CIHI
ICIS

Canadian Institute
for Health Information

Institut canadien
d'information sur la santé

CIHI Submission:
2017 Prescribed Entity Review

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 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 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) or 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 Commissioner, CIHI had its status renewed on October 31, 2008. While the Commissioner was 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 Commissioner 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 Commissioner'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 continued to be 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:

- That CIHI ensure that a review of its policies and procedures is conducted, at a minimum, on an annual basis, as required by the *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities*.

- That CIHI include a mechanism in the tracking of their security incidents and breaches for the categorization of breaches of policy separately from breaches of data, which will enhance the accuracy and clarity of the reporting of information security breaches to the IPC in the next report.

At the time of submission of the final report to the IPC/ON in September 2014, CIHI had already put in place the necessary processes to ensure that the required annual review of policies and procedures would take place and that the tracking of security incidents and breaches reflects the requested categorization.

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 Information and Privacy Commissioner of Ontario every three years. Subsection 45(4) of the Act also requires that such approvals are required 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 Information and Privacy Commissioner of Ontario prepared the *Manual For the Review and Approval of Prescribed Persons and Prescribed Entities* (the IPC 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 2014 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 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 (employees[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 to ensure compliance with CIHI's *Code of Business Conduct*.

CIHI implemented in 2010 a *Code of Business Conduct* that 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 (employees) 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 (employees) are responsible to report actual, potential or suspected violations of the Code of Conduct to their immediate supervisor/manager. Agents (employees), 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 (employee) 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

[1] For purposes of this report and review, the term "agent (employee)" has been 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.

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,
- 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.

Pursuant to a general note to all Prescribed Persons and Prescribed Entities issued with the October 31, 2014 letter of approval, for the 2017 review, the IPC/ON requires that the report, especially with regard to the Indicators, cover the period from November 1, 2013 up to and including October 31, 2016. 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, 17 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, 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. In order to be a 'prescribed entity,' CIHI must have policies, practices and procedures to protect the privacy of individuals whose information it receives and to maintain the confidentiality of the information. The policies, practices and procedures are subject to review by the Information and Privacy Commissioner of Ontario every three years; this report forms part of that review process.

CIHI's *Privacy and Security Framework, 2010*, sets out CIHI's status as a prescribed entity under section 45 of the Act. The Framework describes how CIHI has implemented policies, procedures and practices to protect privacy and the confidentiality of the information it receives and for ongoing review of these privacy policies, procedures and practices.

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 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 structures 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 (employees). More specifically, CIHI policies, procedures and practices ensure that its agents (employees) 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.

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. 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

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. CIHI does not use personal health information for research purposes as contemplated by paragraph 37(1)(j) of the Act.

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. It further permits 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(4) 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.

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. 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.

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 disposition. 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 *Information 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, 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. 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 Information and Privacy Commissioner of Ontario, 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 their jurisdiction in which the person making the complainant resides to submit a complaint. A link to contact information for the Information and Privacy Commissioner/Ontario as well as all other provincial/territorial privacy oversight bodies in Canada will be included.

Transparency of Practices in Respect of Personal Health Information

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 to coordinate the review of all privacy and security policies respectively. The review will take place at least yearly. 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 were revised in October 2012 to include responsibility for the annual review of CIHI's privacy policies and protocols and to recommend changes as needed. An annual 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 Information and Privacy Commissioner of Ontario 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.

CIHI will communicate all updates or changes by ensuring that all 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.

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 generally the information 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. As such, CIHI makes the Framework and its privacy and security policies, including the *Privacy Policy, 2010*, accessible to the public through its external website (www.cihi.ca). Other documentation is also available publicly such as CIHI's *Privacy and Confidentiality* brochure, documentation related to the review by the Information and Privacy Commissioner of Ontario of the policies, procedures and practices implemented by CIHI to protect the privacy of individuals whose personal health information is received and to maintain the confidentiality of that information and a list of the data holdings of personal health information maintained by CIHI. Included in this material is the name and/or title, mailing address and contact information of the Chief Privacy Officer to whom inquiries, concerns or complaints regarding compliance with the privacy policies, procedures and practices implemented and regarding compliance with the Act and its Regulation may be directed. The *Privacy and Confidentiality* brochure describes in general terms how CIHI respects personal privacy, collects and uses health information, limits disclosure of information, and safeguards personal information.

In addition, CIHI's *Privacy Impact Assessment Policy* requires that, once approved, the CPO makes 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*, identifies 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.

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.

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 is 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*.

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 is 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.. 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, 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). CIHI recently developed a new tool whereby 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 to review annually any existing PIAs for discrepancies between their content and actual practices or processes, and to advise the CPO, and together determine if an update or a new PIA is required.

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*.

Use of Personal Health Information

8. Policy and Procedures for Limiting Agent (Employee) 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 (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).

Moreover, 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 (employees) 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 (employees), 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 (employees) 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.

Review and Approval

Analysis at CIHI is generally conducted with the use of record-level data, where the health card number has been removed or encrypted. In exceptional instances, Program Area staff will require access to original health card numbers. 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 10.14 of CIHI's *Privacy Policy Procedures*.

Specifically:

- Where ITS staff require ongoing access to original health card numbers in order to perform their duties and/or services, approval from their ITS Manager is required.
- Where non-ITS staff (that is, Program Area staff) require access to original health card numbers to fulfill an operational activity such as data processing, data quality or error correction, systems development work or testing, returns of own data or disclosures under data-sharing agreements, approval from the program area Director is required.
- For any staff requiring access to original health card numbers for analytical activities, approval from CIHI's Privacy, Confidentiality and Security Committee is required.

Tracking Approved Access to and Use of Personal Health Information

Once approved, access requests are documented and forwarded to Information Technology and Services (ITS), whose responsibility it is to log and track access requests, grant agents (employees) 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 internal data access audit.

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

Secure Retention and Destruction of Accessed/Used Records

When access is approved, files 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 disposition. 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 Information and Privacy Commissioner of Ontario.

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

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

- Name of agent (employee);
- Data holdings to which access and use was granted;
- Level or type of access and use;
- The date access and use was granted; and
- The termination date or the date of the next audit of access and use.

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

The following sections deal with disclosures of data by CIHI broken-down along the following lines:

- Disclosures of personal health information for purposes other than research; and
- Disclosures of personal health information for research purposes.

Section 37 of CIHI's *Privacy Policy, 2010*, states very generally that all disclosures must be consistent with CIHI's mandate. It reads as follows:

> *37. 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.*
>
> *These disclosures typically fall into one of four categories:*
>
> *(a) Disclosures to parties with responsibility for the planning and management of the health care system to enable them to fulfill those functions;*
>
> *(b) Disclosures to parties with a decision-making role regarding health care system policy to facilitate their work;*
>
> *(c) Disclosures to parties with responsibility for population health research and/or analysis; and*
>
> *(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.*

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

CIHI has adopted a uniform approach to the protection of personal health information for both disclosures for research purposes under section 44 of PHIPA and disclosures for purposes of planning and management of the health system under section 45.

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 PHIPA. 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 Information and Privacy Commissioner of Ontario's requirements as set out in the IPC 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 Submission Guidelines*.

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 case 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.

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

Not applicable.

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

Section 40 of CIHI's *Privacy Policy, 2010*, stated above, also governs the disclosure of personal health information for research purposes. 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 the IPC 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 the Research Plan comply with the requirements of the Act and its Regulation?
- Does the Research Plan set out the affiliation of each person involved in the research?
- Does it set out the nature and objectives of the research and the public or scientific benefit of the research that the researcher anticipates?
- Has the Research Plan been approved by a research ethics board?
- Does CIHI have a copy of the decision of the research ethics board, approving the Research Plan?
- Is the information requested consistent with the information identified in the Research Plan approved by the research ethics board?
- Can other, de-identified and/or aggregate information serve the research purpose?
- Is more personal health information being requested than is reasonably necessary to meet the research purpose?
- Does the Research Plan contain a retention period for the personal health information records?

All disclosures of personal health information for research purposes must be reviewed and approved by CIHI's Privacy, Confidentiality and Security Committee, in writing.

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 – https://www.cihi.ca/en/access-data-and-reports/make-a-data-request

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.

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 recipients of third-party 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.

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

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.

All elements listed in the IPC 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 are contained in CIHI's Template 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 Research Agreements (at CIHI, these are referred to as Data Protection Agreements in the case of disclosures of personal health information and Non-Disclosure/Confidentiality Agreements in the case of disclosures of de-identified 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 Research 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 Research 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 Research Agreement;
- The date by which the records of personal health information must be securely destroyed; and
- The certificate of destruction.

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 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 41.1 and 41.2 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.

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.

17. Template Data Sharing Agreement

All elements listed in the IPC Manual, namely, all items in the General Provisions, Purposes of Collection, Use and Disclosure, Secure Transfer, Secure Retention, Secure Return or Disposal, Notification, and Consequences of a Breach and Monitoring Compliance are contained in the following CIHI 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.

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 Policy* sets the guidelines that govern the acquisition of all goods and services by CIHI in meeting its goals and objectives. CIHI has developed template agreements for the acquisition of goods and services pertaining to personal health information. These templates include the CIHI Services Agreement, a Master Services Agreement and a Services Agreement template to be 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 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.

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 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 will maintain 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 has converted its manual off-boarding process for external professional services staff hired under Service Provider Agreements to an automated task-based process in its business process management workflow tool. An advance notice email is sent to the relevant Program Manager five working days in advance of the last day of work of the external professional services staff member with 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. Secure destruction of confidential information, including personal health information, requires prior approval from the Chief Information Security Officer or the Chief Privacy Officer, and the requirement for a Certificate of Destruction to 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.

Twenty-four hours in advance of the last day of work, the business process management workflow tool issues a task to the relevant Program Manager to complete the automated off-boarding process. 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, 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 Manager is to contact the Chief Privacy Officer/General Counsel.

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.

CIHI's template agreements, that is the CIHI Services Agreement, Master Services Agreement and the Services Agreement template to be used for contractors providing secure retention and destruction services only, contain all elements listed at pages 51 to 57 in the IPC Manual, namely, all items in the General Provisions, Obligations with Respect to Access and Use, Obligations with Respect to Disclosure, Secure Transfer, Secure Retention, Secure Return or Disposal following Termination of the Agreement, Secure Disposal as a Contracted Service, Implementation Safeguards, Training of Employees of the Third Party Service Provider, Subcontracting of Services, Notification, Consequences of Breach and Monitoring Compliance and are, therefore, consistent with the requirements for the *Template Agreement for all Third Party Service Providers*.

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 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.

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, and the requirement for a Certificate of Destruction to 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

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. More specifically, data linkage for CIHI purposes is addressed in sections 18 and 19 of the *Policy*, and data linkage by or on behalf of third parties is addressed in sections 20 and 21.

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.

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*.

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 consistently encrypted health card numbers or through the use of the Client Linkage Index or other comparable methodologies as may be developed from time to time. 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.

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 disposition. 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.

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

Data De-identification

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 digits (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 (employees) 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.

Privacy Impact Assessments

25. Privacy Impact Assessment Policy and Procedures

Over the years, CIHI has developed 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 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 its *Privacy Impact Assessment Policy*, Directors in the Program Areas are responsible to review Privacy Impact Assessments annually for discrepancies between their content and actual practices or processes, and to advise the CPO, and together they will determine if an update or a new PIA is required. As part of the annual review of its privacy policies, CIHI amended the *Privacy Impact Assessment Policy* in 2012 to extend the standard renewal period for existing PIAs from three years to five years. This change was deemed to be relatively low risk, since the Policy still 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 was further amended in 2014 to require 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) (employee(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.

26. Log of Privacy Impact Assessments

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) (employee(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) (employee(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 Program, CIHI carries out three types of reviews to monitor and ensure privacy compliance:

1. *CIHI Program Area Audits* **–** These audits assess the Program Area's compliance with CIHI's privacy policies and privacy best practices. The audits help identify actual or potential privacy vulnerabilities and gaps in CIHI's policies. It is important to note that these audits perform a remedial function by including recommendations to address any issues identified and to mitigate risks.
2. *CIHI Topic Audits* **–** These audits are narrower in scope and focus on how a particular issue applies across the organization. Priority for topic audits is given to sensitive, visible, or high risk activities. These audits also perform a remedial function by identifying gaps in CIHI's policies, and actual or potential vulnerabilities.
3. *Data Recipient (external client) Audits* – These audits focus on external recipients of CIHI's data. They evaluate a recipient's use and management of the data, as well as the recipient's disclosure of research findings associated with the data. Specifically, the audits evaluate whether the recipient's activities comply with CIHI's Data Request Form and Non-Disclosure/Confidentiality Agreement or other legally-binding instrument as the case may be such as Data Sharing Agreements.

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 Information and Privacy Commissioner of Ontario.

In addition to the above, the Terms of Reference for CIHI's Privacy Audit 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 schedule 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 every June.

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 program area or topic audits
- The agent(s) (employee(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., Program Audit, Topic Audit, External Data Recipient Audit)
- The status of the audit and subsequently, the date the audit was completed
- The agents(s) (employee(s)) responsible for completing the audit.

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 program area or topic audits
- The agent(s) (employee(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.

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. The Protocol makes it mandatory for CIHI agents (employees) to immediately report all privacy and security breaches or incidents. To make it easy for agents (employees) to do so, CIHI has established a centralized mailbox (Incident@cihi.ca) to which agents (employees) 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.

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

An **information security breach** is any occurrence that impacts or may impact the confidentiality, integrity or availability of CIHI's electronic information assets, or that compromises or may compromise CIHI's information security controls.

A **privacy breach** is any occurrence in which personal health information in CIHI's custody or control is accessed, used, disclosed or disposed of in any unauthorized fashion.

Having protocols in place allows CIHI to respond quickly and in a coordinated manner in the event of a security incident or privacy breach, and ensures responsibilities are clear.

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; or
- May result in unauthorized use, access, copying, modification, disclosure or disposal of CIHI's information assets.

When reporting incidents and breaches to incident@cihi.ca, the Protocol reminds agents (employees) to include the following information: when the incident was discovered; how it was discovered; its location, its cause (if known); the individual 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,

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 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 Breach. The President and CEO, in consultation with the Incident Response

Team, determines whether a privacy 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 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.

Major privacy breaches will be reported to the Governance and Privacy Committee of CIHI's Board of Directors and ultimately to the overall CIHI Board of Directors.

The Incident Response Team is responsible for 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.

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.

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) (employee(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) (employee(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. Inquiries, concerns or complaints related to the privacy policies, procedures and practices implemented by CIHI 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.

The *Privacy Policy Procedures* related to section 64 of CIHI's *Privacy Policy, 2010*, establish the process that CIHI follows in receiving privacy complaints. They are as follows:

64.1 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.

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

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

64.4 Where required, the Chief Privacy Officer or designate will contact the individual to:
  i. Clarify the nature and extent of the inquiry or complaint; and
  ii. 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.

64.5 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.

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 Information and Privacy Commissioner of Ontario.

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 disposition;
  - 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.

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

CIHI’s information security document management procedures require the yearly review of its security policies, standards, guidelines, protocols and procedures in order to determine whether any amendments or additional documents are needed. Document Owners are responsible for managing all reviews. CIHI has implemented an automated notification system where Document Owners receive a document review task 11 months after the most recent review date.

The 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;
- 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. CIHI ensures 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 as well as all related metadata – security classification, version, release date, last review date, next review date, document status, document owner, designated approval authority and designated consultation authorities – consolidated in its Information Security Library, under the Chief Information Security Officer.

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.

CIHI has controlled access to its premises through a photographic card access system together with a personal identification number. CIHI agents (employees) 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 either with surveillance cameras at various points of entry or controlled by security guards who are on duty twenty-four hours a day. Further restrictions are imposed within CIHI premises to its server rooms/data centres where personal health information in stored in electronic format to ensure access is only provided to agents (employees) who routinely require such access for their employment, contractual or other responsibilities.

Policy, Procedures and Practices with Respect to Access by Agents (Employees)

The Manager of the Corporate Administration Department is responsible for granting and revoking building access. Departmental managers are responsible for requesting and authorizing access for their agents (employees), including long-term consultants and students. Full access (24/7) to CIHI offices is granted to CIHI agents (employees), long-term consultants and students. Short-term consultants (less than three months) are issued security access cards with restricted access (6 a.m. to 6 p.m., Monday to Friday in Toronto and 7 a.m. to 7 p.m. in Ottawa) unless otherwise requested/authorized in writing by the Manager or Director.

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 4:15 p.m. will be provided with a temporary 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.

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. Agents (employees) who have lost their security access card must notify the Corporate Administration Department immediately. The Office Administrator in Corporate Administration will request a new security access card for the agent (employee) using the "Request for Security Card Access" form. The lost security access card is deactivated immediately upon receipt of the notification.

Termination of the Employment, Contractual or Other Relationship

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 (employee) 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 (employee'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 (employee) 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 (employees) and long-term consultants are programmed to deactivate on the last day of the employment or contractual arrangement with CIHI.

Audits of Agents (Employees) with Access to the Premises

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

1. A bi-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 (employees) granted access continue to have an employment, contractual or other relationship with CIHI and continue to require the same

level of access ; and

2. Annually, every January, as part of the “January is Privacy Awareness Month at CIHI” campaign, a visual verification is carried out by the Corporate Administration Department to ensure that agents (employees) 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 (employees) granted approval to access CIHI premises and for all documentation related to the receipt, review, approval and termination of such access.

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 (employee) whom they are meeting
- Wear a CIHI Guest ID card at all times on the premises
- Be escorted by a CIHI agent (employee) 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 (employee) 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 (employee) is responsible for signing-out the visitor and for return of the Guest ID Card.

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

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

- The name of the agent (employee) granted approval to access the premises;
- The name of the agent (employee) 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 (employee);

- 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. This occurs as part of the “January is Privacy Awareness Month at CIHI” campaign.

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. 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 Agreement for All Third Party Service Providers* described at Part 1, section 20.

CIHI’s *Secure Information Transfer Standard* provides that records are transferred and retrieved in a documented and secure manner. The requirements for secure transfer are detailed in

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

section 7, below. Infrastructure 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.

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 Confidential Information is protected and retained only on authorized CIHI computing devices/media and in authorized locations; and
- that Confidential Information temporarily stored on CIHI's mobile devices and removable media is secured in the event of theft or loss and is protected against unauthorized use, access, copying, modification, disclosure or disposal.

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* and related *Procedures for Approval to Store Confidential Information on Mobile Devices/Removable Media* are 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 Information and Privacy Commissioner of Ontario 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 (employees) 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 (employees) to notify CIHI at the first reasonable opportunity in accordance with the *Privacy and Security Incident Management Protocol*, if an agent (employee) 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) (employee(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) (employees(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*;

[2] See "Protecting Personal Information Outside the Office", February 2005, Office of the Information and Privacy Commissioner for British Columbia

- 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 ensure appropriate safeguards such as encryption for mobile computing devices. In Order HO-004, for example, the Information and Privacy Commissioner 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 (employees) is to be done on CIHI premises, using CIHI-issued computing devices/media and/or over its secure networks 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; and
- Shall not be stored on mobile devices or removable media except for specific and exceptional circumstances such as re-abstraction studies, where prior approval has been given by the relevant Vice-President. The requirements set out in the "*Procedures for Approval to Store Confidential Information on Mobile Devices/Removable Media*" must be met.

[3] Information and Privacy Commissioner/Ontario, Order HO-004, March 2007 at page 20

Approval Process

Prior approval is required by a Vice-President before personal health information can be temporarily stored on mobile devices/removable media. A formal approval process has been established whereby the Program Area requesting approval must complete a form for review by the Vice-President, who will then determine whether to approve or deny the request based on the information provided. The Chief Privacy Officer must be notified of the approval and provided with an itemized list of the personal health information that will be stored on the mobile device / removable media.

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* and related *Procedures for Approval to Store Confidential Information on Mobile Devices/Removable Media* set 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.
3. Personal health information temporarily stored on mobile devices and removable media will be:
    a. done on CIHI issued equipment;
    b. de-identified to the fullest extent possible; and
    c. encrypted and password protected in keeping with CIHI's current encryption standards.

In accordance with the *Policy on the Security of Confidential Information and Use of Mobile Devices/Removable Media* and related *Procedures for Approval to Store Confidential Information on Mobile Devices/Removable Media*, Infrastructure Services is 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 username and password standard.

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. Written confirmation by both the Manager of the Program Area that originally requested approval and the ITS Manager that the personal health information has been removed from the mobile device / removable media must be documented, including the date of destruction. A copy of the completed form indicating such must be sent to the Vice-President who approved the request for removal, and to the Chief Privacy Officer. All approved requests are documented and tracked by Privacy and Legal Services to ensure secure destruction of the personal health information on mobile devices /removable media occurs.

Remote Network Access

CIHI's workforce is made up of agents (employees) 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 (employees) 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 (employees) 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;
- The user must ensure any data residing on the device is copied to CIHI's secure network server prior to returning the device.

Additionally, all laptop and desktop computers 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 Information and Privacy Commissioner of Ontario under the Act and its regulation.

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 (employees) performing the transfer of personal health information must document the following:
  - Date and method of transfer;
  - Recipient;
  - Nature of the records; and
  - Confirmation of receipt.

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

As of April 2015, 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.

8. Policy and Procedures for Secure Destruction 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 Office of the Information and Privacy Commissioner of Ontario.

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 shredding bins and electronic media must be stored in one of CIHI's computing centers 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 to ensure 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 (Employee), 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 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 (employee) 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 which is based on CIHI's *Secure Destruction Standard*. Paper records destined for destruction are stored in locked bins available to staff throughout the premises. The third party securely destroys these documents on-site and provides a certificate of destruction to CIHI on a monthly basis. 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 (employee(s)) who performed the secure destruction.

Where a third party service provider does not provide the certificate of destruction within the required timeframe, the Corporate Administration Department follows up to ensure the certificate is provided. In instances of data destruction by third-party data requester, 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 in accordance with the *Template Agreement for All Third Party Service Providers* and a certificate of destruction is provided. In cases where the third party performs the destruction off-site, media is first degaussed by CIHI in accordance with the *Secure Destruction Standard*.

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. It's *Username and Password Standard* governs the passwords used for both authentication and access to information systems whether they are owned, leased or operated by CIHI. The *Standard* has been developed with regard to and is consistent with orders, fact sheets, guidelines and best practices issued by the Information and Privacy Commissioner of Ontario and also with regard to current best practices.

The *Standard* lays out the requirements of CIHI's default password schema which includes, for example, passwords of a minimum length and containing characters from at least three different categories. The Standard also establishes 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 Standard where technology permits.   The *Username and Password Standard* imposes 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 *Standard* mandates the following administrative, technical and physical safeguards to be implemented by agents (employees):

- Passwords may not be written down;
- Passwords may not be shared with anyone under any circumstances – and agents (employees) 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.

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* and related documents address the requirements set out in the *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities*:

- Date and time PHI is accessed;
- Date, time and nature of the disconnection;
- Agent(s) (employees(s)) responsible for reviewing system control and audit logs are to notify CIHI at the first reasonable opportunity of a privacy breach or suspected privacy breach in accordance with the *Privacy and Security Incident Management Protocol*;
- Identification of agent(s) (employees(s) responsible for assigning other agent(s) (employee(s)) to address the findings, establishing timelines to address the findings, for addressing the findings and for monitoring and ensuring that the findings have been addressed;
- Requires agents (employees) to comply with the policy and its procedures, addresses how and by whom compliance will be enforce and the consequences of breach;
- Requires agents (employees) to notify CIHI at the first reasonable opportunity, in accordance with the *Privacy and Security Incident Management Protocol*, if an agent (employee) believes there may have been a breach.

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

CIHI audits compliance with its security policies in accordance with its ISMS Audit Program as described in Part 2, section 15 of this document.

Specifically, 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 (employees) with access to personal health information and with the threats and risks associated with the personal health information. The Policy and related documents require the following:

- All information systems, technologies, applications and programs involving personal health information have the functionality to log access, use, modification and disclosure of personal health information;
- The types of events that are required to be audited and the nature and scope of the information that must be contained in system control and audit logs including:
  - date and time that personal health information is accessed;
  - the name of the user access personal health information;
  - the network name or identification of the computer through which the connection is made;
  - the nature of the event - the operations or actions that create, amend, delete or retrieve personal health information including the nature of the operation or action,

the date and time of the operation or action, the name of the user that performed the action or operation and the changes to values, if any.

- Identification of the agent (employee) responsible for ensuring that the types of events that are required to be audited are audited and that the nature and scope of the information that is required to be contained in system control and audit logs is logged;
- System control and audit logs are immutable – procedures and agent (employee) responsible identified;
- The length of time that system control and audit logs are required to be retained, the agent (employee) responsible for retaining the system control and audit logs and where the system control and audit logs will be retained;

Audit logs are 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. In the case of incident management, all such activities and documentation requirements are set out in CIHI's *Privacy and Security Incident Management Protocol*.

11. Policy and Procedures for Patch Management

CIHI's 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 (employee) 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 maintained.

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.

12. Policy and Procedures Related to Change Management

CIHI's *Global Process Policies for Change Management* 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 RFC and communicated to the requestor via the IT Service Management Tool. The impact of, the urgency and the rational 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 (employee) who requested the change;
- The date the change was implemented;

- The agent (employee) responsible for implementing the change;
- The date, if any, the change was tested;
- The agent (employee) who tested the change, if any; and
- Whether the testing was successful.

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

CIHI's 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 back-up and recovery procedures are tested on a weekly basis through operational requests for restoration of data. In addition, back-up and recovery procedures are tested randomly by automated software, at a minimum every quarter.

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 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 Services is responsible for auditing backup tape validity and integrity on an ongoing basis.

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.

14. Policy and Procedures on the Acceptable Use of Technology

Privacy
and Security
September is Information Security Awareness Month at CIHI
Information security is everyone's responsibility. Here are some examples of what you need to know:
Do
Keep passwords confidential—don't share them with anyone.
Lock your work station when away from your office.
Report the loss or theft of any CIHI computing equipment or storage device to the Senior Program Consultant, Security.
Don't
Install any software on any CIHI computing device.
Use the Internet for games.
Connect any removable storage device to any computing device unless authorized.
Act responsibly—follow the privacy and security practices on the intranet.
Canadian Institute for Health Information
Institut canadien d'information sur la santé

A key underpinning of CIHI's privacy and security program is CIHI's *Acceptable Use of Information Systems Policy*. It outlines for all agents (employees) 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 (employees) 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 (employees) 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.

Security Audit Program

15. Policy and Procedures in Respect of Security Audits

CIHI's ISMS Audit program 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
    - Assess the security posture of CIHI's technology and application infrastructure
- 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.

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 Team headed by the President and Chief Executive Officer, 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.

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.

16. Log of Security Audits

CIHI's Senior Program Consultant, 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) (employee(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) (employee(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

Not applicable – to date, CIHI has not experienced any information security breaches. Should an information security breach occur, the Chief Information Security Officer would ensure a log was 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) (employee(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) (employee(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

January is
Privacy Awareness Month
Take the mandatory training and renew your employee confidentiality agreement >>

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 (employees) 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 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 (employees) on their first day of employment. The mandatory privacy and security training is referenced and explained within this session and agents (employees) 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 (employee) 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 (employees) 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 (employees);
- The procedure that must be followed in the event that an agent (employee) 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 (employees) 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 (employees) 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 (employees) 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.

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 to confirm 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 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);
- InfoSec Newsletter;
- 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.

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' (employees') mandatory privacy and security training.

Confidentiality Agreement

3. Policy and Procedures for the Execution of Confidentiality Agreements by Agents (Employees)

CIHI requires all agents (employees) 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. One hundred per cent completion is required and is ensured by monitoring and direct follow-up with agents (employees). Amongst other things, the renewal states that agents (employees) 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 (employees) 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 (employee). The Confidentiality Agreement is included in the employment offer package and new agents (employees) 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 (employee) file.

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

4. Template Confidentiality Agreement with Agents (Employees)

In addition to the Confidentiality Agreement used for CIHI staff referred to above, CIHI also uses template agreements for external third-party service providers to ensure confidentiality. All elements listed in the *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities*, issued by the Information and Privacy Commissioner of Ontario, 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 are contained in CIHI's template Confidentiality Agreement for third-party service providers. For example, and without limitation, key provisions include:

- A description of CIHI's status as a prescribed entity under PHIPA including its duties and responsibilities arising from this status;

- A definition of personal health information that is consistent with the definition that is contained in PHIPA;
- Requirements for service providers to comply with PHIPA and its Regulation as it relates to prescribed entities, including complying with purposes for which the service provider is permitted to collect, use and disclose personal health information on behalf of CIHI;
- Requirements that the service providers have familiarized themselves and agree to comply with CIHI's privacy and security policies and procedures;
- A duty to notify CIHI at the first reasonable opportunity in the event of a breach of the Agreement; and CIHI's unfettered right to audit the service provider, need be;
- Requirements that service providers securely return to CIHI, or securely and permanently destroy all confidential information upon termination of the relationship including records of personal health information on or before the date of termination – including also the manner in which the confidential information will be securely returned or destroyed which may vary from time to time depending on technology and Commissioner Orders.

Third-party service providers must provide CIHI with written confirmation of the secure destruction of confidential information, including personal health information and de-identified data. CIHI has developed a Certificate of Destruction based on the Commissioner's requirements, to be used where appropriate.

5. Log of Executed Confidentiality Agreements with Agents (Employees)

The log of confidentiality agreements with agents (employees) includes the name of the agent (employee), 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 (employees), in a manner at par with the requirements of the Information and Privacy Commissioner of Ontario.

Responsibility for Privacy and Security

6. 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 Information and Privacy Commissioner of Ontario, 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 (employees) are aware of the Act and its regulation and their duties thereunder;
- Ensuring agents (employees) 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.

7. 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 Information and Privacy Commissioner of Ontario, namely:

- Developing, implementing, reviewing and amending security policies, procedures and practices;
- Ensuring compliance with the security policies, procedures and practices implemented;
- Ensuring agents (employees) 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

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

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 (employee) 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 Human Resources Generalist 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 (employee) is leaving CIHI, as well as creating a Service Desk request to inform the Information Technology team of the agent's (employee's) last day in the office.

Once the Information Technology team receives the Service Request, the Senior Technical Support Specialist disables the departing agent's (employee's) account, changes the expiration date on the user account, and sends the Employee Departure Information Technology Checklist to the departing agent's (employee'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 (employee). 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 (employee's) last day. Should CIHI property not be duly returned by the departing agent (employee), 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 (employee) 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 (employee) out of the building.

Discipline

9. 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

[3] 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 (employees). This Division has a set of policies and procedures that ensure such employment-related issues within the organization are dealt with effectively.

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. It 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.

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 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 breaches and privacy complaints that were investigated, including the results, and any recommendations arising from these investigations and the status of implementation of the recommendations.

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
- Senior Management Committee
  - Chaired by the President and CEO, and comprising Executive Committee members and all Directors including the Chief Privacy Officer and the Chief Information Security Officer
- IT Operations Committee
  - 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 Senior Program Consultant, 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 (employees) 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 the appropriate Executive Committee member (Risk Champion); these are reviewed by the Finance and Audit Committee of the CIHI Board, and an update 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. The Framework requires that the corporate risk register be reviewed annually. 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 Executive 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 (employee) 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
- Privacy audits
- The investigation of privacy incidents and breaches

- The investigation of privacy complaints
- The Information and Privacy Commissioner of Ontario’s review every three years.

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

This information is subsequently fed into CIHI’s Master Log of Action Plans, is 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 them. Furthermore, each owner of the action plan 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.

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 to provide 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 Action Plans, are monitored and reported on at the corporate level.

7. Consolidated Log of Recommendations

As indicated above, a consolidated log of privacy recommendations, 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 (employee) responsible for addressing the recommendation.

Business Continuity and Disaster Recovery

8. Business Continuity and Disaster Recovery Plan

CIHI has a comprehensive and rigorous Business Continuity and Disaster Recovery Plan to ensure the continued availability of the information technology environment in general, and the personal health information holdings in particular, in the event that there is a business interruption or threats to CIHI's operating capability.

The Business Continuity and Disaster Recovery Plan covers the following key elements in detail:

- Notification of the Interruption – roles and responsibilities, the contact list, timeframes, and form of notification
- Assessment of the Severity of the Interruption – roles and responsibilities, criteria for assessment and documentation, initial impact assessment, a detailed damage assessment
- Resumption and Recovery – activation of the business continuity and disaster recovery plan, an inventory of all critical applications and business functions, procedures for recovery of every critical application and business function, prioritization of recovery activities, recovery time objectives, roles and responsibilities
- 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.

The Director, Human Resources and Administration, is responsible for ensuring that the plan is communicated to all agents (employees).

The Manager, Corporate Administration is responsible for managing all communications to agents (employees) during an interruption or threat event.

PHIPA Review – Indicators

November 1, 2013 to October 31, 2016

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 Information and Privacy Commissioner of Ontario.	- *Privacy Policy on the Collection, Use, Disclosure and Retention of Personal Health Information and De-Identified Data, 2010*, (*Privacy Policy, 2010*) approved by CIHI's Board of Directors March 2010, reviewed June 2014, June 2015 and June 2016 - Privacy Policy Procedures first adopted July 2010; reviewed March 2014, April 2015, October 2015 and June 2016 - *Privacy and Security Framework* first adopted February 2010; ongoing review to update as required; reviewed November 2014, November 2015 and September 2016 - *Privacy and Security Training Policy* first adopted September 2009 and associated Procedures first adopted November 2014; reviewed December 2013, November 2014, November 2015 - *Privacy Impact Assessment Policy* first adopted April 2009; reviewed March 2014, July 2014, July 2015 and July 2016 - *Privacy and Security Incident Management Protocol* approved January 2013; reviewed March 2014, February 2015 and March, 2016 - *Policy on the Security of Confidential Information and Use of Mobile Devices/Removable Media* and associated *Procedures for Approval to Store Confidential Information on Mobile Devices/Removable Media* approved July 2014; reviewed July 2015 and July 2016 - *Privacy and Security Risk Management Framework* first adopted July 2015; reviewed February 2017 - *Privacy and Security Risk Management Policy* first adopted July 2015; reviewed February 2017

Categories	Privacy Indicators	CIHI Indicators
		▪ *Privacy and Security Risk Management Methodology* first adopted July 2015, reviewed February 2017
	• 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 Procedures amended March 2014 – new procedures introduced for data collection; prohibition on use for purposes of re-identification and prohibition on use for research purposes; April 2015 – new procedures introduced (1) prohibiting access and use of personal health information if other levels of information will serve the identified purposes and (2) prohibiting accessing and using more personal health information than is reasonably necessary; June 2016 – minor amendments to update mandate, references and links. • *Privacy and Security Framework* being updated to reflect changes to the privacy and security program in the form of minor clarifications coming out of the November 2015 and September 2016 review • *Privacy Impact Assessment Policy* updated July 2014 to incorporate changes resulting from the 2014 PHIPA review and audit process • *Privacy and Security Incident Management Protocol* amended February 2015 to address evidence preservation; amended April 2015 adding requirement to address when independent third-party forensic experts are to be engaged; amended September 2015 to clarify definition of privacy breach; amended April 2016 to clarify when and how containment measures may occur • *Procedures for Approval to Store Confidential Information on Mobile Devices/Removable Media* amended August 2015 to update reference to the *Secure Information Transfer Standard* • *Policy on the Security of Confidential Information and Use of Mobile Devices/Removable Media* amended

Categories	Privacy Indicators	CIHI Indicators
		July 2016 to update reference to the *Secure Information Transfer Standard*
	- 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.	- *Policy on the Security of Confidential Information and Use of Mobile Devices/Removable Media* approved by Senior Management Committee July 2014 (replaces the *Privacy Policy on the Use of Mobile Computing Equipment)*. Fundamentally, the two policies are consistent. However, the purpose of the new Policy is first to ensure that confidential information is protected and retained only on authorized CIHI computing devices/media and in authorized locations. Secondly, it sets out the requirements for temporary storage of confidential information on CIHI's mobile devices and removable media. While the earlier version contained a statement about performing work on CIHI's premises using CIHI-issue computing devices and/or over its secure networks, it was not evident through the policy title and format that this was the policy where you would find such a requirement.
	- 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 (CIHiway), SmallTalks, targeted presentations and the like. To date, the following communications have been delivered: - *Privacy Policy and Procedures*– March 2014 Updated version of the Procedures and article posted on CIHiway informing staff of new procedures for collections of personal health

Categories	Privacy Indicators	CIHI Indicators
		information; prohibition on identifying or attempting to identify individuals and use of data for research purposes.: • *Privacy Impact Assessment Policy*: Revised Policy posted on CIHiway August 2014 • *Policy on the Security of Confidential Information and Use of Mobile Devices/Removable Media and related Procedures* – September 2014 Policy posted on CIHiway • *Privacy Policy and Procedures* - April 2015 Updated version of the Procedures and article posted on CIHiway informing staff of new procedures (1) prohibiting access and use of personal health information if other levels of information will serve the identified purpose and (2) prohibiting access and use of more personal health information that is reasonably necessary. • *Privacy Policy and Procedures* - October 2015 Updated Procedures and article posted on CIHiway: update to procedures resulting from implementation of the client linkage standard; requirements for Research Plans under section 44 of PHIPA and the Regulations specified; updated links to associated documents • *Privacy Policy and Procedures* – June 2016 Updated Procedures posted on CIHiway: CIHI mandate updated • *Privacy and Security Incident Management Protocol* – Revised Protocol posted on CIHiway: April 2015, May 2015, November 2015 and August 2016 • *Policy on the Security of Confidential Information and Use of Mobile Devices/Removable Media and related Procedures* – July 2016 Updated Policy posted on CIHiway

Categories	Privacy Indicators	CIHI Indicators
	▪ 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* 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*, and *Policy on the Security of Confidential Information and Use of Mobile Devices/ Removable Media* posted on CIHI's external website ▪ Information Sheet on CIHI's Privacy Audit Program for Third-Party Record-level Data Recipients posted on CIHI's external website

Categories	Privacy Indicators	CIHI Indicators
Collection	▪ The number of data holdings containing personal health information maintained by the prescribed person or prescribed entity.	▪ CIHI has17 data holdings containing personal health information
	▪ The number of statements of purpose developed for data holdings containing personal health information.	▪ Statements of purpose for all 17 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 Information and Privacy Commissioner of Ontario.	▪ Since November 2013, CIHI has updated or published10 new PIAs for data holdings containing personal health information, as well as two addenda – see Privacy Impact Assessment Log for list of new or updated Statements of Purpose (pages 117-118 of this Report)
	▪ 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, 2016, 39 agents (employees) have approval to access and use personal health information at CIHI. CIHI does not use personal health information for research purposes.
	• 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
	• 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 Information and Privacy Commissioner of Ontario.	• None
Disclosure	• The number of requests received for the disclosure of personal health information for purposes other than research since the prior review by the Information and Privacy Commissioner of Ontario.	• Four

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 Information and Privacy Commissioner of Ontario.	- Four
	- The number of requests received for the disclosure of personal health information for research purposes since the prior review by the Information and Privacy Commissioner of Ontario.	- Eight – four consent-based and four based on section 44 of PHIPA
	- 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 Information and Privacy Commissioner of Ontario.	- Six granted - Two in review process
	- The number of Research Agreements executed with researchers to whom personal health information was disclosed since the prior review by the Information and Privacy Commissioner of Ontario.	- Five (Note: one request for the disclosure of personal health information was abandoned by the requester prior to the execution of a research agreement.)
	- 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 Information and Privacy Commissioner of Ontario.	- 2013-14: (Q3 – Q4) 144[1] - 2014-15: (Q1 – Q4) 429[1] - 2015-16: (Q1 – Q4) 447[1] - 2016-17: (Q1 – Q2) 193[1]
	- 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 Information and Privacy Commissioner of Ontario.	- 2013-14: (Q3 – Q4) 144[1] - 2014-15: (Q1 – Q4) 429[1] - 2015-16: (Q1 – Q4) 447[1] - 2016-17: (Q1 – Q2) 193[1]
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 Information and Privacy Commissioner of Ontario.	- Three
	- 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 Information and Privacy Commissioner of Ontario.	- None

Categories	Privacy Indicators	CIHI Indicators
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 Information and Privacy Commissioner of Ontario.	▪ 90[1]
Data Linkage	▪ The number and a list of data linkages approved since the prior review by the Information and Privacy Commissioner of Ontario.	▪ 93 linkages ▪ See attached log of *Approved Data Linkages* which can be found at pages 107-116 of this Report
Privacy Impact Assessments	▪ The number and a list of privacy impact assessments completed since the prior review by the Information and Privacy Commissioner of Ontario 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, 2013, ten Privacy Impact Assessments have been completed and two addenda ▪ See attached *Privacy Impact Assessment Log* (pages 117-118 of this Report) and *Summary of Recommendations* (pages 119-123 of this Report) ▪ A total of 10 recommendations were identified (see pages 119-123 of this Report)
	▪ The number and a list of privacy impact assessments undertaken but not completed since the prior review by the Information and Privacy Commissioner and the proposed date of completion.	See attached *Privacy Impact Assessment Log* (pages 117-118 of this Report)
	▪ 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 Information and Privacy Commissioner of Ontario 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 Information and Privacy Commissioner and a brief description of any amendments made.	10 privacy impact assessments since November 1, 2013 See attached *Privacy Impact Assessment Log* (pages 117-118 of this Report)

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 Information and Privacy Commissioner of Ontario 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 (page 135 of this Report)
	• The number and a list of all other privacy audits completed since the prior review by the Information and Privacy Commissioner of Ontario and for each audit: – 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, 2013, CIHI has completed two privacy audits with two audits in progress ▪ See attached *CIHI's Privacy Audit Program* (pages 124 to 129 of this Report)
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 Information and Privacy Commissioner of Ontario.	▪ Ontario - None All other jurisdictions – two
	▪ 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, – The date(s) that the containment measures were implemented,	▪ N/A

Categories	Privacy Indicators	CIHI Indicators
	– 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 Information and Privacy Commissioner of Ontario.	▪ Ontario – None ▪ All other jurisdictions – None
	▪ Of the privacy complaints received, the number of privacy complaints investigated since the prior review by the Information and Privacy Commissioner of Ontario 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 Information and Privacy Commissioner of Ontario and with respect to each privacy complaint not investigated: – The date that the privacy complaint was received, – The nature of the privacy complaint, and	▪ N/A

Categories	Privacy Indicators	CIHI Indicators
	– 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 Information and Privacy Commissioner of Ontario.	▪ *Information Security Policy*, first adopted May 2008, reviewed July 2014, July 2015 and July 2016. ▪ *Acceptable Use of Information Systems Policy*, first adopted December 2008, reviewed July 2014, July 2015, November 2015 and June 2016. ▪ *Secure Destruction Policy,* first adopted March 2010, reviewed June 2014, April 2015 and April 2016. ▪ *Patch Management Policy*, first adopted March 2010. Retired July 2014 as the policy was incorporated into ISMS documents. ▪ *Information Security Audit Policy,* first adopted December 2010, reviewed February 2014. Retired July 2014 as the policy was incorporated into ISMS documents. ▪ *Security and Access Policy*, first adopted March 2008, reviewed August 2014, October 2015, January 2016 and July 2016. ▪ *Information Security Audit Program,* first adopted December 2010. Retired September 2014 as the ISMS Audit Program was created. ▪ *File Encryption Standard,* first adopted May 2008, reviewed June 2014 and retired July 2014 as this standard was incorporated into ISMS documents. ▪ *Username and Password Standard,* first adopted October 2008, reviewed January 2014 and retired January 2015 as the standard was incorporated into ISMS documents. ▪ Privacy and Security Incident Management Protocol, see General Privacy Policies, Procedures and Practices above ▪ *Information Security Document Management Standard,* first adopted October 2010, reviewed February 2014 and retired July 2014 as standard was incorporated into ISMS documents. ▪ *Secure Destruction Standard,* first adopted May 2009, reviewed April 2014, May 2015 and May 2016.

Categories	Security Indicators	CIHI Response
		▪ *Third Party Technical Information Disclosure Standard*, first published September 2009, reviewed, December 2014, December 2015 and January 2017 ▪ *COTS Product Technical Requirements Standard,* first published February 2010, reviewed September 2014, September 2015 and May 2016. ▪ *Manual Changes to Production Data Standard*, first published October 2010. Replaced in December 2014 with Manual Changes to Operational Data Standard reviewed in, October 2015 and October 2016. ▪ *Health Data Collection Standard,* first published November 2010, reviewed October 2014, November 2015, and January 2017. ▪ *Secure Information Storage Standard,* first published November 2010, reviewed February 2014, February 2015 and February 2016. ▪ *Secure Information Transfer Standard,* first published November 2010, reviewed January 2014, January 2015 and January 2016. ▪ *Secure Information Backup Standard*, first published November 2010 and retired July 2014 as this standard was incorporated into ISMS documents. ▪ *Anti-Malware Strategy*, first published December 2010, retired December 2014 as this strategy was incorporated into the ISMS Infrastructure Security Standard. ▪ *Responding to Malware Procedure*, first published October 2009, retired December 2014 as this was incorporated into the ISMS Infrastructure Security Standard. ▪ *Safe Email and Browsing Guideline*, first published December 2008, reviewed October 2014 and in November 2015 this guideline was replaced by *Safe Internet Practices and Email Etiquette Guidelines*. ▪ *Email Etiquette Guidelines, first published December 2008,* reviewed October 2014 and in November 2015

Categories	Security Indicators	CIHI Response
		this guideline was replaced by *Safe Internet Practices and Email Etiquette Guidelines*. ▪ *Safe Internet Practices and Email Etiquette Guidelines,* first published November 2015, reviewed December 2016. ▪ *FAQ – Acceptable Use Policy*, first published December 2008, reviewed August 2014, August 2015 and August 2016. ▪ *Use of Production Data in Non-Controlled Environments Policy*, first adopted December 2011, reviewed March 2014 and retired July 2014 ▪ *Database Access Standard*, first adopted June 2012, retired September 2014 and reinstated February 2016. ▪ *File Encryption Procedures*, first published July 2013, reviewed June 2014, May 2015 and May 2016. ▪ *Sensitive Data in Uncontrolled Environments Procedure,* first published March 2014, retired March 2015. ▪ *Cloud Service Privacy and Security Assessment Guideline,* first published February 2012, reviewed October 2014, April 2015 and April 2016. ▪ *Policy on the Maintenance of System Control and Audit Logs*, first published September 2014, reviewed September 2015 and September 2016. ▪ *Use of Cloud Services Policy*, first published October 2011, reviewed January 2014, April 2015 and April 2016. ▪ *Respect of Third Party Software Licence Agreements,* first published March 2014, reviewed April 2014, April 2015 and April 2016. ▪ *ISMS Audit Program,* first published in February 2014, reviewed May 2015, July 2015 and July 2016 ▪ *ISMS Risk Management Manual*, first published in June 2015, reviewed July 2015 and July 2016. ▪ *ISMS Supplier Management*, first published in July 2016. ▪ *ISMS Infrastructure Security Standard,* first published

Categories	Security Indicators	CIHI Response
		in January 2014, reviewed February 2014, March 2014, September 2014, July 2015, January 2016 and July 2016. - *ISMS Manual*, first published in November 2013, reviewed February 2014, May 2014, August 2014, May 2015, July 2015 and July 2016.
	- 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.	*Acceptable Use of Information Systems Policy*, amended to include section on mobile devices and mobile media. *Secure Destruction Policy*, amended to include simple deletion clause, new compliance section and inclusion of smart cell phones/tablets as mobile devices. *Security and Access Policy*, updates to reflect new security system; updates on time changes, updates on contact information. *Secure Destruction Standard*, updates to reflect simple deletion clause, included punching (crushing), instructions pertaining to cell phones/tablets and mobile device media cards. *Third-Party Technical Information Disclosure Standard*, amended to reflect the removal to the Procurement process reference. *Secure Information Transfer Standard*, amended to reflect the removal to the WinZip reference. *COTS Product Technical Requirements Standard,* updates to reflect the revised Code of Business Conduct and the addition of AODA 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. *Secure Information Storage Standard*, amended to include a definitions section and included Health Workforce Personal Information and technical

Categories	Security Indicators	CIHI Response
		information words. *Safe Email and Browsing Guideline*, combined sections of *Email Etiquette Guidelines* and *Email Etiquette to create Safe Internet Practices and Email Etiquette Guidelines*. *Email Etiquette* combined section of *Safe Email and Browsing Guidelines* to create *Safe Internet Practices and Email Etiquette Guidelines.* *ISMS Audit Program,* amended to include audits of policy compliance, renamed document to ISMS Audit Manual from ISMS Audit Program, minor updates for clarification, inclusion of Quarterly Technical Vulnerability Assessment. *ISMS Risk Management Manual*, incorporated minor clarifications for Procurement ad hoc risk assessment requirements. *ISMS Infrastructure Security Standard,* added Data Security Standard, revised anti-malware section and connection restriction for SSH and SFTP, minor word changes to 2.3 Network Connection, and Routing Control, 3.7 System Access Control, addition to 3.6 Strong Password, inclusion of Password/Account Dissemination and added examples in 4.1 Information Classification, minor revisions to 3.9 Connection Restrictions and 4.4 Encryption Standard. *ISMS Manual*, updated security statements, added process for incident management, updates to management processes to reflect minor changes in reporting and monitoring, added new security incident classifications, updates to supplier management, significant updates for compliance with ISO 27001:2013, clarifications in procedures and in “interested parties,

Categories	Security Indicators	CIHI Response
	▪ 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
	▪ 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 (CIHiway). To date, the following communications have been delivered: ▪ *Acceptable Use of Information Systems Policy* – Revised Policy posted on CIHiway August, 2014, December 2014, August 2015, November 2015 and July 2016 ▪ *COTS Product Technical Requirements Standard* – Revised Standard posted on CIHiway November 2014, November 2015 and June 2016 ▪ *Health Data Collection Standard* – Revised Standard posted on CIHiway October 2014, July 2015, February 2016 and February 2016.

Categories	Security Indicators	CIHI Response
		▪ *Safe Internet Practices and Email Etiquette Guidelines* – Revised Guidelines posted on CIHiway November 2015 and January 2017 ▪ *Secure Destruction Policy* – Revised Policy posted on CIHiway June 2014, May 2015 and June 2016 ▪ *Secure Destruction Standard* – Revised Standard posted on CIHiway April 2014, May 2015, November 2015, February 2016 and May 2016. ▪ *Secure Information Storage Standard* – Revised Standard posted on CIHiway March 2014, March 2015, May 2016 and February 2017. ▪ *Secure Information Transfer Standard* – Revised Standard posted on CIHiway March 2014, February 2015, August 2015, January 2016 and March 2017 ▪ *Security and Access Policy* – Revised Policy posted on CIHiway August 2014, October 2015, January 2016 and July 2016 ▪ *Third-Party Technical Information Disclosure Standard* – Revised Standard posted on CIHiway December 2014, December 2015 and January 2017 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.	▪ None
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 Information and Privacy Commissioner 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.	• Bi-weekly audit of access cards issued by CIHI reception • Annual physical audit of access cards every January as part of the "January is Privacy Awareness Month at CIHI" campaign. No recommendations

Categories	Security Indicators	CIHI Response
Security Audit Program	• The dates of the review of system control and audit logs since the prior review by the Information and Privacy Commissioner of Ontario 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* (pages 130-136 of this Report)
	• The number and a list of security audits completed since the prior review by the Information and Privacy Commissioner of Ontario 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* (pages 130 – 136 of this Report). CIHI has completed the following 61 audits: o External Third Party Vulnerability Assessment and Penetration Test (3) o External Third Party Vulnerability Assessment and Penetration Test of 1 Business Application (1) o Database Security Audit (36) o Yearly Internal Data Access Audit (3) o Local Administrator Audit (12) o ISO/IEC 27001:2013 Surveillance / Recertification Audit (3) o 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 Information and Privacy Commissioner of Ontario.	▪ Since November 1, 2013, CIHI has logged 528 information security incidents, none 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. **Note**: The Incident tracking tool was upgraded early 2014 and all data archived. This indicator does not include incidents prior to the upgrade.

Categories	Security Indicators	CIHI Response
	▪ 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.	▪ None of the incidents was classed as a security breach.

Part 3 – Human Resources Indictors

Categories	Privacy 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 Information and Privacy Commissioner of Ontario.	- 431 agents (employees) have received initial privacy and security orientation training in the review period - Agents (employees) returning from an extended leave period of greater than 180 days are required to re-do the privacy orientation training - From May 1, 2015 to October 31, 2016, 35 agents (employees) were re-boarded and completed the required mandatory training (the previous business process management system did not track re-boarding)
	- 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 the Information and Privacy Commissioner of Ontario.	- 100% completed – mandatory training requirements - January 2014 – 733 agents (employees) - January 2015 – 745 agents (employees) - January 2016 – 699 agents (employees)
	- 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 Information and Privacy Commissioner of Ontario 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. - On-line mandatory training modules for all CIHI agents (employees): (1) January 2014 – Privacy Awareness Month Mandatory Training and Confidentiality Agreement

Categories	Privacy Indicators	CIHI Response
		Renewal for all agents (employees) (2) January 2015 – Privacy Awareness Month Mandatory Training and Confidentiality Agreement Renewal for all agents (employees) (3) January 2016 – Privacy Awareness Month Mandatory Training and Confidentiality Agreement Renewal for all agents (employees) ▪ March 2014: Email to all staff from the President and CEO in response to a minor privacy breach and related documentation on “safe excelling” procedures ▪ July 2014: targeted privacy training session for staff of area involved in privacy breach focusing on privacy principles including data minimization and need-to-know ▪ September 2014: Privacy information session for staff of program area including what’s new coming out of the 2014 PHIPA review process, PIAs, privacy audits, incident management and privacy principles as they relate to CIHI’s third-party data request process ▪ December 2014: Privacy information session for staff of Human Resources ▪ March 2015: Privacy and Security information session for staff of CPHI ▪ April 2015: Privacy Information session for staff of Data Quality ▪ September 2015 – Privacy participated in SmallTalk on Privacy and Security by Design as part of Security Awareness Month ▪ November 2015: Privacy and Security information session on Privacy and Security Risk Management program for staff of Centralized Client Services ▪ Email to all staff on 2016 Data Privacy Day

Categories	Privacy Indicators	CIHI Response
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 Information and Privacy Commissioner of Ontario.	▪ 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 Information and Privacy Commissioner of Ontario.	▪ See Privacy and Security Training and Awareness, above.
	▪ 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 Information and Privacy Commissioner of Ontario.	▪ 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 the Information and Privacy Commissioner of Ontario.	▪ 431 agents (employees) have executed Confidentiality Agreements in the current reporting period – 341 employees and 90 third-party service providers ▪ No agents (employees) 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

Categories	Privacy Indicators	CIHI Response
Termination or Cessation	▪ The number of notifications received from agents since the prior review by the Information and Privacy Commissioner of Ontario related to termination of their employment, contractual or other relationship with the prescribed person or prescribed entity.	▪ 312

Categories	Privacy 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 Information and Privacy Commissioner of Ontario.	▪ 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: September 4 – October 31, 2014 February 18 – March 24, 2016 November 2 – December 7, 2016
	▪ 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 was identified as one of four strategic risks for the organization. Specifically, there is a risk that the current privacy and security risk mitigation strategies will not meet emerging threats. The CIO is the risk champion responsible to oversee the development and monitoring of mitigation strategies and action plans for the coming fiscal year.
Business Continuity and Disaster Recovery	▪ The dates that the business continuity and disaster recovery plan was tested since the prior review by the Information and Privacy Commissioner of Ontario.	▪ The Business Continuity Plan was most recently tested March 2015 and is scheduled for another test in Fall 2016. ▪ The Disaster Recovery Plan was last tested in June 2016.
	▪ 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 and Disaster Recovery Plan was adopted December 2009. ▪ The Plan is revised on a monthly (Call Lists) and annual basis (plan) as well as when required, for example, due to organizational changes. ▪ Recommendations resulting from the March 2015 test have been compiled and an action plan to address them is under development. A review of the Business Impact Analysis (BIA) and Business Continuity Plan (BCP) is scheduled for Q2-Q4 of FY2016-17. ▪ Addition of a new appendix that illustrates all CIHI critical business processes, recovery times and resources required to carry these processes (being finalized)

		▪ A static, externally hosted web page, with pre-scripted messages, was created to facilitate communication with staff and stakeholders in an emergency situation. ▪ Recommendation resulting from the September 2016 DR test was to maintain better records of the activities for the purposes of better integration with ISMS and associated requirements

Approved Data Linkages

Fiscal Year 2013-14 (November 1, 2013 to March 31, 2014)					
No.	**DL - #**	**Date Approved**	**Files Linked**	**Subject**	**Date of Data Destruction**
1	269	21-Feb-14	NTR CDS, DAD, NRS	Outcomes for acute trauma patients in Canada	February 2017
2	323	19-Nov-13	DAD-HMDB, CORR	Organ Donation Potential	April 2014
3	329	19-Nov-13	DAD (Episodes of care)	Trends in Pediatric All-Terrain Vehicles versus Motor Vehicle Crash-Related Injuries in Canada	December 2016
4	346	12-Dec-13	NPDUIS	Thiazolidinedione and heart failure	January 2017
5	351	20-Dec-13	DAD, NRS	Analysis-in-Brief on outcomes for bilateral simultaneous versus staged total knee arthroplasties	January 2017
6	353	6-Jan-14	DAD	Monitoring Quality of Care for Joint Replacements: Assessing Alternative Statistical Techniques to Accurately Measure Time to Revision	January 2017
7	380	23-Jan-14	DAD, NACRS, NRS	Stroke Report 2014: Quality of stroke care in Canada	January 2017
8	382	21-Jan-14	OTR CDS (Episodes of care)	Analysis on trauma and burn care in Ontario	January 2017
9	409	6-Feb-14	CCRS, NACRS, DAD	Avoidable (Emergency Department) ED Utilization	October 2015
10	422	19-Feb-14	DAD and NTR CDS	Developing trauma centre performance indicators for non-fatal outcomes	February 2017
11	436	13-Mar-14	NRS and DAD	Influence of Timely Access to Inpatient Rehabilitation Following Acute Care Admission to Hip Fracture	January 2016 or 1-year after publication
12	191	10-Apr-14	DAD-HMDB	Canadian Pediatric Trauma Systems: From Policy to Practice	May 2017

Approved Data Linkages

Fiscal Year 2014-15					
No.	**DL - #**	**Date Approved**	**Files Linked**	**Subject/ Project or Study Title**	**Date of Data Destruction**
1	126	28-May-14	N/A	Other CIHI Use of PRAG (linked) data	March 2017
2	119	2-Jun-14	DAD (Episodes of Care)	CIHR Team in Child and youth Injury Prevention	June 2017
3	115	22-Apr-14	DAD, NACRS, CCRS	Advanced Directives in Long Term Care	April 2017
4	136	28-May-14	SMDB, AFMC-CAPER	Create a national approach, founded on robust data, to establish and adjust the number and type of specialty positions needed in Canadian residency programs in order to meet societal needs	June 2017
5	148	20-May-14	NPDUIS	Data linkage of NPDUIS record-level claims data	May 2017
6	146	14-May-14	DAD, NACRS, Researcher's Data	PeriOperative ISchemic Evaluation ("POISE") study	May 2017
7	174	6-Jun-14	DAD, NACRS	An economic assessment of disease burden due to parasitic zoonoses (Echinococcosis, Toxoplasmosis, Toxocariasis) in Canada	June 2017
8	178	25-Jun-14	HMBD, BC Transplant potential organ donor data	Estimating Donor Potential and Donor Conversion Rates	April 2015
9	192	20-Jun-14	NPDUIS, DAD and NACRS	Data linkage of NPDUIS, DAD and NACRS record-level data	June 2017
10	201	4-Jul-14	DAD-HMDB, NACRS	Annual System Performance Report: Breast Cancer Treatment	June 2017
11	218	29-Jul-14	HCRS, NACRS, DAD	Avoidable (Emergency Department) ED Utilization	November 2015
12	231	25-Aug-14	CORR, DAD, NACRS	Cost-effectiveness of Dialysis Modality Distribution in Canada	September 2017
13	234	22-Aug-14	HMHDB and NPDUIS	Analysis-in-Brief on psychiatric medication use among mental health patients	March 2016

Approved Data Linkages

Fiscal Year 2014-15					
No.	**DL - #**	**Date Approved**	**Files Linked**	**Subject/ Project or Study Title**	**Date of Data Destruction**
14	246	5-Sep-14	DAD	Benchmark for Surgery: The Canadian Collaborative Study of Hip Fractures	September 2017
15	262	26-Sep-14	DAD, NACRS, PLPB (AB, SK)	Linkage of NACRS, DAD and Alberta and Saskatchewan Physician Level Billing data for a Health Reports product	May 2016
16	265	30-Sep-14	DAD, NPDUIS	Adolescent Mental Health	September 2017
17	269	9-Oct-14	CJRR-DAD	Renewal of Annual Approval of linked CJRR_CAD data quality and analytical activities	October 2017
18	274	14-Oct-14	DAD	Seeking approval to link 10 years of record-level DAD data (moms & babes)	October 2014
19	268	24-Oct-14	DAD, NACRS, PLPB (AB, SK)	Linkage of NACRS, DAD and Alberta and Saskatchewan Physician Level Billing data for a Physicians Team product	April 31, 2016
20	318	11-Dec-14	NPDUIS to CCRS	Follow-up to Drug Use in Seniors (May 2014)	December 2017
21	319	15-Jan-15	PRAG	Health Service Utilization and Costs for Chronic Obstructive Pulmonary Disease (COPD): Understanding Characteristics of the High Cost COPD Population	March 2017
22	338	2-Feb-15	DAD and NACRS	Assessing rotavirus vaccine safety in Canada with regard to intussusception using administrative data	February 2018
23	345	2-Mar-15	CCRS, DAD, NACRS	The Prevalence and Impact of Spine Pain in Ontario Long Term Care Seniors	March 2018
24	348	9-Feb-15	DAD, HCRS, CCRS	Sex differences in admission to intensive care unit (ICU)	February 2018
25	357	29-Jun-15	CCRS & interRAI Quality of Life Survey data	Use of the interRAI Subjective Quality of Life Survey in Canadian Long-Term Care Homes	July 2040

Approved Data Linkages

Fiscal Year 2014-15					
No.	**DL - #**	**Date Approved**	**Files Linked**	**Subject/ Project or Study Title**	**Date of Data Destruction**
26	360	2-Mar-15	DAD-HMDB and NACRS non-Ontario data (2002/03-2013/14)	A component of the Canadian Alliance for Healthy Hearts and Minds study	March 2020
27	381	1-Apr-15	HCRS, CCRS, DAD, NACRS	The Relationship between Health Service Utilization and Health-related Outcomes Among Older Adults with Sensory and Cognitive Impairments	April 2018

Approved Data Linkages

Fiscal Year 2015-16					
No.	**DL - #**	**Date Approved**	**Files Linked**	**Subject/ Project or Study Title**	**Date of Data Destruction**
1	48	25-May-15	CMSMS and DAD	The Interface between Critical Illness and Chronic Disease	June 2018
2	46	June 5, 2015	DAD, NACRS, AB and SK PLPB	Choosing Wisely Canada Project	December 2016
3	65	12-Jun-15	DAD, NACRS, HCRS and CCRS	Landscape Assessment of Chronic Pain Management in Ontario	June 2018
4	79	27-Jul-15	HCRS, CCRS, DAD, NACRS, OMHRS, NPDUIS, PLPB	CIHI Project: Seniors in Home Care and Long Term Care	July 2018
5	95	20-Jul-15	DAD	Benchmarking Quality of Care for Renal Cell Carcinoma (RCC) Surgery in Canada: A Population Based Analysis	July 2018
6	104	30-Jul-15	DAD, NRS	Internal Linkage of DAD and NRS to evaluate the AlphaFIM® data submitted for stroke clients in the DAD	July 2018
7	107	4-Aug-15	DAD	Optimal timing of delivery for women with pre-existing and gestational diabetes	August 2018
8	82	24-Jul-15	NRS, Researcher's records	Early PM&R Consultation & Outcomes for Trauma Patients	April 2022
9	84	27-Jul-15	CCRS, NACRS, DAD	Hip fracture risk assessment; Long-Term Care Facilities (LTCFs)	July 2018
10	105	31-Jul-15	DAD, Researcher's records	Incidence/predictors cardiovascular & psoriatic disease	August 2020
11	118	7-Oct-15	CJRR, DAD	Renewal of Annual Approval of linked CJRR_CAD data for CJRR data quality, analytical activities, and creation of external information products	October 2018

Approved Data Linkages

Fiscal Year 2015-16					
No.	**DL - #**	**Date Approved**	**Files Linked**	**Subject/ Project or Study Title**	**Date of Data Destruction**
12	126	25-Aug-15	CORR,DAD	Approval of linked CORR_DAD data for data quality activities	September 2017
13	127	19-Oct-15	DAD, NACRS, OMHRS	Strategy for Patient Oriented Research (SPOR): Dynamic cohorts of individuals with complex needs (high users)	Phase 1 - Ongoing approval for the creation of internal rosters
14	135	7-Oct-15	DAD, NACRS, OMHRS, NRS, CCRS, HCRS, CORR, CJRR, NPDUIS, PLPB	Data quality analysis to support the ongoing maintenance of the corporate client linkage methodology	Ongoing linkage, where linked data sets will be destroyed 3 months after completion of each data analysis
15	141	11-Sep-15	DAD, HMDB	Canadian children previously hospitalized to the pediatric intensive care unit (PICU) for asthma exacerbation: long-term rehospitalisation rates and associated predictors	September 2018
16	140	16-Sep-15	DAD, NACRS, & Researcher's records	Is Electrolyte Maintenance Solution Administration Required in Low-Risk Children with Gastroenteritis	October 2020
17	178	28-Oct-15	10 years of DAD	Intensive care utilization patterns and long-term outcomes for critically ill Canadians	October 30, 2018
18	196	10-Nov-15	CORR, DAD, NACRS	The Clinical and Economic Burden of Infectious Diseases in Canadian Transplant Recipients	November, 2018
19	201	21-Dec-15	HCRS, CCRS, DAD, NACRS	Extending Dimensional Modeling through the abstraction of data relationships and development of the Associative Dimension	January 2019
20	211	7-Dec-15	HCRS, CCRS, DAD, NACRS	Developing and testing quality indicators for palliative care using existing data	January 2019

Approved Data Linkages

Fiscal Year 2015-16					
No.	**DL - #**	**Date Approved**	**Files Linked**	**Subject/ Project or Study Title**	**Date of Data Destruction**
21	192	17-Dec-15	DAD, NACRS, NRS, CCRS	Stroke Report 2016, Quality of Stroke Care in Canada	December 2020
22	212	4-Dec-15	CORR, DAD, OMHRS, CMDB	Data linkage for CORR Analysis-in-brief	December 2018
23	225	6-Jan-16	HCRS, CCRS, OMHRS, DAD, NACRS, NPDUIS	Research study on the care of frail, acutely ill, older persons	December 2018
24	179	5-Jan-16	DAD and NACRS	Linkage of 13 years of NACRS and 21 years of DAD data for Ontario patients to analyze the trend of ED visits, including the trend of workplace injury incidence, utilization of resources (number of visits within a time interval, in-patient LOS, number and types of procedures) as well as quality of care (time to first treatment, comparison of WSIB patients to non-WSIB patients).	January 2019
25	220	18-Jan-16	DAD, NACRS, PLPB, CCRS, HCRS, NPUDIS	Characteristics and Healthcare Utilization Patterns of Chronic Obstructive Pulmonary Disease (COPD) Patients Across Multiple Sectors of Care in Alberta	Fall 2017
26	234	14-Jan-16	DAD	Regional and temporal variations in incidence, prevalence and outcomes of critical illness among pregnant and post-partum women and newborns in Canada	January 2019
27	233	12-Jan-16	DAD, NACRS, OMHRS, NRS, CCRS, NACRS	Ongoing Data Quality Analyses: Linkage of a rolling five years of closed year data plus open year data for all applicable jurisdictions	Ongoing linkage, where linked data sets will be destroyed 3 months after the completion of each analysis

Approved Data Linkages

Fiscal Year 2015-16					
No.	**DL - #**	**Date Approved**	**Files Linked**	**Subject/ Project or Study Title**	**Date of Data Destruction**
28	239	15-Jan-16	OMHRS, HCRS, CCRS	Cognitive decline and mental health conditions, across health care settings	February 2017
29	250	29-Jan-16	AB PLPB, CCRS	Linkage of three years (FY 2010-11 to 2012-13) of Alberta Patient Level Physician Billing (PLPB) data to Continuing Care Reporting System (CCRS) data to generate a more comprehensive cost estimate for a standard resident day.	February 2017
30	269	11-Feb-16	NACRS/DAD with NPDUIS, NACRS/DAD with PLPB	Health Reports project regarding hysterectomies	Q1 of 2017
31	274	10-Feb-16	DAD, NACRS	Linkage of five years (FY2010-11 - 2014-15) of DAD and NACRS data for study on testicular torsion in minors	February 2019
32	276	4-Apr-16	DAD-HMDB, NACRS, AACRS, and OMHRS	Longitudinal Patterns of Hospital Use by High Users of Inpatient Acute Care Services	June 2017
33	304	24-Mar-16	DAD,NACRS,OMHRS	High system users cohorts to support future disclosures for the Strategy for Patient Oriented Research (SPOR) Primary and Integrated Care Innovations (PICHI) Network	April 2019
34	309	24-Mar-16	DAD/HMDB and NACRS	Estimating the Number of Cardiovascular Events Attributable to Major Risk Factors in Canada using a Cardiovascular Disease Policy Model	March 2019
35	325	15-Apr-16	DAD, NACRS, PLBP, CCRS, HCRS, NPDUIS	Characteristics and Healthcare Utilization Patterns of COPD Patients Across Multiple Sectors of Care in Alberta	Fall 2017
36	318	6-Apr-16	PLPB and DAD	Readmissions and physician follow-up analysis for Saskatchewan HSP Workshop	April 2017

Approved Data Linkages

Fiscal Year 2016-17 (up to and including October 31, 2016)					
No.	**DL - #**	**Date Approved**	**Files Linked**	**Subject/ Project or Study Title**	**Date of Data Destruction**
1	9	6-Apr-16	PRAG	Development a product to examine the effectiveness of post-discharge follow-up in reducing unplanned readmissions (acute care and ED visits).	March 2017
2	12	20-Apr-16	DAD	Care Setting Transitions in the Last Year of Life	April 2019
3	39	9-May-16	DAD, NACRS, PLPB	Production of the cost estimates that form the core of the OECD Hospital Cost Variation Pilot project	June 2017
4	40	11-May-16	DAD, NACRS, AACRS	Maintenance of reference files for standard client linkage methodology	When no longer required
5	51	1-Jun-16	CORR, DAD, NACRS	"Knowledge Translation Interventions to Prevent the Early Initiation of Dialysis: A Cluster Randomized Trial"	July 2019
6	45	10-Jun-16	DAD, NACRS, NRS, CCRS and HCRS	Monitoring Cardiac Care in Canada" - Annual Heart Report and Survivor Support	June 2021
7	174 (15-16)	8-Jun-16	DAD, NACRS & Cardiac Care Network registry data	Exercise to confirm coding quality of cardiac procedures	June 2021
8	101	24-Jun-16	DAD and NACRS	Primary Biliary Cholangitis (PBC) and Liver Transplants in Canada	June 2017
9	46	11-Jul-16	HMHDB, CAD	Ongoing mental health program of work	July 2021
10	130	25-Jul-16	DAD	An outcome-based approach to studying the optimal rate of caesarean delivery in Canada	August 2019
11	136	29-Jul-16	NPDUIS, DAD	Linkage of DAD to NPDUIS files for CIHI work in support of Choosing Wisely Canada	July 2019
12	168	30-Aug-16	DAD (Moms & Babes)	Adult Congenital Heart Disease, Pregnancy and Long-Term Cardiovascular Functioning	September 2019

Approved Data Linkages

Fiscal Year 2016-17 (up to and including October 31, 2016)					
No.	**DL - #**	**Date Approved**	**Files Linked**	**Subject/ Project or Study Title**	**Date of Data Destruction**
13	171	26-Sep-16	DAD, HCRS	Program Evaluation of the Stroke Rehabilitation Community Model in Waterloo Wellington	October 2019
14	189	23-Sep-16	DAD (Moms & Babes)	Indicator Development & Data Quality: Obstetric Trauma Indicator	When no longer required
15	176	16-Sep-16	DAD/HMDB, OMHRS, NACRS, and NRS	High Users of Hospital Beds indicator	When no longer required
16	215	Open	DAD-HMDB	Childbirth Quick Stats	tdb
17	222	24-Oct-16	DAD-HMDB, NACRS, Saskatchewan re-contact data, T1 Family File, Vital Statistics Death data, Immigrant Landing file data	Profiles of repeated contact with the Saskatchewan criminal justice system	‘March 2027
18	225	24-Oct-16	DAD-HMDB, NACRS	Examination of the long-term community adjustment of offenders: Linking Federal correctional data with income, health and immigration data	‘March 2027
19	220	28-Oct-16	NPDUIS-CCRS	Use of Antipsychotics Among Seniors Living in Long-Term Care Facilities	‘October 2019

Privacy Impact Assessment Log

Data Holding / Information System / Technology / Program	Last Completed	Next Scheduled 5-Yr Review	Comments	Statement of Purpose
Methodologies and Specialized Care				
Hospital Mental Health Database (HMHDB)	2016	2021/22		Reviewed – no change
Home Care Reporting System (HCRS)	2011	2016-17	Renewal In progress – expected completion Q4 2016-17	
Continuing Care Reporting System (CCRS)	2012	2017-18		
Ontario Mental Health Reporting System (OMHRS)	2011	2016-17	Renewal In progress – expected completion Q4 2016-17	
National Rehabilitation Reporting System (NRS)	2015	2019-20		Reviewed – no change
Paediatric Rehabilitation Database			No further requirement for a PIA (see Addendum to CAD PIA)	
Population Risk Adjustment Group (PRAG) Project	2015	2019-20		New
Pharmaceuticals and Health Workforce Information Services				
National Prescription Drug Utilization Information System (NPDUIS)	2011	2016-17	Renewal In progress – expected completion Q4 2016-17	
National System Incident Reporting (NSIR)	2015	2020-21	De-identified data	Reviewed – no change
Patient Level Physician Billing Data	2015	2019-20		New
Health Spending & Strategic Initiatives				
Canadian Patient Cost Database	2012	2017-18		
Vital Statistics (Death) Data			On hold pending further discussions on access to Vital Statistics Data	
Clinical Data Standards & Quality				
Reabstraction Studies	2015	2020-21		New

Integrated e-Reporting and Portal Services				
CIHI Portal	2014	2018-19	De-identified data	Reviewed – no change
HMD SRI (Client Linkage Index)			No further requirement for a PIA	
e-Reporting			Replaced by Your Health System: Insight	
Your Health System: Insight	2015	2020-21		New
Clinical Administrative Databases and Decision Support Services and Clinical Registries				
Canadian Joint Replacement Registry (CJRR)	2010	2015-16	Renewal in progress – expected completion Q4 2016-17	
Canadian Organ Replacement Registry (CORR)	2010	2015-16	Renewal in progress – expected completion Q4 2016-17	
➢ CORR WAVE Addendum	2012	2015-16	Addendum to be incorporated into renewal of PIA	
Clinical Administrative Database (DAD, HMDB, NACRS)	2012	2017-18	Addendum in progress – expected completion Q4 2016-17	
National & Ontario Trauma Reporting Dataset (NTR/OTR)	2013	2017-18		
Canadian MS Monitoring System (CMSMS)	2013	2018-19	Addendum completed October 2016	
Canadian Patient Experiences Data Collection and Reporting System	2015	2019-20		New
Conceptual PIA for Patient Reported Outcome Measures (PROMs)	2015		One-time conceptual PIA	N/A
Primary Health Care				
Primary Health Care Voluntary Reporting System	2013	2017-18		
➢ Addendum re. Cessation of Data Collection	2016		Addendum updated January 2016	Reviewed – no change

CIHI'S Privacy Impact Assessment Program – Summary of Recommendations

Fiscal Year: __2013-14____

Description of Privacy Impact Assessment	Recommendations	Manner Addressed	Completion Date
CIHI Portal A privacy impact assessment that updates the foundational PIA completed in 2008 and the related Addendums 2008/09 and 2010/11, and re-examines the potential privacy, confidentiality and security risks associated with CIHI Portal in its entirety, including any scheduled enhancements planned for 2013-14. (May 2014)	No recommendations	n/a	n/a
Primary Health Care Voluntary Reporting System (PHC VRS) – January 2014 Addendum – Updated January 2016 An addendum to the 2013 PHC VRS PIA was published in January 2014 with notification that, effective December 1, 2013, CIHI ceased collecting EMR data. CIHI intends to continue using the data to inform the evolution of the PHC EMR Content Standard and may use the data for analytical purposes. It will review this decision in December 2015 to determine whether it will retain the data or securely destroy it. The Addendum will be updated accordingly at that time. Addendum updated January 2016.	No recommendations	n/a	n/a

Fiscal Year: __2014-15____

Description of Privacy Impact Assessment	Recommendations	Manner Addressed	Completion Date
Population Risk Adjustment Group (PRAG) Project A 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.	No recommendations	n/a	n/a
Patient Level Physician Billing Data Repository A 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.	No recommendations	n/a	n/a
Canadian Patient Experiences Data Collection and Reporting System A privacy impact assessment of the privacy and security risks associated with the Canadian Patient Experiences Data Collection and Reporting System. The scope of the current assessment is development of an operational system at CIHI that will begin accepting patient experience dated by April 1, 2015, collected by, or on behalf of, jurisdictions using the new CPERS data standard.	No recommendations	n/a	n/a
Conceptual PIA for Patient Reported Outcome Measures (PROMs) A privacy impact assessment of the privacy and security risks associated with the concept whereby CIHI would be the direct collector of PROMs from patients.	As part of the conceptual assessment, possible risks were identified along with associated recommended actions/ mitigations.	n/a	n/a

Fiscal Year: __2015-16____

Description of Privacy Impact Assessment	Recommendations	Manner Addressed	Completion Date
Reabstraction Studies A privacy impact assessment of the privacy and security risks associated with reabstraction studies conducted by CIHI.	1.1 Develop and adopt procedures to mitigate risk of unauthorized disclosure of record-level data to facility staff during on-screen review of Debrief File (p.17 of PIA).	As per recommendation	Q2 2015-16
	2.1 The Service Desk implemented enhanced procedures to ensure that when CIHI's Human Resources department initiates immediate revocation of staff access, staff access to CIHI's external applications (including the Reabstraction Web Tool) will also be revoked immediately as well.	As per recommendation	Q3 2015-16
	2.2 By the end of Q3 2015–2016, Classifications and Terminologies to embed retention requirements in the reabstraction studies procedures and study project plan template.	As per recommendation	Q3 2015-16
	2.3 Centralized Client Services (CCS) to conduct an annual audit of CIHI staff with access to high-risk applications/services to verify that access is revoked when no longer necessary. It is recommended that CCS consider coordinating the audit with CIHI's annual SAS data access.	As per recommendation	Q4 2015-16
	3.1. Module 1: Privacy and Security section of reabstractor training updated to reflect operational requirements unique to reabstraction studies. audit to reduce burden on data owners.	As per recommendation	Q2 2015-16
National Rehabilitation Reporting System (NRS) A privacy impact assessment of the privacy and security risks associated with the National Rehabilitation Reporting System (NRS). The NRS supports the planning and management of publicly funded inpatient rehabilitation services in Canada.	No recommendations	n/a	n/a

Description of Privacy Impact Assessment	Recommendations	Manner Addressed	Completion Date
Your Health System: Insight A privacy impact assessment of the privacy and security risks associated with CIHI's Your Health System: Insight (YHS: Insight) analytical, web-based tool available to registered clients in a secured private environment. Q3 update: Complete. The process was implemented in 2015 with the Standard Operating procedure to be completed by January 29, 2016.	1. Increase the frequency of audit reviews to the level that would be closer to monitoring, as opposed to conducting infrequent historical audits;	Option analysis completed and received approval for recommended approach.	Q4 2015-16
	2. Define a process to ensure timely response to jurisdictional/organizational changes (within CIHI);	Completed	Q3 2015-16
	3. Review and improve, where possible, the process for organization contacts to enter (log) changes for themselves or for users;	Deferred – to be part of the Single Source of Truth for Contacts and Organizations project.	n/a
	4. Define a process to validate that the organization contact is current when making access changes; and	Standard Operating Procedure	Q4 2015-16
	5. Develop a plan to ensure appropriate user awareness within CIHI and with clients.	Included part of above recommendations	Q4 2015-16
National System Incident Reporting (NSIR) A privacy impact assessment of the privacy and security risks associated with the National System for Incident Reporting, a voluntary reporting system designed to facilitate sharing and learning from medication incidents.	No recommendations	n/a	n/a

Fiscal Year: __2016-17____

Description of Privacy Impact Assessment	Recommendations	Manner Addressed	Completion Date
Hospital Mental Health Database (HMHDB) A privacy impact assessment of the privacy and security risks associated with the Hospital Mental Health Data Base which is a pan-Canadian database containing information regarding hospital inpatient care provided for mental illness and addictions	No recommendations	n/a	n/a
CMSMS Addendum An Addendum to the PIA for the Canadian MS Monitoring System to identify end of data collection as of April 2016.	No recommendations	n/a	n/a

CIHI’S Privacy Audit Program

Fiscal Year: 2012-13

Description of Audit	Recommendations	Manner Addressed	Completion Date
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.	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. Seven of the eight have been completed to date.	March 2017

Fiscal Year: 2013-14

Description of Audit	Recommendations	Manner Addressed	Completion Date
A privacy audit of CIHI's Identity Management Access to determine whether: • The authorization and authentication procedures for Identify management are being followed; • Security Incidents have occurred as a result of failure to comply with Identity management standard operating procedures	Privacy Audit Framework for Access Management completed in Q1 2014-15 The four phases of the audit have been completed. Preparation of report in progress.		

Fiscal Year: 2014-15

Description of Audit	Recommendations	Manner Addressed	Completion Date
A compliance audit of two external third-parties that received data from CIHI to ensure the third-parties are meeting or have met their contractual obligations, as set out in CIHI's confidentiality agreement. The data was originally disclosed to a recipient for a study. Subsequent to this, a working copy of the data was sent to a second researcher in another jurisdiction for the purpose of completing the study. The audit involved following the trail of the data.	**Recipient 1 and Organization 1** 1. That all individuals who have access to CIHI data sign Part F of CIHI's Non-Disclosure/Confidentiality Agreement.	Accepted as per recommendation	February 2015
	2. That any future transmissions of CIHI data only occur if the information is first encrypted.	Accepted as per recommendation	February 2015
	Recipient 2 and Organization 2 3. That the original CD-ROM that contains the unencrypted data is destroyed.	Accepted as per recommendation	March 2015
	4. That the USB ports be de-activated for the computer terminal that is used to access CIHI data.	Accepted as per recommendation	January 2015
	Recipient 1 and Organization 1 & Recipient 2 and Organization 2 5. That logs to track access to CIHI data are created and monitored.	**Recipient 1 and Organization 1** Closed - determined to be impracticable	February 2015
		Recipient 2 and Organization 2 Accepted as per recommendation	January 2015
	6. That the obligation to include the disclaimer in every publication arising from the use of the CIHI data found in paragraph 16 of CIHI's Non-Disclosure/Confidentiality Agreement is met.	Accepted as per recommendation	**Recipient 1 / Organization 1** (February 2015) **Recipient 2 / Organization 2** (September 2015)

Fiscal Year: 2015-16

Description of Audit	Recommendations	Manner Addressed	Completion Date
A Privacy topic audit of third-party record-level data requests to ensure external releases of record-level data to third-parties that have a destruction requirement were correctly flagged by Program Areas in CIHI's Data Request Process (DRP) application.	(1) That Corporate Data Request Program (CDRP) with the support of Privacy and Legal Services, develop a routine audit process to ensure that appropriate data releases are flagged for destruction, and that the outcomes expected by the July 2015 enhancements are achieved.	Accepted as per recommendation	February 2016
	(2) That CDRP update and enhance the user documentation available to Program Area staff, such that the expectations associated with Destruction Flag with the Release and Closing Step of the DRP are clearly understood by staff. Privacy and Legal Services input should be sought to contribute to the document enhancements.	Accepted as per recommendation	February 2016

Fiscal Year: 2016-17

Description of Audit	Recommendations	Manner Addressed	Completion Date
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.	In progress		

External Audit of CIHI’s Privacy and Security Program

Fiscal Year: 2014-15

Description of Audit	Recommendations	Manner Addressed	Completion Date
Office of the Ontario Privacy Commissioner’s mandatory 3-year review of CIHI’s Prescribed Entity status.	(1) That CIHI ensure that a review of its policies and procedures are conducted, at a minimum, on an annual basis, as required by the *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities.* (2) That CIHI include a mechanism in the tracking of their security incidents and breaches for the categorization of breaches of *policy* separately from breaches of *data*, which will enhance the accuracy and clarity of the reporting of information security breaches to the IPC in the next report.	Accepted as per recommendation	October 2014

CIHI’S Security Audit Program

Fiscal Year: 2013-14

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. Key activities – Physical Security – • Review of CIHI’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	There were a total of 29 specific technical recommendations related to system configuration, processes and implementation. Due to the confidential nature of these recommendations, the specifics will not be provided here.	Of the 29 recommendations: • 18 were addressed • 11 were not actioned either because they were deemed low risk and/or low impact, or were no longer applicable due to retirement of affected systems or no longer applicable	Note - The exact completion dates for this fiscal are unavailable. During this time we were refining our action tracking process and transitioning to a new tracking tool.

Fiscal Year: 2014-15

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. 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	There were a total of 25 specific technical recommendations related to system configuration, processes and implementation. Due to the confidential nature of these recommendations, the specifics will not be provided here.	Of the 25 recommendations: • 20 were addressed • 5 were not actioned because they were deemed low risk or no longer applicable	1. 2015-01-11 2. 2015-01-11 3. 2015-01-24 4. 2015-02-15 5. 2015-03-30 6. 2015-03-30 7. 2015-03-30 8. 2015-05-13 9. 2015-05-28 10. 2015-05-28 11. 2015-06-04 12. 2015-11-01 13. 2015-12-17 14. 2015-12-17 15. 2015-12-17 16. 2015-12-17 17. 2016-03-31 18. 2016-03-31 19. 2016-04-01 20. 2016-09-08

Fiscal Year: 2015-16

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. Key activities – Physical Security • Assessment of 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	There were a total of 38 specific technical recommendations related to system configuration, processes and implementation. Due to the confidential nature of these recommendations, the specifics will not be provided here.	Of the 38 recommendations: • 10 were related to physical security and were incorporated into a physical security risk assessment and strategy, which is currently underway • 24 were addressed • 3 were not actioned because they were deemed low risk or no longer applicable • 1 is underway	1. 2016-01-14 2. 2016-02-02 3. 2016-02-02 4. 2016-02-02 5. 2016-02-11 6. 2016-02-12 7. 2016-02-12 8. 2016-02-12 9. 2016-02-18 10. 2016-02-25 11. 2016-03-04 12. 2016-03-08 13. 2016-03-09 14. 2016-03-09 15. 2016-03-10 16. 2016-03-18 17. 2016-03-30 18. 2016-04-14 19. 2016-04-15 20. 2016-04-18 21. 2016-04-22 22. 2016-05-11 23. 2016-06-06 24. 2016-06-06

Description of Audit	Description of Recommendation	Manner Addressed	Completion Date
External Third Party Vulnerability Assessment and Penetration Test of 1 Business Application In 2015-16, one security vulnerability assessment was conducted on a business application. Due to the confidential nature of these recommendations, the specifics will not be provided here.	There were a total of 4 recommendations.	Completed	November 2015

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. Key activities – Physical Security – Toronto • 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	In progress		In progress

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 27001:2013 Surveillance / Recertification Audit The ISO 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.	2014-2015 Audit – 0 findings 2015-2016 Audit – 2 findings 2016-2017 Audit – 2 findings	Completed/Addressed	2015-2016 1. August 2015 2. June 2016 2016-2017 1. May 2017 2. In progress
ISMS Internal Audit The ISMS Internal Audit is conducted on an annual basis as required by the ISO 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 27001:1013 standard and that it is effectively implemented and maintained.	2014-2015 Audit – 10 Findings 2015-2016 Audit – 8 Findings 2016-2017 Audit – 9 Findings	Completed/Addressed	2014-2015 1. April 2014 2. April 2014 3. Aug 2014 4. Aug 2014 5. Aug 2014 6. Aug 2014 7. July 2014 8. Sept 2014 9. April 2014 10. Aug 2014 2015-2016 1. July 2015 2. Sept 2015 3. Mar 2016 4. June 2015 5. Nov 2015 6. July 2015 7. July 2015 8. Nov 2015 2016-2017 1. July 2016 2. July 2016 3. Nov 2016

Description of Audit	Description of Recommendation	Manner Addressed	Completion Date
			4. Aug 2016 5. Nov 2016 6. Dec 2016 7. Dec 2016 8. Jan 2017 9. Feb 2017

.

InfoSec Staff Awareness, Education and Communication Log

Date	Provider	Attendees	Subject
2013-12	InfoSec	Targeted	Bits ‘n’ Bytes Newsletter for ITS Branch
2014-01	InfoSec & Privacy	All Staff	Privacy Awareness Month
2014-01	Internal	All Staff	InfoSec Newsletter #6
2014 03-18	InfoSec & Privacy	All Staff	Revised *Procurement Policy and Competitive and Non-Competitive Procedure*
2014-03-24	Internal	All Staff	Staff Awareness Article in CIHighway re: Acceptable Use Policy
2014-04-11	Internal	All Staff	InfoSec Strategic Plan uploaded to InfoSec Landing page
2014-04-11	Internal	All Staff	Heartbleed Vulnerability at CIHI
2014-04-23	Internal	All Staff	InfoSec Newsletter #7
2014-05-05	Internal	Targeted	Reminded personnel that providing external consultant access to CIHI network and the sharing of passwords amongst colleagues is a serious security incident and they should review Information Systems Acceptable Use Policy, if unclear or send us an email.
2014-05-29	Consultant	All Staff from Technology & Infrastructure Services	ISMS Audit Training
2014-06-23	InfoSec	Targeted	Bits ‘n’ Bytes Newsletter for ITS Branch
2014-06-25	Consultant	All Staff from Technology & Infrastructure Services	ISMS Audit Update – Kick-off Activities
2014-06-18	InfoSec	CPHI Branch	Provided staff awareness training to CPHI staff
2014-06-30	Internal	All Staff	InfoSec Newsletter #8
2014-07-14	Internal	All Staff from Technology & Infrastructure Services	ISMS Audit Training
2014-09-02	InfoSec & Privacy	All Staff	Security Awareness Month Campaign

Date	Provider	Attendees	Subject
2015-01-04	Internal	All CIHI Staff	Privacy Awareness Month
2015-01-19	InfoSec	ITS	Bits ‘n’ Bytes Newsletter for ITS Branch
2015-01-29	InfoSec	All Staff	Protecting your personal Systems and Data Information Session
2015-01-30	PLS & Security Team Retreat	PLS Staff and Security Staff	First session and introduction to the new Privacy and Security R Risk Assessment framework/program.
2015-02-09	InfoSec	All Staff	InfoSec News
2015-02-13	InfoSec	All Staff	Phishing Email
2015-02	Communications	All Staff and External	ISO 27001 announcement
2015-03-09	InfoSec	CPHI staff	Staff Awareness training
2015-03-11	MARSH	Hassan Gesso	Cyber as a Strategic Risk
2015-03-20	InfoSec	Targeted	Reminder: Technical Vulnerability Management Process
2015-03-25	InfoSec	Targeted	Email re: Fake Canada Post Delivery
2015-04-25	RSA	Hassan Gesso	RSA Conference
2015-05	IAPP	Cal Marcoux	IAPP Canada Symposium
2015-05-20	Cal Marcoux and Hassan Gesso	Ontario Connections, Privacy Confidentiality and RM Conference	Conference for civil servants in the Security, Privacy, Records Management and Freedom of information sector. Session on ‘**Implementing an ISO 27001 Information Security Management System - Lessons from the Trenches’**
2015-06-01	e-Health	Cal Marcoux and Hassan Gesso	Sessions geared towards privacy, security and governance of health data.
2015-06-15	InfoSec	All staff from Technology & Infrastructure	Mandatory meeting to review the ISMS ISO27001: 2013 changes

Date	Provider	Attendees	Subject
		Services	
2015-06-16	InfoSec	All Staff	Forged Emails Article
2015-06-08	InfoSec	All Staff	InfoSec Newsletter
2015-06-23	InfoSec	HSSI Staff	Staff awareness training
2015-07-21	InfoSec	All staff from Technology & Infrastructure Services	Review #2 ISMS ISO-27001:2013 – July 21, 2015
2015-07-22	InfoSec	Targeted	Bits ‘n’ Bytes Newsletter for ITS Branch
2015-07-22	InfoSec	Targeted	Security and Privacy and Legal considerations during projects
2015-08-04	InfoSec	All Staff	IT Services article
2015-08-18	ISACA	Hassan Gesso	Cybersecurity in the Era of Cloud
2015-08-31	InfoSec	All Staff	Information Technology and Services re-organization
2015-09-01	InfoSec & Privacy	All Staff	Security Awareness Month Campaign – month-long series of articles, InfoSec open house
2015-09-30	PhishMe	Allister Miran and Nicole Slunder	User Anti-Phishing Training: How to Build a Successful Program
2015-10	InfoSec	Targeted	Bits ‘n’ Bytes Newsletter for ITS Branch
2015-10-13	InfoSec	All Staff	Introduction of Phishing Program
2015-10-28	ISTS Branch	ISTS Branch	Branch Retreat and 24-hour challenge
2015-10-30	InfoSec	All Staff	InfoSec Newsletter
2015-11-04	GovSec by ConnexSys	Hassan Gesso and JL Guertin	Annual seminar style event: Keynotes, Exhibits, a chance to speak with the experts on the latest IT threats and how to combat them and a panel of experts featuring Jeffery Carr for an in-depth best practice session to combat Cyber Espionage.
2015-12-14	InfoSec	ISTS Branch	First Phishing Scenario launched (free coffee)
2016-01-04	Internal	All CIHI Staff	Privacy Awareness Month

Date	Provider	Attendees	Subject
2016-01-28	Internal	CIHI Staff	Happy Data Privacy Day!
2016-02-08	InfoSec	All CIHI except ITS Division	Phishing Campaign
2016-02-16	Corp Adm	All CIHI Staff	Article on physical security audit findings
2016-02-18	Targeted	Bits ‘n’ Bytes (ITS)	Bits ‘n’ Bytes Newsletter for ITS Branch
2016-02-28	Internal	CIHighway	InfoSec Newsletter – February 2016
2016/04/04	CIHighway	Internal – All CIHI staff	Article on reporting Phishing
2016/04/11	CIHighway	Internal – All CIHI staff	Article on Ransomware
2016/04/20	InfoSec	All CIHI Staff	Phishing Campaign
2016-04-29	Internal	CIHighway	InfoSec Newsletter – April 2016
2016-05-18	Cal Marcoux, CISO	All staff	Important Information on Ransomware
2016/05/25	InfoSec	150 recipients 100 random and past repeat offenders	Phishing Campaign
2016/07/06	InfoSec	118 recipients 76 random & past repeat offenders	Phishing Campaign
2016/07/15	Allister Miran	Presentation to ITS in-scope staff	Review session on Risk Management
2016/07/22	Allister Miran	Presentation to ITS in-scope staff	Review session on Risk Management (second session for absent staff)
2016/07/22	InfoSec	120 recipients 74 random & past	Phishing Campaign

Date	Provider	Attendees	Subject
		repeat offenders	
2016-08-02	Internal	CIHighway	InforSec Newsletter – August 2016
2016-09-06	Internal	All CIHI Staff	Information Security Awareness Month – month-long series of articles, InfoSec open house
2016-09-08	Internal	All CIHI Staff	Small Talk – Privacy and Security by Design