadership Team
  - Chaired by the Vice President and Chief Information Officer
- Privacy, Confidentiality and Security Committee
  - Chaired by the Chief Privacy Officer
- Information Security Management System (ISMS) Steering Committee
  - Chaired by the Vice President and Chief Information Officer, comprising all ITS directors and key ISMS personnel
- ISMS Working Group
  - Chaired by the Manager, Information Security, comprising senior ITS staff in support of CIHI's Information Security Management System.

CIHI's *Privacy and Security Framework, 2010*, is available to all CIHI agents on its intranet site, as well as to its stakeholders and the general public on CIHI's external website (www.cihi.ca).

2. Security Governance and Accountability Framework

Refer to Part 4, Section 1, above.

3. Terms of Reference for Committees with Roles with Respect to the Privacy Program and/or Security Program

CIHI has written terms of reference for the committees that have a role in the privacy or security programs. These include:

- Identification of membership in the committee
- The chair of the committee
- The committee mandate and responsibilities in respect of privacy and/or security
- The frequency of meetings
- To whom the committee reports
- Types and frequency of reports produced by the committee, if any
- To whom such reports are presented.

Risk Management

4. Strategic Risk Management Framework

CIHI has developed and implemented a Strategic Risk Management Framework that is designed to identify, assess, mitigate and monitor risks, including risks with respect to the protection of personal health information under its control.

Corporate Services is responsible for this Framework which contains the following key elements:

- Risks are identified annually by members of the Executive Committee
- Risks are ranked based on the likelihood of occurrence and the potential impact to CIHI if the risk does materialize, taking into consideration existing mitigation strategies
- Additional strategies to mitigate the high level risks are identified by a member of Senior Management (Risk Champion); these are reviewed by the Finance and Audit Committee of the CIHI Board, and an update is provided to the full Board
- Timelines and a process to implement the mitigation strategies are developed
- Upon developing the action plans based on the mitigation strategies, policies, procedures and practices may be developed or revised as appropriate
- The implementation of the mitigation strategies is monitored and reported on quarterly at Senior Management Committee meetings
- Results of the identification and assessment of risk, strategies to mitigate risks, the status of the implementation of the mitigation strategy, including how and to whom are communicated in CIHI's Annual Report
- Documentation of and assignment of responsibilities for all of the above rests with Corporate Services

Pursuant to the Strategic Risk Management Framework, Corporate Services maintains a corporate risk register for CIHI to ensure that all risks to the organization, including risks with respect to the protection of personal health information under its control, continue to be identified, assessed and mitigated. . Key risks for any given year are assessed are on an annual basis to determine the strategic risks for the subsequent fiscal year but are monitored on an ongoing (sometimes daily) basis, and if there are emerging strategic risks, they are addressed immediately (COVID-19 being a relevant example). Strategic risks that are set-out during the annual framework review are reported on quarterly at a minimum. Responsibility for the coordination of the annual review by the Executive Team is with the Manager, Governance and Strategy, and the process is outlined in the Framework. Risk champions, who are members of CIHI's Senior Management Committee, undertake quarterly reviews and updates, which are discussed with the Senior Management team.

In 2015, CIHI formally approved its *Privacy and Security Risk Management (PSRM) Framework* designed to integrate and align with CIHI's Strategic Risk Management Framework. PSRM informs and aligns with corporate risk management activities through adopting a similar methodology, terminology and governance structure. At the same time, CIHI also introduced its

Policy on Privacy and Security Risk Management which sets out the requirements for CIHI to identify, assess, treat and monitor privacy and security risks, as well as associated roles and responsibilities. A related *Privacy and Security Risk Assessment Methodology* document describes the steps involved in assessing privacy and security risks: identifying, assessing, treating, and monitoring and reviewing risk.

5. Corporate Risk Register

CIHI's corporate risk register identifies each risk that may negatively affect CIHI's ability to deliver on its strategic goals. For each identified risk it includes:

- An assessment of the risk;
- A ranking of the risk;
- The mitigation strategy to reduce the likelihood of the risk occurring or the impact if it occurs;
- The date the mitigation strategy was implemented or will be implemented;
- Agent responsible for the implementation

Privacy and Security has been identified as one of CIHI's strategic risks for the organization – specifically the risk of a major privacy or security event impacting CIHI's business operations. CIHI's Privacy and Security Risk Management program informs the mitigation of this corporate risk.

6. Policy and Procedures for Maintaining a Consolidated Log of Recommendations

CIHI maintains two separate consolidated logs of recommendations: one for privacy recommendations and one for security recommendations. CIHI's Privacy and Legal Services maintains a consolidated log of privacy recommendations to improve its privacy program. The recommendations in the log are drawn from the following sources:

- Privacy impact assessments
- Internal privacy audits
- The investigation of privacy incidents and breaches
- Privacy and security risk management assessments
- The investigation of privacy complaints
- The IPC/ON's review every three years.

The log is updated after any of the foregoing events and is reviewed on an ongoing basis.

The recommendations are subsequently fed into CIHI's Master Log of Corporate Action Plans, are monitored and reported on at the corporate level. The owner of the individual action plan (i.e, recommendation) is responsible for documenting the recommendations and the actions taken (or planned) to address them. Furthermore, each owner of the action plan related to a recommendation is required to provide regular updates/presentations to the Senior Management Committee. Regular updates will continue to be provided to the Senior Management Committee

until such time as the recommendations are addressed. Review of the Corporate Action Plans is included in the Terms of Reference for the Senior Management Committee. A Corporate Action Plan Process Manual sets out the frequency and circumstances in which the Corporate Action Plans are to be reviewed, the department responsible for reviewing and amending the log, and the process that must be followed in this regard.

The Office of the Chief Information Security Officer maintains a consolidated log of security recommendations arising from internal and external security audits, the investigation of security incidents and general operational recommendations relating to information security. Each recommendation is assigned an owner who is responsible for providing a target completion date as well as monthly updates. Recommendations resulting from security audits conducted by an independent third party (e.g. vulnerability assessments and penetration testing) are included in the Master Log of Corporate Action Plans, are monitored and reported on at the corporate level.

7. Consolidated Log of Recommendations

A consolidated and centralized log of privacy recommendations arising from privacy impact assessments, internal privacy audits, the investigation of privacy and security incidents and breaches, privacy and security risk management assessments, the investigation of privacy complaints, and reviews by the IPC/ON, as well as recommendations resulting from security audits are incorporated into CIHI's Master Log of Action Plans which contains the following data elements for each recommendation:

- The name and date of the document, investigation, audit or review from which the recommendation arose;
- A description of the recommendation;
- The manner in which the recommendation was addressed or is proposed to be addressed;
- The date the recommendation was addressed or by which it is required to be addressed; and
- The agent responsible for addressing the recommendation.

Business Continuity and Disaster Recovery

8. Business Continuity and Disaster Recovery Plans

CIHI has a business continuity management (BCM) program and disaster recovery plan that is designed to protect CIHI from extended disruptions to business, protect corporate resources and agents, safeguard vital records of CIHI and its clients and assure the continued availability of CIHI's critical services. The business continuity plan (BCP) is a tactical manifestation of the BCM. It details the activities that CIHI should execute in the event of a disruption to business operations in order to restore at least the critical business processes and services identified in the Business Impact Assessment (BIA) within the mandate of the organization so that stakeholders can continue to rely upon the organization, even after a debilitating interruption. The disaster recovery plan (DRP) outlines the process to ensure that IT systems and

services/processes will be recovered in a timely manner to support the BCP. The BCP and the DRP outline the procedures for responding to a business interruption that involves CIHI and its critical services and includes the following key elements:

- Notification of the Interruption – roles and responsibilities, the contact list, timeframes, and form of notification as well as crisis communication strategy and plan
- Assessment of the Severity of the Interruption – roles and responsibilities including the criteria pursuant to which this assessment is to be made and the agents and other persons or organizations that must be consulted in assessing the severity level of the interruption or threat criteria for assessment and documentation, initial impact assessment, a detailed damage assessment including the documentation that must be completed, provided and/or executed resulting from or arising out of this assessment; the required content of the documentation; the agent(s) to whom the documentation must be provided; and to whom the results of this assessment must be reported
- In relation to the assessment of the interruption or threat, the BCP sets out the agent(s) responsible and the process that must be followed in conducting an initial impact assessment of the interruption or threat, including its impact on the technical and physical infrastructure and business processes. This includes the agents and other persons or organizations that are required to be consulted in undertaking the assessment; the requirements that must be satisfied and the criteria that must be utilized in conducting the assessment
- Resumption and Recovery – activation of the BCP and DRP; an inventory of all critical applications and business functions, as well as a full inventory of CIHI systems in the the Configuration Management Data Base including all hardware and software, software licences, recovery media, equipment, system network diagrams, hardware configurations, software configuration settings, configuration settings for database systems and network settings for firewalls, routers, domain name servers, email servers and the like; procedures for recovery of every critical application and business function; prioritization of recovery activities; recovery time objectives; and roles and responsibilities
- Governance During an Event – the procedure by which decisions are made by the Business Continuity Management Team
- Testing, Maintenance and Assessment of the Plan – frequency of testing, roles and responsibilities, plan amendments process, approval of the plan and amendments thereto.
- Communications -- the BCP identifies the agent(s) responsible and the procedure to be followed in communicating the BCP and the DRP to all agents, including any amendments thereto, and the method and nature of the communication. The agent(s) responsible for managing communications in relation to the threat or interruption are also identified, including the method and nature of the communication.

The BCP and DRP are tested every two years. Testing requirements have been met during the current review period, either in the form of a test, or by the application of the plans in real-world situations.

The Vice-President, Corporate Services has overall responsibility and accountability for the effectiveness and maintenance of CIHI's BCM Program and implementation of program elements throughout CIHI and serves as the designated alternate for the President and CEO.

PHIPA Review – Indicators

November 1, 2016 to October 31, 2019

Part 1 – Privacy Indicators

Categories	Privacy Indicators	CIHI Indicators
General Privacy Policies, Procedures and Practices	• The dates that the privacy policies and procedures were reviewed by the prescribed person or prescribed entity since the prior review of the IPC/ON.	▪ *Privacy Policy on the Collection, Use, Disclosure and Retention of Personal Health Information and De-Identified Data, 2010*, (*Privacy Policy, 2010*), reviewed June 2017, July 2018 ▪ Privacy Policy Procedures reviewed May 2017, June 2017, June 2018 and July 2019 ▪ *Privacy and Security Framework, 2010* - reviewed May 2019 ▪ *Privacy and Security Training Policy* reviewed November 2016, November 2017, February 2019 ▪ Procedures related to *Privacy and Security Training Policy* reviewed January 2017, November 2017, July 2018 ▪ *Privacy Impact Assessment Policy* reviewed August 2017, October 2018 ▪ *Privacy and Security Incident Management Protocol* reviewed February 2017, March 2018, November 2018 ▪ *Policy on the Security of Confidential Information and Use of Mobile Devices / Removable Media* reviewed July 2017, September 2018 and June 2019 ▪ *Privacy and Security Risk Management (PSRM) Framework* reviewed February 2017, April 2018, March 2019 ▪ *Policy on Privacy and Security Risk Management* reviewed February 2017, March 2018, March 2019 ▪ *Privacy and Security Risk Assessment Methodology* reviewed February 2017, April 2018, March 2019

Categories	Privacy Indicators	CIHI Indicators
	• 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.	▪ *Privacy Policy, 2010* – June 2017 change to definitions – removed reference to Client Linkage Index, as it is no longer used; July 2018 – no changes ▪ Privacy Policy Procedures amended May 2017 to reflect BC DSA requirements; to revise document storage and retention requirements for documentation relating to requests from individuals for access to own PHI; and to include consultation with the CPO/GC in cases of uncertainty around mandate and disclosures. June 2017 – update references and links to client linkage standard; update to reflect Manitoba DSA requirement to obtain Ministry approval prior to disclosing de-identified record-level data outside of Canada. June 2018 – Privacy Policy Procedures amended to update internal link. ▪ Interim Privacy Policy Procedures published July 2019 on Access to Privacy Sensitive Data Elements ▪ *Privacy and Security Framework, 2010* – May 2019 - general updates to align terminology ▪ *Privacy and Security Training Policy* – no changes ▪ Procedures for the *Privacy and Security Training Policy* amended January 2017 to address changes to delivery of training instructions. Now supplied within business tool notification email and on-boarding orientation documentation produced by Human Resources. November 2017 – minor administrative changes. July 2018 – minor administrative changes. ▪ *Privacy Impact Assessment Policy* – August 2017 – no changes; updated October 2018 – minor editorial changes to align language. ▪ *Privacy and Security Incident Management Protocol* amended February 2017 to add “personal Information” to the definition of privacy breach and to include definition of personal information; specify time-frame for completion of reports; include language to distinguish between events and

Categories	Privacy Indicators	CIHI Indicators
		incidents (ISO audit requirement). March 2018 – no changes. Amended December 2018 to add the role of Communications and Crisis Communication Plan. ▪ *Policy on the Security of Confidential Information and Use of Mobile Devices / Removable Media* amended July 2017 to remove Procedures; replaced by PSRM assessment. Amended September 2018 – minor editorial changes/clarifications and added references. Amended June 2019 to update definition of Technical Information. ▪ *Privacy and Security Risk Management (PSRM) Framework* - no changes ▪ *Policy on Privacy and Security Risk Management* - February 2017 – administrative update; March 2018 - no changes; March 2019 – change to responsibilities of the PC&S Committee as reflected in the June 2018 Terms of Reference of the Committee ▪ *Privacy and Security Risk Assessment Methodology* – no changes
	• 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.	None
	• The date that each amended and newly developed privacy policy and procedure was communicated to agents and, for each amended and newly developed privacy policy and procedure communicated to agents, the nature of the communication.	CIHI communicates material changes to all privacy policies, standards and procedures to those staff that are impacted by the change. Communication mechanisms include CIHI's intranet (CIHighway), SmallTalks, targeted presentations and the like. To date, the following communications have been delivered: ▪ *Privacy Policy and Procedures*– May 2017 - Updated version of the Procedures posted on CIHighway; June 2017 – updated version of the Policy and Procedures posted on CIHighway; June 2018 – Updated version of the Procedures posted on CIHighway; July 2019 – Interim Privacy Policy Procedures on Access to Privacy

Categories	Privacy Indicators	CIHI Indicators
		Sensitive Data Elements published on CIHighway, with an email communication to all agents ▪ *Privacy and Security Framework, 2010* – May 2019 – updated version of the framework posted on CIHighway; ▪ Updated procedures related to *Privacy and Security Training Policy* posted on CIHighwayJanuary 2017, July 2018 ▪ *Privacy Impact Assessment Policy*: Revised Policy posted on CIHighwayNovember 2018; ▪ *Policy on the Security of Confidential Information and Use of Mobile Devices / Removable Media and related Procedures* – Revised Policy posted on CIHighway November 2017, September 2018 and June 2019 ▪ *Privacy and Security Incident Management Protocol* – Revised Protocol posted on CIHighway April 2017 and January 2019 ▪ *Policy on Privacy and Security Risk Management* – Revised Policy posted on CIHighway May 2017, May 2018 and June 2019
	▪ 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.	▪ CIHI's *Privacy Policy, 2010* and the *Privacy and Security Framework, 2010* posted on CIHI's external website (www.cihi.ca) ▪ CIHI's *Privacy and Security Incident Management Protocol*, *Privacy Impact Assessment Policy*, *Privacy and Security Training Policy*, *Policy on the Security of Confidential Information and Use of Mobile Devices / Removable Media*, *Privacy and Security Risk Management (PSRM) Framework* and *Policy on Privacy and Security Risk Management* posted on CIHI's external website ▪ An updated Information Sheet on CIHI's Privacy Audit Program for Third-Party Record-level Data Recipients posted on CIHI's external website to include a new learning from one of CIHI's compliance audits, specifically, to ensure

Categories	Privacy Indicators	CIHI Indicators
		processes are implemented to ensure contract obligations are not affected in situations where there are role changes within the project team or team members are transitioning on or off the project.

Categories	Privacy Indicators	CIHI Indicators
Collection	▪ The number of data holdings containing personal health information maintained by the prescribed person or prescribed entity.	▪ CIHI has 18 data holdings containing personal health information and 2 containing de-identified data
	▪ The number of statements of purpose developed for data holdings containing personal health information.	▪ Statements of purpose for all 20 data holdings are found in the relevant Privacy Impact Assessment
	▪ The number and a list of the statements of purpose for data holdings containing personal health information that were reviewed since the prior review by the IPC/ON.	▪ See Appendix B - Privacy Impact Assessment Log where the data holdings whose statements of purpose were reviewed since November 1, 2016 are marked with an asterisk. Statements of purpose are also reviewed on an annual basis for all 18 data holdings containing personal health information as part of the annual revision to the *Products and Services Guide*.
	▪ Whether amendments were made to existing statements of purpose for data holdings containing personal health information 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.	▪ None.
Use	• The number of agents granted approval to access and use personal health information for purposes other than research.	▪ As of October 31, 2019, 171 agents have approval to access and use personal health information at CIHI.
	• The number of requests received for the use of personal health information for research since the prior review by the Information and Privacy Commissioner of Ontario.	▪ None. CIHI does not use personal health information for research purposes.
	• The number of requests for the use of personal health information for research purposes that were granted and that were denied since the prior review by the IPC/ON.	▪ None. CIHI does not use personal health information for research purposes.
Disclosure	• The number of requests received for the disclosure of personal health information for purposes other than research since the prior review by the IPC/ON.	▪ Three requests for amendments to existing data sharing agreements.

Categories	Privacy Indicators	CIHI Indicators
	• The number of requests for the disclosure of personal health information for purposes other than research that were granted and that were denied since the prior review by the IPC/ON.	▪ Three granted (see above)
	• The number of requests received for the disclosure of personal health information for research purposes since the prior review by the IPC/ON.	▪ Ten – two consent-based and eight based on section 44 of PHIPA ▪ Five requests were abandoned - four section 44 requests and 1 consent-based ▪ One section 44 request is in process
	• The number of requests for the disclosure of personal health information for research purposes that were granted and that were denied since the prior review by the IPC/ON.	▪ Three granted (section 44) ▪ One consent-based denied
	• The number of Research Agreements executed with researchers to whom personal health information was disclosed since the prior review by the IPC/ON.	▪ Three (section 44)
	• The number of requests received for the disclosure of de-identified and/or aggregate information for both research and other purposes since the prior review by the IPC/ON.	▪ 2016-17: (Q3 – Q4) 424 ▪ 2017-18: (Q1 – Q4) 470 ▪ 2018-19: (Q1 – Q4) 414 ▪ 2019-20: (Q1 – Q2) 138
	• 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/ON.	▪ 2016-17: (Q3 – Q4) 424 ▪ 2017-18: (Q1 – Q4) 470 ▪ 2018-19: (Q1 – Q4) 414 ▪ 2019-20: (Q1 – Q2) 138
Data Sharing Agreements	• The number of Data Sharing Agreements executed for the collection of personal health information by the prescribed person or prescribed entity since the prior review by the IPC/ON.	▪ Three

Categories	Privacy Indicators	CIHI Indicators
	• The number of Data Sharing Agreements executed for the disclosure of personal health information by the prescribed person or prescribed entity since the prior review by the IPC/ON.	▪ Three amendments to existing DSAs ▪ Two amendments to the ICES DSA ▪ One amendment to the BORN DSA
Agreements with Third Party Service Providers	▪ The number of agreements executed with third party service providers with access to personal health information since the prior review by the IPC/ON.	▪ 76[1]
Data Linkage	▪ The number and a list of data linkages approved since the prior review by the IPC/ON.	▪ 114 linkages (3 of PHI, 111 of de-identified data) ▪ See *Appendix A - Approved Data Linkages*
Privacy Impact Assessments	▪ The number and a list of privacy impact assessments completed since the prior review by the IPC/ON and for each privacy impact assessment: – 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.	▪ Since November 1, 2016, 11 Privacy Impact Assessments have been completed (see Appendix B - Privacy Impact Assessment Log), 10 for personal health information and 1 for de-identified data ▪ No recommendations were identified (see *Appendix C – CIHI's Privacy Impact Assessment Program - Summary of Recommendations - CIHI's Privacy Impact Assessment Program – Summary of Recommendations*) ▪ Note: The *Summary* table includes PIAs in progress in addition to the 11 PIAs that were completed.
	▪ The number and a list of privacy impact assessments undertaken but not completed since the prior review by the IPC/ON and the proposed date of completion.	▪ 4 Privacy Impact Assessments have been undertaken but not completed (See Appendix B - Privacy Impact Assessment Log
	▪ The number and a list of privacy impact assessments that were not undertaken but for which privacy impact assessments will be completed and the proposed date of completion.	▪ None

[1] Third-party service providers who need access to CIHI systems and data in order to provide the contracted service are required to sign an agreement that is compliant with PHIPA.

Categories	Privacy Indicators	CIHI Indicators
	▪ The number of determinations made since the prior review by the IPC/ON that a privacy impact assessment 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 privacy impact assessments reviewed since the prior review by the IPC/ON and a brief description of any amendments made.	Since November 1, 2016, 11 privacy impact assessments have been reviewed, 10 for personal health information and 1 for de-identified data See Appendix B - Privacy Impact Assessment Log

Categories	Privacy Indicators	CIHI Indicators
Privacy Audit Program	• The dates of audits of agents granted approval to access and use personal health information since the prior review by the IPC/ON and for each audit conducted: – A brief description of each recommendation made, – The date each recommendation was addressed or is proposed to be addressed, and – The manner in which each recommendation was addressed or is proposed to be addressed.	▪ See Part 2, Security Audit Program – Yearly Internal Access Audit.This is an entry on the "CIHI's Security Audit Program" table. ▪ Annual audit of agents by Client Engagement and Support to validate that access to CIHI's secure applications and tools containing personal health information is still required - See *Appendix D - CIHI's Privacy Audit Program* - privacy audit of CIHI's Identity and Access Management System
	• The number and a list of all other privacy audits completed since the prior review by the IPC/ON and for each audit: – A description of the nature and type of audit conducted, – The date of completion of the audit, – A brief description of each recommendation made, – The date each recommendation was addressed or is proposed to be addressed, and – The manner in which each recommendation was addressed or is proposed to be addressed.	▪ Since November 1, 2016, three audits carried out in previous reporting periods were completed (i.e., recommendations addressed). In addition, CIHI has completed two privacy audits carried out in the current reporting period with two audits in progress ▪ See *Appendix D - CIHI's Privacy Audit Program* ▪ See *Appendix E – External Audit of CIHI's Privacy and Security Program*
Privacy Breaches	▪ The number of notifications of privacy breaches or suspected privacy breaches received by the prescribed person or prescribed entity since the prior review by the IPC/ON.	▪ Ontario - None All other jurisdictions –none
	▪ With respect to each privacy breach or suspected privacy breach: – 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 personal health information at issue, – The date that senior management was notified, – The containment measures implemented,	▪ N/A

Categories	Privacy Indicators	CIHI Indicators
	– 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.	
Privacy Complaints	▪ The number of privacy complaints received since the prior review by the IPC/ON.	▪ Ontario – None ▪ All other jurisdictions – None
	▪ Of the privacy complaints received, the number of privacy complaints investigated since the prior review by the IPC/ON and with respect to each privacy complaint investigated: – 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 complaint describing the nature and findings of the investigation and the measures taken in response to the complaint.	▪ N/A
	▪ Of the privacy complaints received, the number of privacy complaints not investigated since the prior review by the IPC/ON and with respect to each privacy complaint not investigated: – The date that the privacy complaint was received,	▪ N/A

Categories	Privacy Indicators	CIHI Indicators
	– 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.	

Categories	Security Indicators	CIHI Response
General Security Policies, Procedures and Practices	▪ The dates that the security policies and procedures were reviewed by the prescribed person or prescribed entity since the prior review of the IPC/ON.	▪ *Information Security Policy*, reviewed December 2017, July 2018 and August 2019. ▪ *Acceptable Use of Information Systems Policy*, reviewed February 2017, October 2018 and August 2019. ▪ *Secure Destruction Policy,* reviewed March 2017, April 2018 and April 2019. ▪ *Security and Access Policy*, reviewed October 2017 and July 2019. ▪ *Privacy and Security Incident Management Protocol*, see General Privacy Policies, Procedures and Practices above ▪ *Secure Destruction Standard,* reviewed April 2017, June 2018 and June 2019. ▪ *Third Party Technical Information Disclosure Standard*, reviewed January 2017, December 2017 and January 2019 ▪ *COTS Product Technical Requirements Standard,* reviewed May 2017, May 2018 and May 2019. ▪ *Manual Changes to Production Data Standard*, Replaced in December 2014 with Manual Changes to Operational Data Standard - retired in April 2019. ▪ *Health Data Collection Standard,* reviewed December 2016, October and December 2017 and January 2019. ▪ *Secure Information Storage Standard,* reviewed February 2017, April 2018, April 2019, August 2019and September 2019. ▪ *Secure Information Transfer Standard,* reviewed January 2017, December 2017, February 2019 and September 2019. ▪ *Safe Internet Practices and Email Etiquette Guidelines,* reviewed December 2016, September 2017, and January 2019 ▪ *FAQ – Acceptable Use Policy*, reviewed August 2018 and September 2019.

Categories	Security Indicators	CIHI Response
		▪ *Database Access Standard*, retired September 2014 and reinstated February 2016. Reviewed January 2017 and February 2019 ▪ *File Encryption Procedures*, reviewed May 2017, June 2018 and June 2019. ▪ *Cloud Service Privacy and Security Assessment Guideline,* reviewed September 2017, August 2018 and October 2019. ▪ *Policy on the Maintenance of System Control and Audit Logs*, reviewed August 2017 and January 2019. ▪ *Use of Cloud Services Policy*, reviewed March 2017, September 2017, August 2018 and October 2019. ▪ *Respect of Third Party Software Licence Agreements,* reviewed March 2017, July 2018 and September 2019. ▪ *ISMS Audit Program,* reviewed May 2017, June 2018 and June 2019 ▪ *ISMS Risk Management Manual*, reviewed June 2017, June 2018 and June 2019 ▪ *ISMS Supplier Management*, reviewed June 2017, June 2018 and July 2019 ▪ *ISMS Infrastructure Security Standard,* reviewed June 2017, June 2018, and January 2019 ▪ *ISMS Manual*, reviewed June 2017, June 2018 and July 2019. ▪ *User Password Guidelines*, created January 2017, reviewed March 2018 and June 2019.
	▪ 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.	*Information Security Policy,* minor editorial updates, changed the term from staff to employees, added CPO/GC position, added Manager of Information Security position which replaced Senior Program Consultant of Information Security. *Acceptable Use of Information Systems Policy*, updated information about mobile devices, added bullet regarding responsibility of agents to remove personal records from CIHI information systems prior to their departure from CIHI, and simplified monitoring definitions.

Categories	Security Indicators	CIHI Response
		Secure Destruction Policy, no amendments were documented. *Security and Access Policy*, October 2017 - revised to include requirement to wear CIHI-issued access card on a lanyard; July 2019– consolidated two contractor access cards into one; added to the policy a quarterly audit of access to restricted areas that was occurring but had not been identified in the policy; replaced reference to the acess log with reference to the audit records. *FAQ Acceptable Policy*, no revision history documented since it is a supporting document and not a formal document. *Database Access Standard*, updated ITOC to IT Leadership Committee. *File Encryption Procedures*, moved to new format, added Scope, Compliance, and Office 2016, added instructions for WinZip 20.0, removed WinZip 11 and Office 2010/2013. *Cloud Service Policy and Security Assessment Guidelines*, revised definitions for the following terms: Personnel, Health Workforce Personal Information and Personal Health Information. The term Personnel was updated to "Employee" and ITOC revised to IT Leadership Committee, refined to align with new automated process, Cloud strategy will be finalized before end of fiscal as part of our cloud migration plan. We will continue to use this document and will revisit once a strategy has been finalized. *Policy on the Maintenance of System Control and Audit Logs,* no major updated and only minor edtis. *Use of Cloud Services Policy,* the following terms/definitions were revised to ensure consistency: aggregate data, de-identified data, health workforce personal information and personal health information, refined to align with new automated process, Cloud

Categories	Security Indicators	CIHI Response
		strategy will be finalized before end of fiscal as part of our cloud migration plan. We will continue to use this document and will revisit once a strategy has been finalized. *Policy on the Security of Confidential Information and Use of Mobile Devices/Removable Media*, procedures replaced by process for approval to include PSRM assessment, added references, and updated technical information requirements. *Respect of Third Party Software Licence Agreements*, revised definitions for the following terms: Information Assets, Software Products and Staff. "Staff" was updated to "Employee". *Secure Destruction Standard*, updated chart and changes about wiping encrypted solid state drives. *Third-Party Technical Information Disclosure Standard*, updated Information Technology Operational Committee to IT Leadership Committee and added results of technology audits to scope. *Secure Information Transfer Standard*, minor content edits and updated the technical information definition. Also, updated approval authority to CISO, added Personal Information definition, removed Information Classifications, removed rare and exceptional circumstances paragraph. *COTS Product Technical Requirements Standard,* minor editorial changes. *Health Data Collection Standard*, amended to reflect revised Branch name, revised the term "personnel" to "staff" and added (including external consultants or other third-party service providers) to the definition. Clarified reference "no longer collecting PHI in paper format as of April 1, 2012" will read CIHI does not collect PHI in paper format. Updated contact information for Data

Categories	Security Indicators	CIHI Response
		Acquisition method *Secure Information Storage Standard*, amended to include a definitions section and included Health Workforce Personal Information and technical information words. Clarified Personal Health Information on paper not to be stored offsite. Updated approval authority to CISO, updated confidential information definition, removed information classifications, removed restricted information, added personal information definition, added removable media definition, added Storage of Personal Information and other Confidential Information on CIHI's Networks heading, and other minor edits. *Safe Email and Browsing Guideline*, Email Etiquette guidelines removed and title updated to reflect the change and revision regarding logging into sites over Wi-Fi. *User Password Guidelines,* minor content revisions. *ISMS Audit Program,* Added internal audit methodology and revised InfoSec Audit Section 2.4. *ISMS Risk Management Manual* no updates noted. *ISMS Infrastructure Security Standard,* Minor updates to mobile pass and SSL, RC4 deprecation, removed reference to "operator" in section 3.5.1. *ISMS Manual*, minor updates and clarifications in procedures, updated Appendix B. *ISMS Supplier Management*, Minor changes made to section 2.3.1 Contract Types.
	▪ 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.	None

Categories	Security Indicators	CIHI Response
	▪ 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.	CIHI communicates material changes to all security policies, standards and procedures directly to those staff that are impacted by the change. Communication mechanisms include CIHI's intranet (CIHighway). To date, the following communications have been delivered: ▪ *Information Security Policy* – Revised Policy posted on CIHIghway January 2018, August 2019, and August 2019 ▪ *Acceptable Use of Information Systems Policy* – Revised Policy posted on CIHighway February 2017, October 2018 and September 2019. ▪ *Database Access Standard* – Revised Standard posted on CIHIghway January 2017 and February 2019. ▪ *File Encryption Procedures* – Revised Procedures posted on CIHighway May 2017, July 2018 and June 2019. ▪ *Cloud Service Privacy and Security Assessment Guideline* – Revised Guideline posted on CIHighway April 2017, October 2017 and September 2018. ▪ *Policy on the Maintenance of System Control and Audit Logs* – Revised Policy posted on CIHighway August 2017 and January 2019. ▪ *Use of Cloud Services Policy,* Revised Policy posted on CIHighway April 2017, October 2017 and September 2018. ▪ *Policy on the Security of Confidential Information and Use of Mobile Devices/Removable Media* – Revised Policy on CIHighway July 2017, September 2018 and June 2019. ▪ *Respect of Third Party Software License Agreements,* Revised Policy posted on CIHighway April 2017, July 2018 and September 2019. ▪ *COTS Product Technical Requirements Standard* – Revised Standard posted on CIHighway May 2017, May 2018 and June 2019. ▪ *Health Data Collection Standard* – Revised Standard

Categories	Security Indicators	CIHI Response
		posted on CIHighway December 2016, October and December 2017, and January 2019. ▪ *Safe Internet Practices and Email Etiquette Guidelines* – Revised Guidelines posted on CIHighway December 2016, September 2017 and January 2019 ▪ *FAQ – Acceptable Use Policy* – Revised supporting document posted on CIHighway August 2018 and September 2019. ▪ *Secure Destruction Policy* – Revised Policy posted on CIHighway March 2017, April 2018 and April 2019. ▪ *Secure Destruction Standard* – Revised Standard posted on CIHighway April 2017, June 2018, June 2019. ▪ *Secure Information Storage Standard* – Revised Standard posted on CIHighway February 2017, April 2018 and May 2019 and August 2019 ▪ *Secure Information Transfer Standard* – Revised Standard posted on CIHighway January 2017, December 2017, February 2019 and September 2019 ▪ *Security and Access Policy* – Revised Policy posted on CIHighway October 2017 and October 2019. ▪ *Third-Party Technical Information Disclosure Standard* – Revised Standard posted on CIHighway January 2017, December 2017 and January 2019. ▪ *User Password Guidelines, posted on CIHighway February 2017, April 2018 and June 2019.* Note: ISMS documents are approved and communicated through the ISMS Steering Committee and the ISMS Working Group
	▪ 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.	*Information Security Policy*, minor editorial updates, changed the term from staff to employees, added CPO/GC position, added Manager of Information Security position which replaced Senior Program Consultant of Information Security. *Policy on the Security of Confidential Information and Use of Mobile Devices/Removable Media*, procedures replaced by process for approval to include PSRM

Categories	Security Indicators	CIHI Response
		assessment, added references, and updated technical information requirements. *Health Data Collection Standard*, amended to reflect revised Branch name, revised the term "personnel" to "staff" and added (including external consultants or other third-party service providers) to the definition. Clarified reference "no longer collecting PHI in paper format as of April 1, 2012" will read CIHI does not collect PHI in paper format. Updated contact information for Data Acquisition method.
Physical Security	• The dates of audits of agents granted approval to access the premises and locations within the premises where records of personal health information are retained since the prior review by the IPC/ON and for each audit: – A brief description of each recommendation made, – The date each recommendation was addressed or is proposed to be addressed, and – The manner in which each recommendation was addressed or is proposed to be addressed.	• Weekly audit of access cards issued by CIHI reception • A quarterly audit of cards with access to restricted areas (Finance, HR, IT), confirmed with the respective managers conducted January, April, July and October of each year • Annual physical audit of access cards April 2017, April 2018 and April 2019 No recommendations
Security Audit Program	• The dates of the review of system control and audit logs since the prior review by the IPC/ON and a general description of the findings, if any, arising from the review of system control and audit logs.	• Review of system control and audit logs occurs as part of CIHI's security audit activities – See attached *CIHI's Security Audit Program*
	• The number and a list of security audits completed since the prior review by the IPC/ON and for each audit: – A description of the nature and type of audit conducted, – The date of completion of the audit, – A brief description of each recommendation made, – The date that each recommendation was addressed or is proposed to be addressed, and – The manner in which each recommendation was addressed or is expected to be addressed.	▪ See attached *CIHI's Security Audit Program*. ▪ CIHI has completed the following 61 audits: ○ External Third Party Vulnerability Assessment and Penetration Test (3) ○ External Third Party Vulnerability Assessment and Penetration Test of 1 Business Application (1) ○ Database Security Audit (36) ○ Yearly Internal Data Access Audit (3) ○ Local Administrator Audit (12)

Categories	Security Indicators	CIHI Response
		○ ISO/IEC 27001:2013 Surveillance / Recertification Audit (3) ○ ISMS Internal Audit (3)
Information Security Breaches	▪ The number of notifications of information security breaches or suspected information security breaches received by the prescribed person or prescribed entity since the prior review by the IPC/ON.	▪ Since November 1, 2016, CIHI has logged 1,012 reported information security incidents, one of which was classed as a security breach. Notes: (1) Not all incidents necessarily impact data under CIHI's control, and may or may not involve Ontario data. (2) Information security incidents include such circumstances as computer viruses, discovered weaknesses in infrastructure, etc.
	▪ With respect to each information security breach or suspected information security breach: – The date that the notification was received, – The extent of the information security breach or suspected information security breach, – The nature and extent of personal health information 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 ▪ The manner in which each recommendation was addressed or is proposed to be addressed.	▪ One security breach – no unauthorized access to personal health information (Report available on request)

Part 3 – Human Resources Indicators

Categories	Human Resources Indicators	CIHI Response
Privacy and Security Training and Awareness	▪ The number of agents who have received and who have not received initial privacy orientation since the prior review by the IPC/ON.	▪ 381 agents have received initial privacy and security orientation training in the review period (November 1, 2016 to October 31, 2019) ▪ 0 agents who began (or re-boarded) an employment, contractual, or other relationship with CIHI between November 1, 2016 – October 31, 2019 but did not receive initial privacy and security orientation on or before October 31, 2019 ▪ Agents returning from an extended leave period of greater than 180 days are required to re-do the privacy orientation training ▪ From November 1, 2016 to October 31, 2019, 77 agents were re-boarded and completed the required mandatory training
	▪ 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.	▪ Ongoing process – as per the requirements under CIHI's *Privacy and Security Training Policy*, all new-hires have completed mandatory privacy and security training on their first day of employment or as soon as possible thereafter, but within 15 days of commencement of employment.
	▪ The number of agents who have attended and who have not attended ongoing privacy training each year since the prior review by IPC/ON.	▪ 100% completed – mandatory training requirements ▪ January 2017 – 711 agents ▪ January 2018 – 727 agents ▪ January 2019 – 773 agents
	▪ The dates and number of communications to agents by the prescribed person or prescribed entity in relation to privacy since the prior review by the IPC/ON and a brief description of each communication.	▪ Ongoing Privacy and Security poster campaign "January is Privacy Awareness Month at CIHI" ▪ Ongoing Privacy and Security poster campaign "September is Information Security Awareness Month at CIHI" ▪ On-line mandatory training modules for all new-hires as well as external professional services (EPS) who will have access to CIHI systems and/or data as in order to provide the contracted services.

Categories	Human Resources Indicators	CIHI Response
		▪ On-line mandatory training modules for all CIHI agents: (1) January 2017 – Privacy Awareness Month Mandatory Training and Confidentiality Agreement Renewal for all agents (2) January 2018 – Privacy Awareness Month Mandatory Training and Confidentiality Agreement Renewal for all agents (3) January 2019 – Privacy Awareness Month Mandatory Training and Confidentiality Agreement Renewal for all agents ▪ January 2017: Presentation to Client Affairs Managers regarding relevant privacy legislation in Canada, including PHIPA. ▪ December 2018: Presentation to program area on non-standard data collections in the context of ongoing work for PROMs ▪ February 2019: Presentation to BSA Forum on Privacy and Security by Design ▪ March 2019: Presentation to Client Support Applications about Privacy and Security By Design
Security Training and Awareness	▪ The number of agents who have received and who have not received initial security orientation since the prior review by the IPC/ON.	▪ See Privacy and Security Training and Awareness, above.
	▪ The date of commencement of the employment, contractual or other relationship for agents that have yet to receive initial security orientation and the scheduled date of the initial security orientation.	▪ See Privacy and Security Training and Awareness, above.
	▪ The number of agents who have attended and who have not attended ongoing security training each year since the prior review by the IPC/ON.	▪ See Privacy and Security Training and Awareness, above.

Categories	Human Resources Indicators	CIHI Response
	▪ The dates and number of communications to agents by the prescribed person or prescribed entity to agents in relation to information security since the prior review by the IPC/ON.	▪ Every January and September, CIHI staff receives communication and training as part of Privacy Awareness Month (January) and Information Security Awareness Month (September). ▪ Additionally, regular communication and awareness is offered as required throughout the year. See attached *InfoSec Staff Awareness, Education and Communication Log*.
Confidentiality Agreements	▪ The number of agents who have executed and who have not executed Confidentiality Agreements each year since the prior review by IPC/ON.	▪ 457 agents have executed Confidentiality Agreements in the current reporting period – 381 agents and 76 third-party service providers ▪ No agents failed to execute a Confidentiality Agreement in the current reporting period
	▪ The date of commencement of the 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.	▪ None
Termination or Cessation	▪ The number of notifications received from agents since the prior review by the IPC/ON related to termination of their employment, contractual or other relationship with the prescribed person or prescribed entity.	▪ 333

Categories	Organizational Indicators	CIHI Response
Risk Management	▪ The dates that the corporate risk register was reviewed by the prescribed person or prescribed entity since the prior review by the IPC/ON.	▪ The Corporate Risk Register is developed on an annual basis. Action plans for the strategic risks are reviewed and monitored on a quarterly basis. ▪ Dates reviewed during the current reporting period are as follows: January 2017 February 2018 February 2019
	▪ 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.	Privacy and security remained on the corporate risk register, specifically a major risk of privacy or security breach. Changes to risks year over year are as follows: 2016-17 & 2017-18 • Funding and operational management • Complexity and magnitude of change • Listening to and adapting to stakeholders' needs • Privacy and security 2018-19 • Technology deficit • Maintaining focus to achieve the 2016-2021 strategic plan • Listening to and adapting to stakeholders' needs • Privacy and security • PCHO review 2019-20 • Addressing emerging technology needs • Maintaining focus to achieve the 2016-2021 strategic plan • Developing and maintaining effective stakeholder relationships • Addressing the risk of a major privacy and security breach • Addressing recommendations from the PCHO Review

Business Continuity and Disaster Recovery	▪ The dates that the business continuity and disaster recovery plan was tested since the prior review by the IPC/ON. ▪ 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.	▪ The Business Continuity Plan (BCP) was most recently tested February 2018 and is scheduled for another test in spring 2020. ▪ Note: Due to COVID-19, the BCP was invoked in March 2020 and continues to successfully support business functions. ▪ The Disaster Recovery Plan (DRP) was last tested in June 2017. Due to significant systems architecture changes underway, CIHI has postponed the 2019 test as the plan is in transition. ▪ Note: The DRP was invoked in September 2018 as a result of a local tornado in Ottawa and was successful in restoring access to required systems.The BCP is revised on a monthly (Call Lists) and annual basis (Plan) as well as when required, for example, due to organizational changes. ▪ Last comprehensive review of the BCP was conducted in 2018 and resulted in updates to roles and responsibilities, namely the role of VP Corporate Services and Event Commander. These changes were carried through in updates to the communication activities and event management. ▪ Recommendations resulting from the February 2018 test have been addressed. ▪ Clarification regarding communication during a disruptive event was added, specifically regarding ownership of communicating with internal vs. external stakeholders. ▪ Crisis communication plan has been developed. ▪ Emergency mass notification system acquisition (to replace the manual call lists) is underway. ▪ Event management framework was updated including incident tracking protocol. ▪ DRP updated continuously as changes to technology occur, to ensure that the plan includes most recent procedures. ▪ All DRP changes are documented in DR Framework in which regular maintenance of the plan as well as participant information is captured throughout the year.

Appendix A - Approved Data Linkages

November 1, 2016 – March 31, 2017 (FY 2016/17) – Third-Party Requests for Data Linkage

No.	DL #	Date Approved	Files Linked	Subject/ Project or Study Title	Date of Destruction
1	227	Nov 3, 2016	BC Home and Community Care (HCC) Minimum Reporting Requirements (MRR), CCRS, NPDUIS, DAD, HCRS, NACRS	*Data linkage to support analysis of home and community care services in BC*	Nov 2019
2	219	Nov 16, 2016	CORR, CORR Wave	*The Access to Kidney Transplantation Feasibility Project (CORR Wave)*	Nov 2019
3	233	Nov 14, 2016	CCRS, NPDUIS, DAD, HCRS, NACRS	*Epidemiology and Economic Burden of Refractory and Super Refractory Status Epilepticus in Canada*	Dec 2019
4	313	Feb 15, 2017	DAD, NACRS, CCRS, HCRS, NRS	*Stroke Report 2017, Quality of Stroke Care in Canada*	Mar 2022
5	314	Feb 15, 2017	DAD, NACRS, CCRS, HCRS, NRS	*Monitoring Cardiac Care in Canada - Annual Heart Report and Survivor Support*	Mar 2022
6	315	Feb 21, 2017	NPDUIS, DAD, HCRS, NACRS	*Epidemiology and Economic Burden of Primary and Secondary Immunodeficiency in Canada*	Feb 2020
7	337	Mar 23, 2017	DAD	*Access to Allogeneic Stem Cell Transplant in Canada: Does Location Matter?*	Mar 2022

November 1, 2016 – March 31, 2017 (FY2016/17) – Linkages for a CIHI Use/Purpose

No.	DL #	Date Approved	Files Linked	Subject/Project or Study Title	*Date of Destruction*
8	305	Feb 8, 2017	DAD, NPDUIS, PLPB	*NPDUIS-DAD-PLPB Opioid Study*	Feb 2020
9	306	Feb 8, 2017	DAD, NPDUIS	*Drug Use Among Seniors on Public Drug Programs in Canada (report)*	Feb 2020
10	304	Feb 3, 2017	HMDB, NACRS, CCRS, HCRS, PLPB, NPDUIS, OMHRS, NRS	*Dementia Project*	July 2018

FY2017/18 – Third-Party Requests for Data Linkage

No.	DL #	Date Approved	Files Linked	Subject/Project or Study Title	Date of Destruction
11	5	Apr 27, 2017	PLPB, POP Grouper	*Proof of concept demonstration to better understand the number of physicians required to meet the current and future health needs of Canadians*	April 2020
12	6	Apr 25, 2017	DAD	*Mechanisms of Injury Priority Scores in Canada*	April 2020
13	43	May 3, 2017	DAD	*Determinants of adverse maternal and perinatal outcomes in Canada*	May 2020
14	104	Jun 5, 2017	CCRS, DAD, HCRS, NACRS, NPDUIS	*Economic and Humanistic Burden of Aortic Stenosis in Canada*	June 2020
15	167	Jun 22, 2017	DAD	*A systems approach for enhancing perinatal care regionalization*	June 2020
16	185	Jul 4, 2017	CAD	*PHAC Opioid Surveillance in Canada project*	July 2020

No.	DL #	Date Approved	Files Linked	Subject/ Project or Study Title	Date of Destruction
17	208	Jul 17, 2017	DAD and OMHRS	*Such a Scary Place for a Kid: The Impact of Youth Hospitalization on Adult Psychiatric Units*	July 2020
18	235	Jul 20, 2017	DAD, NACRS, PLPB	*Continuity of Care with Family Medicine Physicians: Why it Matters*	Jul 2020
19	324	Aug. 29, 2017	DAD and NACRS	*Health Care Cost of Cystic Fibrosis in Canada and Alberta*	Aug 2020
20	347	Sep 29, 2017	DAD and NACRS	*Temporal trends in the frequency of Emergency Department visits, surgery, and hospitalization for kidney stones*	Sep 2020
21	430	May 18, 2018	CORR, DAD, CMDB, OMHRS	*CORR-Collaborative Investigation into Home Dialysis Outcomes*	May 2021
22	466	Nov 2, 2017	DAD and NACRS	*Temporal trends in the frequency of Emergency Department visits, surgery, and hospitalization for obstructive sleep apnea*	Nov 2020
23	484	Nov 15, 2017	DAD and NTR	*An assessment of the impacts of Canadian minimum legal drinking age legislation (MLDA) on emergency department utilization and National Trauma Registry admissions for alcohol-related injuries among youth*	Nov 2020
24	493	Nov 17, 2017	DAD and NPDUIS	*Safety of bowel cleansers when combined with the stimulant laxative bisacodyl (Dulcolax and generics)*	Nov 2020
25	518	Dec 20, 2017	DAD and NTR	*Traumatic spinal cord injury incidence in Canada from 2004-present*	Dec 2020
26	555	Dec 12, 2017	DAD, HMDB, NACRS, NPDUIS	*Examining Cardiovascular Care in Canada*	Dec 2020
27	631	Feb 21, 2018	DAD and NACRS	*Improving Outcomes for Preterm Infants and their Families: A Canadian Collaborative Network*	Feb 2021
28	680	Feb 9, 2018	NPDUIS	*Prescription Opioid Use in Canada: Scope of Problem and Effects of Regulation*	Feb 2021

No.	DL #	Date Approved	Files Linked	Subject/ Project or Study Title	Date of Destruction
29	689	Feb 9, 2018	DAD and NACRS	*Scaling up INSPIRED approaches to COPD*	Feb 2021
30	724	Feb 27, 2018	NPDUIS and DAD	*Domperidone use among Canadian pregnant women*	Feb 2021
31	729	Apr 5, 2018	DAD, NACRS, NPDUIS	*"Evaluating the effects of pump coverage policy in Canada on pump uptake and health outcomes of patients with diabetes"*	Apr 2021
32	739	Mar 8, 2018	CPCD, DAD, HMDB, NACRS, NPDUIS, PLPB	*The Canadian Hysterectomy Alternatives*	Mar 2021
33	759	Mar 9, 2018	DAD and CCRS	*An examination of persons who receive/do not receive hospice care at end of life in long-term care facilities in Canada*	Mar 2021
34	793	Apr 4, 2018	NPDUIS	*Comparative Effectiveness and Safety of Biosimilar and Legacy Drugs*	Apr 2021
35	802	Mar 29, 2018	DAD and NACRS	*The Health Care Burden of Major Surgery in Canada*	Mar 2021

FY2017/18 – Linkages for a CIHI Use/Purpose

No.	DL #	Date Approved	Files Linked	Subject/ Project or Study Title	Date of Destruction
36	66	Mar 15, 2017	HMDB, NACRS, CCRS, HCRS, PLPB, NPDUIS	*Development of an interactive digital report to provide baseline information about palliative care in Canada*	Oct 2018
37	240	Aug 1, 2017	PLPB, DAD, NACRS, HCRS, CCRS, PRAG	*Impact of physician care on hospitalizations in seniors with multimorbidity*	Oct 2018

No.	DL #	Date Approved	Files Linked	Subject/ Project or Study Title	Date of Destruction
38	480	Nov 7, 2017	CCRS and NPDUIS	*An evaluation of the degree to which drug claims appear in NPDUIS that are consistent with the drug use coded in CCRS*	Oct 2018
39	787	Mar 22, 2018	DAD, HCRS, NACRS, NPDUIS, CCRS, OMHRS, PLPB, NRS	*Using Canadian Acute Care Data to Select/Develop a Frailty Measure to Inform the Quality of Care and Research in Seniors*	2019 – Extended retention of data pending

FY 2018/19 – Third-Party Requests for Data Linkage

No.	DL #	Date Approved	Files Linked	Subject/ Project or Study Title	Date of Destruction
40	845	Apr 16, 2018	CAD and PLPB	*Remuneration Study*	Apr 2021
41	877	May 4, 2018	CAD, CJRR, DAD, HMDB, NACRS	*Patellofemoral arthroplasty demographic and survival comparison from multiple joint registries*	May 2021
42	936	Jul 6, 2018	DAD, NACRS, NRS, HCRS, CCRS	*Stroke Report 2018*	Jul 2021
43	952	Jul 6, 2018	DAD, NACRS, NRS, HCRS	*Monitoring Cardiac Care in Canada – Annual Heart Report and Survivor Support – 2018 Report*	Jul 2021
44	962	Jun 26, 2018	DAD and OMHRS	*Epidemiological Relationships of Stroke and Dementia: A Canada Wide Study*	Jun 2021
45	1054	Jul 23, 2018	DAD and NPDUIS	*Evidence base around low dose codeine misuse and adverse events*	Jul 2021
46	1055	Aug 2, 2018	CJRR, DAD, NACRS	*Hip Fracture Outcomes in a Canadian Population*	Aug 2021
47	1062	Aug 2, 2018	NPDUIS, DAD, NACRS	*Intravitreal bevacizumab for retinal conditions: real world safety assessment*	Aug 2021

No.	DL #	Date Approved	Files Linked	Subject/ Project or Study Title	Date of Destruction
48	1074	Aug 13, 2018	NACRS and Ontario Workplace Safety and Insurance Board/ Workplace Safety and Insurance Board records	PHI disclosure *Improve the recognition of hazards in contemporary workplaces, and to better measure the performance of the Ontario prevention system by using records of emergency department visits in the surveillance of work-related injury and illness*	Aug 2021
49	1082	Jul 24, 2018	DAD	*Patient transfer for acute cardiovascular conditions: national practices and outcomes*	Jul 2021
50	1093	Aug 7, 2018	CORR, DAD, OMHRS, CMDB	*Contemporary trends and factors associated with home dialysis morbidities and mortality in Canada*	Aug 2021
51	1115	Aug 30, 2018	DAD and NACRS	*Understanding Frequent Emergency Department Visitors in Alberta and Ontario through Advanced Statistical Modeling Techniques*	Aug 2021
52	1117	Aug 28, 2018	CPERS and DAD	*To investigate the relationship between those identified as experiencing a hospital harm as part of CIHI's Hospital Harm indicator, and the respondents' self-reported experience of harm captured in CPERS-Inpatient Care*	Aug 2021
53	1176	Sep 27, 2018	CCRS, DAD, HCRS, NACRS	*Understanding long-term care (home and residential care) clientele and changes in client complexity over time*	Sep 2021
54	1201	Oct 12, 2018	HMHDB	*Psychiatric care in Canada*	Oct 2021
55	1219	Oct 30, 2018	DAD and NPDUIS	*Describing the Association of Potentially Inappropriate Medications and Health System Use in Canada*	Oct 2021
56	1222	Oct 12, 2018	DAD, NACRS, NPDUIS	*Association between initial opioid prescribing patterns and subsequent long term-use and associated harms among opioid naïve patients: A Canadian retrospective cohort study*	Oct 2021

No.	DL #	Date Approved	Files Linked	Subject/ Project or Study Title	Date of Destruction
57	1234	Oct 22, 2018	DAD and HMDB	*To examine trends in admission rate of adults patients diagnosed with asthma and COPD in Canada*	Oct 2021
58	1259	Oct 26, 2018	DAD and NACRS	*National Trends of Out of Hospital Cardiac Arrest*	Oct 2021
59	1337	Dec 5, 2018	CAD	*Canadian children previously hospitalized to the pediatric intensive care unit (PICU) for asthma exacerbation: long-term rehospitalisation rates and associated predictors*	Dec 2021
60	1359	Jan 2, 2019	CCRS, HCRS, DAD, NACRS	*Identifying and predicting trajectories of decline in physical and cognitive function*	Jan 2022
61	1382	Jan 31, 2019	DAD, NPDUIS, NACRS	*Patterns of use of SGLT2i and risk of DKA among diabetes mellitus patients*	Jan 2022
62	1389	Jan 7, 2019	CCRS, HCRS, DAD, NACRS, HMHDB	BN Linkage DAD, NACRS, CCRS, HCRS, HMHDB *Identifying Risk and Transitions Among Frequent Emergency Department Users: Whose Needs Can Safely Be Met Elsewhere?*	Jan 2022
63	1409	Jan 24, 2019	SPOR Dynamic Cohort (DAD, NACRS, OMHRS) and DAD	*High cost users' inpatient care at the end of life (SPOR) – Patient characteristics, course of treatment, and involvement of palliative care*	Jan 2022
64	1432	Jan 23, 2019	DAD and NACRS	*Epidemiology of Rare Cancers in Canada: Developing a framework for surveillance, cost analysis and etiologic research*	Jan 2022
65	1470	Feb 28, 2019	DAD	*Adult Congenital Heart Disease, Pregnancy and Long-Term Cardiovascular Functioning*	Feb 2022
66	1502	Mar 6, 2019	NPDUIS	*CNODES Common Data Model Pilot Project*	Mar 2022
67	1566	May 23, 2019	DAD, NACRS, NRS, OMHRS	*Developing a multi-source surveillance system for Fetal Alcohol Spectrum Disorder and Prenatal Alcohol Exposure (SSFASD/PAE) in Canada*	Jun 2022
68	1591	Apr 25, 2019	DAD, HCRS, CMDB	*Transitions in and out of home care*	May 2022

FY2018/19 – Linkages for a CIHI Use/Purpose

No.	DL No.	Date Approved	Files Linked	Subject/ Project or Study Title	Date of Destruction
69	842	May 28, 2018	CPERS and DAD	Data linkage of CPERS data to DAD for 2 purposes (See also DL-963). This approval was for activities that are part of an ongoing program of work: *1. Enhance the reporting methodology for the CPERS Comparative Results Tool* *2. Identify and report service line information currently missing in CPERS but available in DAD*	N/A On-going linkage
70	882	May 11, 2018	DAD, NACRS, PHC	*Explore the quality and comparability of data*	Apr 2020
71	960	Jun 11, 2018	DAD and NACRS	*Yukon hospital profiles*	May 2019
72	963	May 28, 2018	CPERS and DAD	Data linkage of CPERS data to DAD for 2 purposes (See also DL-842). This approval was for time-limited CIHI analytical project. *Exploring drivers and variations in positive care experiences in Canadian hospitals*	– Nov 2019
73	1004	Jul 9, 2018	DAD and NRS	Stroke Congress: *Further explore how projected function scores relate to inpatient rehabilitation outcomes for patients with stroke, using descriptive and comparative statistics*	Jul 2021
74	1046	Aug 7, 2018	CJRR, CAD, CPCD	*Implant Cost Analyses - examine the relationships between joint replacements, outcomes, and costs*	Jul 2021
75	1067	Aug 31, 2018	OMHRS, DAD, NACRS	On-going linkage for the replacement of postal codes missing in OMHRS (postal code rescue) to: *1. support OMHRS's analytical work; and* *2. fulfill an MOHLTC request for the rescued postal codes in its quarterly cuts of OMHRS data*	N/A On-going linkage
76	1185	Nov 9, 2018	CCRS and NACRS	Data Linkage (CCRS and NACRS) - Proof of Concept (Data Hub)	– Nov 2019

No.	DL No.	Date Approved	Files Linked	Subject/ Project or Study Title	Date of Destruction
77	1264	Nov 5, 2018	PROMs, CJRR, DAD, NACRS	On-going linkage PROM_CJRR, DAD, NACRS *(1) Ontario PROMs pilot (2) CIHI leadership for the OEC*	N/A On-going linkage
78	1306	Jan 12, 2019	PLPB, DAD, NACRS	*Does Having a Usual Primary Care Provider Influence Hospitalization and Emergency Department Visit Rates?*	Nov 2021
79	1363	Dec 6, 2018	DAD, NACRS, OMHRS	*Examine trajectories of care for individuals who are included in the SHP indicator Repeat Emergency Department (ED)/Urgent Care Centre Visits for Mental Health & Addiction and compare them to less frequent ED users for mental health and addictions*	May 2020
80	1380	Feb 8, 2019	DAD and PLPB	*Test the ability to link Ontario PLPB to DAD*	Feb 2020
81	1410	Jan 21, 2019	DAD and NRS	*Investigate coding practices for clients with spinal dysfunction, including clients with spinal cord dysfunction and clients with orthopaedic spinal surgery*	Jan 2023
82	1426	Jan 21, 2019	CCRS and NACRS	*Data Hub second Proof of Concept*	Apr 2019
83	1431	Jan 28, 2019	PLPB and DAD	*Patient Cost Estimator (PCE)*	Mar 2021
84	1499	Mar 6, 2019	PHC, DAD, NACRS	*Explore the quality and comparability of data*	Mar 2021
85	1569	Apr 30, 2019	OMHRS, CCRS, CPCD	*Development and evaluation of variants of the RUG-III Plus case-mix system*	Dec 2020

April 1, 2019 – October 31, 2019 (FY2019/20) – Third-Party Requests for Data Linkage

No.	DL No.	Date Approved	Files Linked	Subject/ Project or Study Title	Date of Destruction
86	1605	May 9, 2019	DAD, NACRS	*Exposure of low-dose ionizing radiation (LDIR) from imaging procedures and cancer in Canada's adult and children population with congenital heart disease (CHD)*	May 2022
87	1625	May 6, 2019	CORR, DAD, NACRS	*Reducing Diabetic Foot Complications Through A Multidisciplinary Chiropodist-Based Intervention*	May 2022
88	1656	May 15, 2019	DAD, NACRS, CORR	*Contemporary anemia management and outcomes in incident dialysis patients in Canada*	May 2022
89	1676	May 22, 2019	DAD, NPDUIS	*Acetaminophen and Acute Liver Injury*	July 2020
90	1679	May 15, 2019	DAD	*Prevalence of non-resident births in Canada*	Aggregate Disclosure – No destruction requirement
91	1696	May 22, 2019	DAD, NACRS	*Efficacy of Toe and Flow Model in Canadian Health Care*	June 2022
92	1701	Jun 10, 2019	DAD, NACRS	*Prevalence, incidence and health impact of hemochromatosis in Canada*	May 2021
93	1724	Jun 12, 2019	DAD, NACRS	*The impact of introduction of Quality Based Procedures (QBP) for hip and knee replacement on orthopedic care quality, intensity and care substitution in Ontario*	Jun 2022
94	1746	Jun 20, 2019	DAD	Re-purpose of previously linked data *Assessing the association between the spatiotemporal distribution of Kawasaki disease and environmental factors: discovering clues into the elusive etiology of a complex disease*	Jun 2021
95	1775	Jul 16, 2019	DAD, NACRS, NPDUIS	*Association between initial opioid prescribing patterns and subsequent long term-use and associated harms among opioid naïve patients: A Canadian retrospective cohort study*	Jul 2020

No.	DL No.	Date Approved	Files Linked	Subject/ Project or Study Title	Date of Destruction
96	1792	Sep 13, 2019	DAD, NACRS, Emergency Medical Service data from the client	PHI Disclosure (Research Agreement not signed) *Measure the true burden of sudden cardiac arrest within the Greater Toronto Area*	Oct 2022
97	1817	Jul 25, 2019	DAD	*Determining the Spatiotemporal Association between Weather, Hospital Admissions and Mortality Related to Acute Cardiac Events in Canada*	Aug 2022
98	1841	Sep 11, 2019	CORR, DAD, CMDB, OMHRS	Re-Purpose of previously linked data *Towards a Better Understanding of Hospitalization in Home versus In-Center Dialysis*	Oct 2022
99	1882	Sep 3, 2019	CCRS, HCRS, DAD, NACRS, NRS	*Annual update on Heart and Stroke in Canada - 2020*	Sep 2022
100	1894	Sep 13, 2019	DAD	*Regional and temporal variations in incidence, prevalence and outcomes of critical illness among pregnant and post-partum women and newborns in Canada*	Oct 2022
101	1921	Oct 3, 2019	DAD, NACRS	*Explore rates of re-excision following breast conserving surgery and reconstruction surgery performed at the same time as the initial procedure*	Oct 2022
102	1939	Oct 10, 2019	DAD, NACRS	*Incidence, Treatment Trends and Complications for Symptomatic Kidney Stones in Canada- A Population-Based Study*	Oct 2022
103	1945	Oct 23, 2019	CORR, DAD	*Impact of socioeconomic factors on living kidney donation: A Canadian Perspective*	Nov 2022
104	1997	Oct 31, 2019	DAD, NACRS	*Epidemiology of Pediatric Injury and Ambulance Transport in Ontario*	Nov 2022

No.	DL No.	Date Approved	Files Linked	Subject/ Project or Study Title	Date of Destruction
105	1501	July 5, 2019	DAD, NACRS, OMHRS	PHI Disclosure (2 recipient institutions) *Micro and Macro Predictors of Readmissions among Patients Discharged from a Tertiary Mental Health Hospital*	July 2022

April 1, 2019 – October 31, 2019 (FY2019/20) – Linkages for a CIHI Use/Purpose

No.	DL No.	Date Approved	Files Linked	Subject/ Project or Study Title	Date of Destruction
106	1702	Jun 4, 2019	CCRS, DAD, HCRS, NACRS, NRS	*Development of case-mix groupers*	Dec 2020
107	1731	Jun 11, 2019	DAD, NACRS, OMHRS, Primary Health Care (PHC) Electronic Medical Record (EMR) records	*Proof of concept analysis focused on Mental Health and Addiction*	Apr 2020
108	1732	Jun 18, 2019	DAD-HMDB, NACRS, PLPB, NRS, HCRS, CCRS, POP	*Children and youth with medical complexity*	Jun 2021
109	1759	Jun 27, 2019	DAD, PLPB	*Physician cost estimate for analytical report on comparing costs for hip and knee replacement primary and revision surgeries*	Mar 2021
110	1771	Jul 4, 2019	POP, PHC EMR (Primary Health Care Emergency Medical Records)	*Assess the feasibility of using EMR data to enhance the Population Grouping Methodology*	Apr 2020
111	1831	Aug 14, 2019	CCRS, HCRS	*Long-term Care Provided at the Appropriate Time (Indicator)*	Dec 2020

No.	DL No.	Date Approved	Files Linked	Subject/ Project or Study Title	Date of Destruction
112	1702	Jun 4, 2019	CCRS, DAD, HCRS, NACRS, NRS	*Data linkage for internal CIHI purposes - development of case-mix groupers*	Dec 2020
113	1957	Oct 16, 2019	DAD, PLPB	*Implantable medical devices – insights into costs, high volume procedures and complications*	Mar 2020
114	1995	Oct 30, 2019	OSMHC EMR data, OMHRS, NACRS	*Evaluate the relationship between adherence to OSMHC clinical standards and patient outcomes*	Nov 2022

Appendix B - Privacy Impact Assessment Log

Data Holding / Information System / Technology / Program	Last Completed	Next Scheduled 5-Yr Renewal	Comments	Statement of Purpose Reviewed
Specialized Care				
Hospital Mental Health Database	2016-17	2021-22		Reviewed – no change
Home Care Reporting System	2016-17*	2021/22		Reviewed – no change
Continuing Care Reporting System	2016-17*	2021-22		Reviewed – no change
Ontario Mental Health Reporting System	2016-17*	2021-22		Reviewed – no change
National Rehabilitation Reporting System	2015-16	2020-21		Reviewed – no change
interRAI Reporting System (IRRS)			In progress – expected completion Q4 2019-20	New PIA
Advanced Analytics				
Population Risk Adjustment Grouping (PRAG) Project	2014-15	2019-20	Renewal in progress – expected completion Q4 2019-20	
Pharmaceuticals and Health Workforce Information Services				
National Prescription Drug Utilization Information System	2017-18*	2022-23		Reviewed – no change
National System for Incident Reporting	2018-19*	2023-24	De-identified data	Reviewed – no change
Patient-Level Physician Billing Repository	2014-15	2019-20	Renewal in progress – expected completion Q4 2019-20	
Health Spending & Strategic Initiatives				
Canadian Patient Cost Database	2018-19*	2023-24		Reviewed – no change
Clinical Data Standards & Quality				
Reabstraction Studies	2015-16	2020-21	This is a new PIA, first conducted in 2015-16.	

Integrated e-Reporting and Portal Services				
CIHI Portal	2014-15	2019-20	De-identified data – Renewal in progress – expected completion in Q4 2019-20	
Your Health System: Insight	2015-16	2020-21		
Clinical Administrative Databases and Decision Support Services and Clinical Registries				
Canadian Joint Replacement Registry (CJRR)	2017-18*	2022-23		Reviewed – no change
Canadian Organ Replacement Register (CORR)	2017-18*	2022-23		Reviewed - no change
Clinical Administrative Database (DAD, HMDB, NACRS)	2019-20*	2024-25		Reviewed – no change
Trauma Registries	2019-20*	2024-25		Reviewed – no change
Canadian Patient Experiences Data Collection and Reporting System	2014-15	2019-20	Renewal in progress – expected completion Q4 2019-20	
Patient Reported Outcome Measures (PROMs)	2019-20*	2024-25		New PIA

***11 PIAs** reviewed and completed within the current review period, 1 of which was a PIA for de-identified data (NSIR)

Appendix C - CIHI'S Privacy Impact Assessment Program – Summary of Recommendations

Description of Privacy Impact Assessment	Recommendations	Manner Addressed	Date Recommendation Completed
Population Risk Adjustment Group (PRAG) Project A renewal of the privacy impact assessment of the privacy and security risks associated with the Population Risk Adjustment Grouping Project which was established to develop a methodology and grouping software for population grouping using CIHI data and expertise.	Renewal in progress		
Patient Level Physician Billing Data Repository A renewal of the privacy impact assessment of the privacy and security risks associated with the Patient-Level Physician Billing (PLPB) Repository. The PLPB Repository was established to support patient-focused analysis, to support CIHI's development of more comprehensive inpatient cost estimates and to enhance the quality of historical National Physician Database data and indicators.	Renewal in progress		
Canadian Patient Experiences Data Collection and Reporting System A renewal of the privacy impact assessment of the privacy and security risks associated with the Canadian Patient Experiences Data Collection and Reporting System (CPERS). CPERS collects and reports on patient experiences within the health care system in Canada, beginning with inpatient acute care hospitals. The purpose of the CPERS is to provide standardized patient experience information from across Canada.	Renewal in progress		

Description of Privacy Impact Assessment	Recommendations	Manner Addressed	Date Recommendation Completed
Patient Reported Outcome Measures (PROMs) For Hip and Knee Arthroplasty A privacy impact assessment of the privacy and security risks associated with the collection and reporting of patient-reported outcome measures (PROMs) for hip and knee arthroplasty.	No recommendations	n/a	n/a
CIHI Portal A renewal of the privacy impact assessment of the privacy and security risks associated with CIHI Portal, which is an analytical web-based tool for health care data. CIHI designed it to provide clients with secure online access to selected de-identified pan-Canadian health care data already held at CIHI.	Renewal in progress		
Clinical Administrative Databases A renewal of the privacy impact assessment of the privacy and security risks associated with the Clinical Administrative Databases (CAD) that collect patient data from admission to discharge for inpatient acute visits, emergency department visits and outpatient (ambulatory care) visits, such as those in clinics or day surgery settings.	No recommendations	n/a	n/a
Trauma Registries A renewal of the privacy impact assessment of the privacy and security risks associated with the National Trauma Registry and the Ontario Trauma Registry, collectively referred to as the Trauma Registries, which contain personal health information related to acute care hospitalizations due to injury and trauma.	No recommendations	n/a	n/a
interRAI Reporting System (IRRS) A privacy impact assessment of the privacy and security risks associated with IRRS, which is a new data collection method (near real-time message based) and new validation process using a cloud-based application.	New – in progress		

Description of Privacy Impact Assessment	Recommendations	Manner Addressed	Date Recommendation Completed
National System for Incident Reporting A renewal of the privacy impact assessment of the privacy and security risks associated with the National System for Incident Reporting, a voluntary reporting system designed to securely and anonymously support the collection, sharing and analysis of standardized incident data (de-identified data). The PIA includes the assessment of the newly implemented radiation treatment (RT) incident-reporting module.	No recommendations	n/a	n/a
Canadian Patient Cost Database A renewal of the privacy impact assessment of the privacy and security risks associated with the Canadian Patient Cost Database (CPCD). CPCD is engaged in patient costing, a process of estimating the actual costs of care for individual service recipient encounters, such as inpatient admissions, emergency visits, ambulatory visits and health centre visits. The PIA includes a review of current and ongoing expansion of operations in terms of an increased volume of records and greater diversity in the types of service recipients.	No recommendations	n/a	n/a

Description of Privacy Impact Assessment	Recommendations	Manner Addressed	Date Recommendation Completed
National Prescription Drug Utilization Information System A renewal of the privacy impact assessment of the privacy and security risks associated with the National Prescription Drug Utilization Information System (NPDUIS), a pan-Canadian database that collects data regarding claims submitted to public drug programs for payment or that were processed for documentation under a drug information system.	No recommendations	n/a	n/a
Canadian Joint Replacement Registry A renewal of the privacy impact assessment of the privacy and security risks associated with the Canadian Joint Replacement Registry, a national registry that collects patient-specific information (clinical, surgical and prosthesis) on hip and knee replacement surgeries performed in Canada. It is a longitudinal database that allows for joint replacement patients to be followed over time to monitor their revision rates and outcomes.	No recommendations	n/a	n/a
Canadian Organ Replacement Registry A renewal of the privacy impact assessment of the privacy and security risks associated with the Canadian Organ Replacement Register (CORR), a national register of patients treated for end-stage renal and extra-renal organ failure and transplantation, as well as organ donors, in Canada. The CORR is a longitudinal database that follows a patient from his or her first treatment for end-stage organ failure (dialysis or transplantation) until the patient dies or is lost to follow-up.	No recommendations	n/a	n/a

Description of Privacy Impact Assessment	Recommendations	Manner Addressed	Date Recommendation Completed
Home Care Reporting System A renewal of the privacy impact assessment of the privacy and security risks associated with the Home Care Reporting System (HCRS), a pan-Canadian database that captures standardized information regarding publicly funded home care services, including clinical, demographic, administrative and resource utilization data about recipients of home care services.	No recommendations	n/a	n/a
Continuing Care Reporting System A renewal of the privacy impact assessment of the privacy and security risks associated with the Continuing Care Reporting System (CCRS), a pan-Canadian database that captures standardized information regarding publicly funded continuing care services, including clinical, demographic, administrative and resource utilization data about residents of continuing care facilities.	No recommendations	n/a	n/a
Ontario Mental Health Reporting System A renewal of the privacy impact assessment of the privacy and security risks associated with the Ontario Mental Health Reporting System (OMHRS), a longitudinal reporting system that captures data on hospital mental health inpatients at multiple points throughout their episodes of care.	No recommendations	n/a	n/a

Appendix D - CIHI'S Privacy Audit Program

Fiscal Year: 2012-13

Description of Audit	Recommendations	Manner Addressed	Completion Date Recommendations Completed
Identity Management Security Assessment to determine whether: • Deployment of people, processes and technologies in Identity Management project has been done in a privacy and security sensitive manner • Technologies have been appropriately privacy and security tested • Processes have been documented, including risk analysis. Audit completed: May 1, 2014	There were 8 recommendations identified to enhance existing identity and access management practices. Due to the confidential nature of these recommendations, the specifics will not be provided here.	All recommendations were accepted and rolled into the Identity Management program of work.	March 2017

Fiscal Year: 2016-17

Description of Audit	Recommendations	Manner Addressed	Date Recommendations Completed
A compliance audit of an external third-party that receives data from CIHI to ensure the third-party is meeting or has met its contractual obligations, as set out in CIHI's confidentiality agreement. Audit completed: September 1, 2016	**Major non-conformity Re: Encryption** The recipient should also create and document a policy and procedure for regularly updating the encryption solution. **Minor non-conformity Re: General security obligation to safeguard CIHI data** The recipient must not store passwords alongside the data they are designed to protect. **Minor non-conformity Re: General security obligation to safeguard CIHI data** The recipient is to implement standard procedures to update and remove old user accounts from the dedicated research computer. **Minor non-conformity Re: General security obligation to safeguard CIHI data** The recipient is to review the Secure Destruction Information Package issued by CIHI and integrate CIHI's secure destruction requirements into existing standard operating procedures (e.g. data transfer process). **Minor non-conformity Re: General security obligation to safeguard CIHI data** The recipient is to properly acknowledge the use of CIHI data in research publications by including in any output from a research project or analytical study an acknowledgement in the following form: "Parts of this material are based on data and information provided by the Canadian Institute for Health Information. However, the analyses, conclusions, opinions and statements expressed herein are those of the author and not those of the Canadian Institute for Health Information."	Accepted as per recommendation	March, 2017

Description of Audit	Recommendations	Manner Addressed	Date Recommendations Completed
A privacy audit of CIHI's Identity and Access Management System to determine whether: • The authorization and authentication procedures for identity management are being followed; • Security Incidents have occurred as a result of failure to comply with Identity management standard operating procedures The objective of this the 4-phased privacy audit of CIHI's Identity and Access Management System, which began in 2013-14, was to determine whether Clients who have access to CIHI's restricted applications have been appropriately authorized. Audit completed: January 2, 2017	**Update from previous submission:** No instances of unauthorized access were identified through the audit; however, the following recommendations were made: 1. Additional Central Client Services (CCS) resources be provided to audit the 122 organizations that did not respond during phase I of the audit; 2. the constraints with generating reports from the Access Management System (AMS) be addressed through system enhancements to the AMS. This work has been delayed due to resources being allocated to higher corporate priority projects, such as Accessibility for Ontarians with Disabilities Act (AODA); and 3. A root cause analysis be completed and action plan developed to understand why organizations are not advising CIHI of changes to Organizational Contact information and why Organizational Contacts are not submitting requests to change or revoke access, and how this process can be improved.	Accepted as per recommendation Accepted as per recommendation Accepted as per recommendation	Completed Q1 2017-18 Completed Q2 2017-18 Completed Q4 2018-19

Fiscal Year: 2018-19

Description of Audit	Recommendations	Manner Addressed	Date Recommendations Completed
A compliance audit of an external third-party that received data from CIHI to ensure the third-party is meeting or has met its contractual obligations, as set out in CIHI's confidentiality agreement. Audit completed: October 26, 2018	5 non-conformities and 1 opportunity for improvement resulted in the following 8 recommendations:		
	1. Establish or amend existing policies for contract execution and management, including termination and closeout to ensure all objectives and requirements related to data acquisition and disposal are met.	Accepted as per recommendation	Completed (Sep 2019)
	2. Establish a person or body with responsibility for overseeing recipients of data from external third parties to ensure they comply with obligations that may be set out in a legal instrument.	Accepted as per recommendation	In Progress
	3. Implement an auditable process for the receipt, protection, retention and disposal of PHI, regardless of format, it receives from external third parties; and promptly notify third party organizations from whom PHI is obtained about any likely or impending breach of a term or condition set out in a legal instrument.	Accepted as per recommendation	Near Completion—formal auditing to commence late Fall 2019
	4. Enhance its access management and back-up systems to ensure logs capture information about who and when folders and data files, for example, are accessed and deleted.	Accepted as per recommendation	Completed (Sep 2019)
	5. Store PHI in a separate location from staff's personal drive on the network, which would allow the organization to audit locations that contain PHI, only.	Accepted as per recommendation	Completed (Sep 2019)
	6. Provide additional training to its IT staff to ensure they are knowledgeable about the capabilities of access management and back-up systems, and processes.	Accepted as per recommendation	Completed (May 2019)
	7. Develop off-boarding (or transitioning) processes to address situations where significant changes are made to the roles and responsibilities of its employees, contractors, and agents who are engaged in research and use external third-party data obtained under a legal instrument; and communicate to those third parties when a change (e.g., change in employment status) to any	Accepted as per recommendation	In Progress (Spring 2020)

Description of Audit	Recommendations	Manner Addressed	Date Recommendations Completed
	provision set out in a legal instrument is required to ensure a written amendment is duly executed. 8. An opportunity for improvement was identified which resulted in 1 recommendation to develop and implement administrative measures (e.g., supplementary instruction) and/or technical measures such as auditing of access logs in situations where cohort data (e.g., PHI from a third- party) is copied or downloaded from a server to a USB or other similar portable device.	Accepted as per recommendation	Completed (Sep 2019)
A compliance survey audit of external third-parties that received and continue to retain de-identified data and/or personal health information from CIHI to ensure the third-parties continue to meet their contractual obligations, as set out in the agreement signed with CIHI. This compliance survey audit replaced the standard annual certification activity for 2018. Audit completed: June 1, 2019	10 respondents were issued and have addressed 12 corrective measures recommended by CIHI to bring the organizations into compliance. Corrective measures implemented by accountable organizations: 1. Accountable organization that previously employed the principal investigator certified secure destruction of all CIHI data received for the project. 2. Organization (new accountable organization) where the principal investigator commenced employment entered a disclosure agreement with CIHI. 3. New principal investigator completed and returned a CIHI form binding the individual to the respective disclosure agreement between CIHI and the accountable organization. 4. The accountable organization certified secure destruction all CIHI data received for the project. 5. The accountable organization completed and returned an amendment form to CIHI, adding a new authorized person requiring access to previously disclosed CIHI data. 6. The accountable organization completed and returned an amendment form to CIHI, adding a new authorized person requiring access to previously disclosed CIHI data. 7. The accountable organization completed and returned an amendment form to CIHI, adding a new authorized person requiring access to previously disclosed CIHI data.	Accepted as per recommendations	Completed June 2019

Description of Audit	Recommendations	Manner Addressed	Date Recommendations Completed
	8. The accountable organization completed and returned an amendment form to CIHI, adding a new authorized person requiring access to previously disclosed CIHI data. 9. The accountable organization ceased secure remote access from outside Canada. 10. Organization securely destroyed failed hard-drive containing CIHI data, as well as the CIHI data temporarily stored on a portable storage device. 11. Organization deployed encryption solution compliant with CIHI standards to external hard drive (used for backup purposes). 12. Organization deployed encryption solution compliant with CIHI standards to desktop computing device (used to analysis CIHI data).		

Fiscal Year: 2019-20

Description of Audit	Recommendations	Manner Addressed	Date Recommendations Completed
A compliance audit of an external third-party that received personal health information from CIHI to ensure the third-party is meeting or has met its contractual obligations, as set out in CIHI's research agreement.	In progress		
An internal privacy audit of CIHI's Access Management System to validate that access by both external clients and CIHI agents to CIHI's secure applications and tools containing personal health information is still required.	In progress		

Appendix E - External Audit of CIHI's Privacy and Security Program

Fiscal Year: 2017-18

Description of Audit	Recommendations	Manner Addressed	Date Recommendation Completed
IPC/ON's mandatory 3-year review of CIHI's Prescribed Entity status. Audit completed: October 31, 2017	It is recommended that, at a minimum, all the privacy policies, procedures and practices put in place by CIHI, be reviewed by CIHI at least once to each scheduled review of these policies, procedures and practices by the IPC/ON pursuant to section 45(4) of the *Act*.	As per recommendation	October 2017

Appendix F - CIHI'S Security Audit Program

Fiscal Year: 2016-17

Description of Audit	Description of Recommendation	Manner Addressed	Completion Date
External Third Party Vulnerability Assessment and Penetration Test Through external internet penetration testing and internal system vulnerability testing (DMZ perimeter and internal LAN), ensure: • CIHI's security architecture is well designed and provides protection from external intruders, • CIHI's security infrastructure guarding CIHI's LAN/WAN network provides protection and robust security and, The confidentiality, integrity and availability of CIHI's electronic information assets are protected. <u>Key activities – Physical Security – Toronto</u> • Assessment of Toronto's physical security controls Key activities – External: • Perform exploratory vulnerability scanning across multiple "Class C" CIHI addresses • Penetration test of up to 12 targeted IPs Key activities – Internal: • Assessment of 250 servers and 1000 workstations Conducted October 2016	External Penetration Test: • 8 high-level recommendations • 10 technical recommendations Internal Network and Physical Security Assessment: • 6 high-level recommendations • 13 technical recommendations Due to the sensitive nature of the recommendations, they will not be articulated in this report.	Addressed/Completed	External Pen Test: 1. April 2017 2. Jan 2017 3. March 2017 4. March 2017 5. April 2017 6. April 2017 7. March 2017 8. March 2017 9. March 2017 10. March 2017 11. April 2017 12. April 2017 13. June 2017 14. March 2017 15. March 2017 16. March 2017 17. April 2017 18. Jan 2018 Internal/Physical Test: 1. Nov 2016 2. Nov 2016 3. Nov 2016 4. Nov 2016 5. Nov 2016 6. Nov 2016 7. Nov 2016 8. March 2017 9. Nov 2016

Description of Audit	Description of Recommendation	Manner Addressed	Completion Date
			10. Nov 2016 11. Nov 2016 12. Nov 2016 13. June 2016 14. Nov 2016 15. March 2017 16. March 2017 17. March 2017 18. Nov 2016 19. Nov 2016

Fiscal Year: 2017-18

Description of Audit	Description of Recommendation	Manner Addressed	Completion Date
External Third Party Vulnerability Assessment and Penetration Test Through external internet penetration testing and internal system vulnerability testing (DMZ perimeter and internal LAN), ensure: • CIHI's security architecture is well designed and provides protection from external intruders, • CIHI's security infrastructure guarding CIHI's LAN/WAN network provides protection and robust security and, The confidentiality, integrity and availability of CIHI's electronic information assets are protected. <u>Key activities – Physical Security – Toronto</u> • Assessment of Toronto's physical security controls Key activities – External: • Perform exploratory vulnerability scanning across multiple "Class C" CIHI addresses • Penetration test of up to 12 targeted IPs Key activities – Internal: • Assessment of 250 servers and 1000 workstations Conducted January 2018	Internal/External Assessment Report: • 22 recommendations Physical Security Assessment • 7 recommendations Due to the sensitive nature of the recommendations, they will not be articulated in this report.	Addressed/Completed	Internal/External Assessment: 1. Jan 2018 2. Feb 2018 3. Feb 2018 4. Feb 2018 5. Feb 2018 6. Feb 2018 7. Feb 2018 8. Feb 2018 9. July 2018 10. July 2018 11. July 2018 12. Sept 2018 13. Sept 2018 14. Feb 2018 15. Sept 2018 16. Feb 2018 17. April 2018 18. April 2018 19. May 2018 20. May 2018 21. Nov 2018 22. Feb 2018 Physical Security: 1. Jan 2018 2. Aug 2018 3. Jan 2018 4. Jan 2018 5. Aug 2018 6. April 2018 7. Jan 2018

Fiscal Year: 2018-19

Description of Audit	Description of Recommendation	Manner Addressed	Completion Date
External Third Party Vulnerability Assessment and Penetration Test Through external internet penetration testing and internal system vulnerability testing (DMZ perimeter and internal LAN), ensure: • CIHI's security architecture is well designed and provides protection from external intruders, • CIHI's security infrastructure guarding CIHI's LAN/WAN network provides protection and robust security and, The confidentiality, integrity and availability of CIHI's electronic information assets are protected. <u>Key activities – Physical Security – Toronto</u> • Assessment of Toronto's physical security controls Key activities – External: • Perform exploratory vulnerability scanning across multiple "Class C" CIHI addresses • Penetration test of up to 12 targeted IPs Key activities – Internal: • Assessment of 250 servers and 1000 workstations Conducted November 2018	External Assessment: • 7 recommendations Internal / Physical Assessment: • 23 recommendations Social Engineering Assessment: • 4 recommendations	Addressed/Completed	External Assessment : 1. Dec 2018 2. Jan 2019 3. Jan 2019 4. Dec 2018 5. Still in progress 6. Dec 2018 7. Still in progress Internal/Physical Assessment: 1. Dec 2018 2. Dec 2018 3. Nov 2018 4. Jan 2019 5. Jan 2019 6. Nov 2018 7. Jan 2019 8. Dec 2018 9. Dec 2018 10. March 2019 11. Feb 2019 12. Feb 2019 13. Dec 2018 14. Jan 2019 15. Apr 2019 16. Jan 2019 17. Still in progress 18. Dec 2018 19. Dec 2018 20. Dec 2018 21. Dec 2018 22. Still in progress

Description of Audit	Description of Recommendation	Manner Addressed	Completion Date
			23. March 2019 Social Engineering: 1. March 2019 2. March 2019 3. March 2019 4. March 2019

Fiscal Year: Ongoing regular audits

Description of Audit	Description of Recommendation	Manner Addressed	Completion Date
Database Security Audit Monthly database security audit to examine all instances of inappropriate sharing of accounts and excessive failed login attempts to CIHI databases for potential security threats. The audit also examines all the current database connections for any potential security implications.	N/A	N/A	N/A
Yearly Internal Data Access Audit Yearly internal data access audit to ensure only authorized staff have access to PHI in CIHI's analytical environment. The audit identifies all individuals who have access to data in CIHI's analytical environment and requires management to formally request continued access or removal for each employee, as appropriate.	N/A	N/A	N/A
Local Administrator Audit Internal audit of local administrator user access to desktop and laptop computers. For any unapproved administrator rights that are discovered, an Incident is opened and the administrator privileges are removed.	N/A	N/A	N/A

Description of Audit	Description of Recommendation	Manner Addressed	Completion Date
ISO/IEC 27001:2013 Surveillance / Recertification Audit The ISO/IEC 27001:2013 is conducted on an annual basis as required by the standard. The purpose of this audit is to ensure CIHI continues to meet the requirements of the Standard and continues to maintain its certification. Conducted in July of each fiscal year.	2017-2018 Audit - 2 Findings 2018-2019 Audit - 5 Findings 2019-2020 Audit - 4 Findings	Completed/Addressed	2017-2018 1. November 2017 2. November 2017 2018-2019 1. December 2018 2. December 2018 3. March 2019 4. May 2018 5. In-progress (re-opened due to another finding) 2019-2020- All findings in progress

ISMS Internal Audit The ISMS Internal Audit is conducted on an annual basis as required by the ISO/IEC 27001:2013 standard. An external party is procured to execute this audit on behalf of CIHI. The purpose of the ISMS Internal Audit is to ensure that CIHI's ISMS conforms to the requirements of the ISO/IEC 27001:2013 standard and that it is effectively implemented and maintained. Conducted in May of each fiscal year.	2017-2018 Audit – 19 2018-2019 Audit – 14 2019-2020 Audit – 6	Completed/Addressed	2017-2018 1. December 2017 2. December 2017 3. December 2017 4. October 2017 5. April 2018 6. June 2017 7. June 2017 8. February 2019 9. June 2017 10. June 2017 11. December 2017 12. June 2017 13. August 2017 14. June 2017 15. June 2017 16. September 2017 17. April 2018 18. December 2017 19. June 2017 2018-2019 1. July 2018 2. February 2019 3. March 2019 4. January 2019 5. December 2018 6. December 2018 7. September 2018 8. January 2019 9. September 2018 10. August 2018 11. February 2019 12. April 2019 13. April 2019 14. February 2019

Description of Audit	Description of Recommendation	Manner Addressed	Completion Date
			2019-2020 - All findings in progress

.

Appendix G - InfoSec Staff Awareness, Education and Communication Log

Date	Provider	Attendees	Subject
2016-11-02	GTEC	Hassan Gesso	http://www.gtec.ca/
2016-12-07	ISACS	Hassan Gesso	CISA Certification – Granted certification as a Certified Information Systems Auditor (CISA) on December 7, 2016
2016-12-05	Targeted	Bits 'n' Bytes (ITS)	Infosec Branch Update
2017-01-04	Internal	All CIHI Staff	Privacy Awareness Month
2017-01-13	InfoSec		Phishing Scenario
2017-01-23	Internal	CIHIghway	InfoSec News
2017-02-13	Internal	CIHIghway	Security Warning: Phishing Emails
2017-03-31	IEEE Ottawa	Hassan Gesso	Internet of Things – Things You Need to Know
2017-04-10	ITS Staff	All CIHI Staff	ITS Bits and Bytes
2017-05-12	Cal Marcoux, Hassan Gesso	ISTS Branch	Quarterly Update – overview of the last quarter, upcoming projects, activites, challenges
2017-05-12	Cal Marcoux, JL Guertin	Senior Management Committee, IT Leadership Team, Security	Ransomware Updates
2017-05-22	Infrastructure and Technology Services	All CIHI Staff	Infrastructure Updates: DR Test, AnyConnect Software Update, ITS Maintenance and Mobile Pass
2017-05-24	ISACA OVC	Hassan Gesso	Business Architecture Driven Risk Bases Audit Plan
2017-05-29	Cal Marcoux	DL-ISTS	Gentle Reminder – Incidents, outages and communication

2017-06-06	OCC	Hassan Gesso, Cal Marcoux	Ontario Connections Conference
2017-06-15	ISAC AGM	Hassan Gesso	Annual General Meeting-ISACA Ottawa Valley Chapter & AEA Ottawa-Gatineau Chapter
2017-06-19	InfoSec	CIHIghway	InfoSec News
2017-07-21	Hassan Gesso	HR Staff	ISMS and HR – What you need to know about CIHI's ISMS and your roles and responsibilities
2017-07-28	ITS Staff	All CIHI Staff	ITS Bits and Bytes
2017-09-05	InfoSec	All CIHI Staff	Information Security Awareness Month
2017-09-07	InfoSec	All CIHI Staff	Small Talk – Information Security in 2017
2017-09-11	InfoSec	All CIHI Staff	Information Security Month Series: Tailgating
2017-09-19	InfoSec	All CIHI Staff	Information Security Month – Town Halls, Phishing, closing article
2017-10-10	InfoSec	All CIHI Staff	InfoSec News Blog
2017-10-16	InfoSec	All CIHI Staff	CIHIghway article – Be on Guard – Look for the Card
2017-10-19	Information Technology Association of Canada	Hassan Gesso	Marketing & Sales Think Tank – ROI with fewer marketing resources
2017-11-16	Mike Smit	ITS Branch	IT IS Branch Retreat – presentation on "moving to the cloud"
2017-11-29	GovSec	Hassan Gesso, JL Guertin, Rene Romard	GovSec
2017-12-04		Hassan Gesso	PHIPA Conference
2018-01-08	InfoSec	All CIHI Staff	Privacy Awareness Month Campaign
2018-01-11	Cal Marcoux	ITSPD Branch	Cloud 2021
2018-01-15	InfoSec	All CIHI Staff	Privacy Awareness Month – article on international privacy
2018-01-26	Internal	All CIH Staff	Cloud 101 Primer for Staff
2018-01-29	Internal	All CIHI Staff	Privacy Awareness Month – Data privacy day in Canada

2018-01-29	Internal	All CIHI Staff	Netflix and Phishing Scam
2018-02-13	HTCIA	Hassan Gesso, JL Guertin	Virtual Crypto monetary systems - Forensic Tools, Techniques and Investigations
2018-02-22	Canadian Summit on Healthcare Cyber Security	Hassan Gesso, Cal Marcoux	Current State of Cyber Security in Canada's Health Sector
2018-03-08	Corbin Kerr, Brent Diverty	Board of Directors	CIHI – Beyond 2021
2018-03-19	Hassan Gesso, Satish Nair	CDSQ Branch	CIHI and the Cloud Presentation
2018-03-29	Gartner	DL-ISTS	State of Cloud Security
2018-04-18	David O'Toole	All CIHI Staff	Employee Information Session – Review of Cloud Technology
2018-04-15	RSA	Hassan Gesso	RSA Conference – Where the world talks security
2018-05-22	Hassan Gesso, JL Guertin, Rene Romard	CIHI Finance Branch	Finance presentation
2018-05-22	IAPP	Cal Marcoux	IAPP Canada Privacy Symposium 2018
2018-06-12	iTech Conference Ottawa	Hassan Gesso, JL Guertin, Rene Romard	Infrastructure, Cloud, Security, Data Centre Virtualization, Networking and Communications
2018-06-14	Association of Enterprise Architects (AEA) and ISACA	Hassan Gesso	ISACA/AEA - Professional Development Day and Annual General Meeting
2018-07-25	BSi	Hassan Gesso, Cal Marcoux, Jeff Levesque	Managing Opportunities and Risks in Information Security Workshop
2018-07-17	Cal Marcoux	CIHI Management	CBC news article about home care data being held for ransom
2018-08-29	InfoSec	All CIHI Staff	Security Awareness Month Small Talk

2018-09-04	InfoSec	All CIHI Staff	Information Security Awareness Month Opening Article
2018-09-10	InfoSec	All CIHI Staff	Information Security Awareness Month: What is risk management?
2018-09-12	Stefany Singh	ITSM	Overview of Digital Strategy
2018-11-30	Internal	All CIHI Staff	Security breach at Marriott Hotels
2018-12-11	Fifalde Consulting Inc.	Hassan Gesso	COBIT 5 - Business Framework for the Governance and Management of Enterprise IT
2019-01-07	Internal	All CIHI Staff	Privacy Awareness Month
2019-03-21	Service Desk	All CIHI Staff	Microsoft 365 Outlook Online Migration
2019-05-02	Stephen Wallis	Mary Ledoux, Hassan Gesso and other attendees	Presentation given on Privacy and Security by design fundamentals and BSA's in PSbD at CIHI
2019-05-15	Nsec	Hassan Gesso	NorthSec 2019 Conference
2019-06-19	InfoSec	InfoSec	Boss of the SOC conference
2019-09-03	InfoSec	All CIHI Staff	Information Security Awareness Month – Opening Article
2019-09-09	Corporate Administration	All CIHI Staff	Information Security Awareness Month – Article 2 on Physical Security
2019-09-10	InfoSec	All CIHI Staff	Information Security Awareness Month - Small Talk on Home and Personal Security
2019-09-11	InfoSec	All CIHI Staff	Information Security Awareness Month – Town Hall in Toronto Office
2019-09-16	Client Engagement & Support	All CIHI Staff	Information Security Awareness Month – Article 3 on Access Management
2019-09-17	InfoSec	All CIHI Staff	Information Security Awareness Month – Town Hall in Ottawa Office
2019-09-19	Client Engagement & Support	All CIHI Staff	Information Security Awareness Month - Small Talk on Access Management
2019-09-23	InfoSec	All CIHI Staff	Information Security Awareness Month – Article 4 on Account Access and Non-repudiation

2019-09-30	InfoSec	All CIHI Staff	Information Security Awareness Month – Article 5 on Data Hoarders/Access Removal
2019-10-07	InfoSec	All CIHI Staff	Information Security Awareness Month – Article 5 Closing Article

Affidavit of David O'Toole, President and CEO of the Canadian Institute for Health Information (CIHI)

I, David O'Toole of Ottawa, in the Province of Ontario, MAKE OATH AND SAY:

1. I am the President and CEO of the Canadian Institute for Health Information (CIHI).

2. As CIHI's President and CEO, I have formally delegated the supervision and management of day-to-day operations of the privacy portfolio to Rhonda Wing, Chief Privacy Officer and General Counsel, and have also formally delegated the supervision and management of day-to-day operations of the IT security portfolio to Cal Marcoux, Chief Information Security Officer.

3. CIHI 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. CIHI is submitting a written report (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 y the Information and Privacy Commissioner of Ontario on April 19, 2010.

5. I have made due inquiries of Rhonda Wing, Chief Privacy Officer and General Counsel and Cal Marcoux, Chief Information Security Officer, regarding (i) the contents of the Privacy and Security Policies implemented by CIHI, (ii) the *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities* and (iii) the Report.

6. Based on my knowledge, having exercised reasonable diligence, the Report describes the Privacy and Security Policies implemented by CIHI in an accurate and complete manner as of the date on which the Report is submitted.

7. Based on my knowledge, having exercised reasonable diligence, CIHI has taken steps that are reasonable in the circumstances to: (i) ensure the Privacy and Security Policies implemented comply with the Manual as set out in the Report; (ii) ensure compliance with the Privacy and Security Policies implemented; and (iii) protect personal health information against theft, loss, unauthorized use, disclosure, unauthorized copying, modification or disposal.

SWORN (OR AFFIRMED) BEFORE ME)
)
at the City of Ottawa, in the)
)
Regional Municipality of Ottawa-Carleton,)
)
in the Province of Ontario,)
)
on 28th October 2019.)

Rhonda Wing
Commissioner for Taking Affidavits

)

[SIGNATURE OF DEPONENT]