CIHI Submission:
2011 Prescribed Entity Review

October 2011

Canadian Institute for Health Information

Institut canadien d'information sur la santé

Who We Are

Established in 1994, CIHI is an independent, not-for-profit corporation that provides essential information on Canada's health system and the health of Canadians. Funded by federal, provincial and territorial governments, we are guided by a Board of Directors made up of health leaders across the country.

Our Vision

To help improve Canada's health system and the well-being of Canadians by being a leading source of unbiased, credible and comparable information that will enable health leaders to make better-informed decisions.

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 analyze and provide accurate and timely information to establish sound health policy, to effectively manage the health system and to generate public awareness about factors affecting good health. Further to this mandate, CIHI collects and analyses personal health information and reports on health system performance, health spending, health human resources and population health in order to improve health system performance and to improve the health of Canadians. In order to support its national mandate, CIHI has offices located in Ottawa and Toronto in addition to regional offices in Victoria, Montreal and St. John's.

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 Information and Privacy Commissioner of Ontario, 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.

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.

The Information and Privacy Commissioner of Ontario has prepared the *Manual For The Review and Approval of Prescribed Persons and Prescribed Entities* (the IPC Manual) which outlines the new review process to be followed, commencing January 31, 2010. The IPC Manual sets out in detail the requirements imposed on such entities arising from the new review process.

This Report is the result of an iterative review process between CIHI and the Office of the Information and Privacy Commissioner of Ontario, as well as telephone discussions and meetings between officials of

the two organizations held on April 19, 2010, May 20, 2010, March 2011 and May 5, 2011, where CIHI's Chief Privacy Officer provided additional information which would enable the IPC/Ontario to satisfy itself fully of the means by which CIHI has met the requirements under PHIPA and in the Manual.

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 employees 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 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.. The Code does not apply to external consultants or third-party service providers. However, similar obligations are contained in agreements that are used to retain these individuals, and these agreements also contain breach provisions.

It 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 dismissal. All employees are responsible to report actual, potential or suspected violations of the Code of Conduct to their immediate supervisor. 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 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 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 implemented a risk-based audit program and developed criteria to be used in the selection of privacy audit activities.

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.

Other means of monitoring compliance include the logging of privacy and security incidents and through Human Resources.

Pursuant to the IPC Manual, CIHI must submit a detailed written report and sworn affidavit to the Information and Privacy Commissioner of Ontario by January 10, 2011, in order to have its status renewed. 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 27 databases (see CIHI's Products and Services Guide), CIHI is a leading source of unbiased, credible and comparable 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. These policies must be approved by the Information and Privacy Commissioner of Ontario. 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 Vice President and Chief Technology 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 employees[1]. More specifically, CIHI policies, procedures and practices ensure that its 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

Although subsection 45(6) of the Act provides that CIHI may only use the personal health information it receives for the purposes for which it was received, it also provides that it may use the information for research provided that it meets the research related requirements set out in subsection 37(3).

Section 1 and 2 of CIHI's *Privacy Policy, 2010*, identify the purposes for which CIHI uses personal health information and distinguishes between the use of personal health information and the use of de-identified and/or aggregate information. In fact, all of CIHI's uses 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 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.

1. Employees, for purposes of access and use of personal health information, include staff, external consultants or other third-party service providers, on a need-to-know basis when required to perform their duties and/or services.

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 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.

Section 40 of CIHI's *Privacy Policy, 2010*, sets out clear rules for the disclosure of personal health information and the statutory requirements that must be satisfied prior to such disclosures.

Sections 40 and 45 of CIHI's *Privacy Policy, 2010*, clearly distinguish between the purposes for which and the circumstances in which personal health information is disclosed and the circumstances in which and the purposes for which de-identified and/or aggregate information is disclosed. 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.

Finally, 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.

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 *Privacy Policy Procedures* – Preferred Methods of Dissemination 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, or controls, 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 individuals may direct complaints regarding such compliance to the Privacy Commissioner of the appropriate jurisdiction, including to the Information and Privacy Commissioner of Ontario, as the case may be.

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 CPO and the CTO 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 CTO will ensure that the required approval process is followed. 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 breaches and information security breaches;
- 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 the Internet are current and continue to be made available to the public and other stakeholders. As for internal communication to staff, this is guided by the *Privacy and Security Training Policy* which clearly stipulates at sections 4 and 5 that the CPO and CTO will be responsible for determining the content of privacy and security training.

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 it 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.

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 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 staff, in developing their programs and activities, establishes data requirements with their relevant stakeholders, including minimum data sets. As well, 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. Moreover, CIHI is committed at all times, as stated in sections 1 and 2 of CIHI's *Privacy Policy, 2010*, to minimal data collection.

Secure Retention of Personal Health Information Collected

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.

Secure Transfer of Collected Personal Health Information

As stated above, CIHI has developed *Health Data Submission Guidelines* that offer 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 *Privacy Policy Procedures – Preferred Methods of Dissemination*.

Secure Return and Disposal of Collected Personal Health Information

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 *Information 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 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

As previously indicated, the *Products and Services Guide* provides a description of CIHI's data holdings, including the purpose for those holdings, and is updated annually and published on CIHI's external website (www.cihi.ca). Furthermore, 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. Moreover, 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 "10 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.

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

As described above, statements of purposes for all CIHI data holdings containing personal health information is routinely made available to the public through CIHI's external website and is addressed generally through our communication program and through the *Privacy Impact Assessment Policy*.

Use of Personal Health Information

8. Policy and Procedures for Limiting 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 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. Moreover, section 10 of CIHI's *Privacy Policy, 2010*, clearly sets out that access to personal health information by CIHI's employees is limited to a "need to know" basis when required to perform their duties and/or services, and only after they have met the mandatory education requirements in the areas of privacy and security. 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, as defined in CIHI's *Acceptable Use Policy*. CIHI has segregated the roles and responsibilities of employees, where feasible and possible, based on a need-to-know principle, to avoid a concentration of privileges.

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 unencrypted health card numbers and personal health information. In both these instances, section 10 of CIHI's *Privacy Policy Procedures* set out strict controls to ensure the request is duly submitted, 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 entire request and approval processes are documented as per sections 10.1 to 10.20 of CIHI's *Privacy Policy Procedures*. For example, employees identifying a need for access to data must provide a demonstrable justification. Pursuant to section 10.5 of CIHI's *Privacy Policy Procedures*, the Program Area Directors or Managers must consider the following in approving access:

- Is access specifically required by the individual(s) to perform job duties and responsibilities?
- Is the purpose for access generally consistent with CIHI's mandate?
- Is the access for a short-term period?
- Is access being requested to perform a data linkage?

- Can the Service Recipient Index[2] (SRI) be used?
- Is there an alternate solution/option that can be used?

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 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 automatically terminated yearly as a result of CIHI's internal data access audit, and Managers and/or Directors are required to re-approve access requests. Only in certain circumstances is access extended, where employees are able to demonstrate continued need for access.

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 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 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 Employees Granted Approval to Access and Use Personal Health Information

The log of employees granted approval to access and use personal health information is maintained by ITS. It includes the following fields of information:

- Name of 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.

2. The Service Recipient Index is a central repository that assigns a meaningless but unique number to each record that enables or facilitates record linkages at the patient dimension in an anonymized manner.

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.

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 research or 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:

(a) Prohibits contacting the individuals;

(b) Prohibits linking the personal health information unless expressly authorized in writing by CIHI;

(c) Limits the purposes for which the personal health information may be used;

(d) Requires that the personal health information be safeguarded;

(e) Limits publication or disclosure to data that do not allow identification of any individual;

(f) Requires the secure destruction of data, as specified;

(g) Permits CIHI to conduct on-site privacy audits pursuant to its privacy audit program; and

(h) 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 *Privacy Policy Procedures – Preferred Methods of Dissemination*, 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.

Furthermore, CIHI's *Information Security Form* sets out CIHI's minimum security requirements and designates the senior information technology official (for example, the Vice President and Chief Technology Officer or equivalent) of the recipient organization as responsible for:

- ensuring that such personal information is securely destroyed in accordance with the terms of the Data Sharing Agreement or other legally binding instrument; and
- by meeting the secure destruction requirements issued by CIHI.

CIHI also requires that this individual complete and remit a Certificate of Destruction to CIHI within 30 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. 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?

Aall disclosures of personal health information for research purposes must be reviewed and approved by CIHI's Privacy, Confidentiality and Security Team.

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 log of 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). The following data elements are contained in the log:

- 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;
- Whether the records of personal health information will be securely returned, securely disposed of or de-identified and retained by the researcher following the retention period set out in the Research Agreement; and
- The date that the records of personal health information were securely returned, a certificate of destruction was received or written confirmation of de-identification was received or the date by which they must be returned, disposed of or de-identified.

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 collection or 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 or from whom the information will be collected. Sections 40.4 and 40.5 of the *Privacy Policy Procedures, 2010,* 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, the Privacy and Legal Services Secretariat 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.

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 CIHI's Template Data Sharing Agreement.

18. Log of Data Sharing Agreements

CIHI's Privacy and Legal Services Secretariat 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;
- The date the personal health information was collected or disclosed;
- 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.

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. As a result of the 2008 Prescribed Entity review, and in particular as a result of the Commissioner's recommendations, CIHI developed template agreements, namely an Independent Contractor Agreement, a Master Services Agreement and a Standing Offer Agreement, all of which are consistent with the Template Agreement for All Third Party Service Providers.

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. The Confidentiality Agreement includes CIHI's *Secure Destruction Information Package*. This Package sets out CIHI's requirements with respect to secure destruction of all data that is accessed and used.

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.

Section 7 of the *Competitive and Non-Competitive Procurement Procedure* states that CIHI's Procurement Unit will maintain all fully executed Supply Agreements for future reference and audit. In addition, the Procurement Unit will maintain a log of all executed Supply/Master Agreements. The Procurement Unit captures all relevant and necessary information from third-party service provider agreements in a database.

The Procurement Unit, in collaboration with the Privacy and Legal Services Secretariat, ensures that the data destruction compliance process is implemented, whereby all data sets disclosed to third parties, whether they contain personal health information or de-identified data, are tracked and monitored to ensure that the data destruction requirements are met at the end of their life cycle. This process includes third-party service providers.

20. Template Agreement for All Third Party Service Providers

Section 5.1 of 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.

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 are contained in CIHI's template agreements – an Independent Contractor Agreement, a Master Services Agreement and a Standing Offer Agreement – all of which are consistent with the Template Agreement for All Third Party Service Providers.

21. Log of Agreements with Third Party Service Providers

CIHI's Procurement Unit maintains a log of all Third Party Service Provider Agreements. The following data elements are contained in the log:

- The name of the third party service provider;
- The nature of the services provided by the third party service provider that require access to and use of personal health information;
- The date that the agreement with the third party service provider was executed;
- The date that the records of personal health information or access to the records of personal health information, if any, was provided; and
- The date of termination of the agreement with the third party service provider.

As noted above, CIHI has instituted an ongoing data destruction compliance process that includes data provided to third-party service providers. The following data elements are captured in that process:

- The nature of the personal health information provided or to which access was provided;
- Whether the records of personal health information, if any, have been securely returned or have been securely disposed of following the date of termination of the agreement; and
- The date the records of personal health information were securely returned or a certificate of destruction was provided or the date that access to the personal health information was terminated or the date by which the records of personal health information must be returned or disposed of or access terminated.

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 Team 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 Team 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 heath 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 Team 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 personal 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 Service Recipient Index that contains randomly assigned meaningless or unique numbers (MBUNs) to enable or facilitate record linkages at the patient level in an anonymized manner. As set out in the procedures related to section 14, data linkages to be conducted using MBUNs must also obtain approval 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. To date, CIHI has not disclosed linked data sets of personal health information.

Retention of Linked Records of Personal Health Information

As stated in section 1 above, 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 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.

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 *Information 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 Information Destruction Standard.

Tracking Approved Linkages of Records of Personal Health Information

Section 21.4 of CIHI's *Privacy Policy Procedures* requires the Privacy and Legal Services Secretariat 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.

Every January, employees at CIHI must renew their employee Confidentiality Agreement whereby they 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.

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

a. On existing programs, initiatives, processes and systems where significant changes relating to the collection, access, use or disclosure of personal information are being implemented that impact the assessment in the current PIA.
b. 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.

c. On any other programs, initiatives, processes and systems with privacy implications as recommended by the CPO in consultation with program area or project management.

As stated above, CIHI's *Privacy Impact Assessment Policy* requires that privacy impact assessments on a new or a change to an existing information system, technology or program involving personal health information must be done at the conceptual design stage and then 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, which is in place on a three-year cycle.

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 stated in section 6 of the *Policy*, PIAs are to be updated in the following circumstances:

a. 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;
b. other changes that may potentially affect the privacy and security of those programs, initiatives, processes and systems;
c. the CPO determines that an update of a PIA or a new PIA is required and recommends same; or
d. every three years at a minimum.

CIHI's Privacy Impact Assessments contain at least the following elements:

- 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.

In order to close the loop on risk management, CIHI's *Privacy Impact Assessment Policy* contains a process for managing the recommendations arising from privacy impact assessments. Section 4 of the *Policy* states that where a PIA includes recommendations, the Vice-President of the relevant program area is responsible for ensuring that a plan to implement the recommendations is drafted. The implementation plan shall include prioritized action items with responsibilities and time lines.

The Privacy and Legal Services Secretariat is responsible for maintaining a scheduling log of all privacy impact assessments completed, undertaken but not complete, and others that are scheduled.

26. Log of Privacy Impact Assessments

CIHI's Privacy and Legal Services Secretariat maintains a log of Privacy Impact Assessments that have been completed. 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 employee(s) responsible for completing or ensuring the completion of the privacy impact assessment.

CIHI's Privacy and Legal Services Secretariat also 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 privacy impact assessment;
- the 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.

Both logs above are cross-referenced at all times.

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 and security-related policies and practices. This includes yearly internal data access audit to ensure only authorized staff have access to PHI in CIHI's analytical environment. The audits identify all individuals who have access to data in CIHI's analytical environment and require management to formally request continued access or removal for each employee, as appropriate. It is important to note that these audits perform a remedial function by including recommendations 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 assess an external data recipient's compliance with the data request form and the Data Protection Agreement or other legally-binding instrument as the case may be such as Data Sharing Agreements. The audits focus on the recipient's use and management of CIHI's data, as well as the recipient's disclosure of findings.

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 set out the purpose of each audit, its nature and scope (i.e., document reviews, interviews, site visits, inspections) and the responsible employee(s). The Terms of Reference details the process for conducting the audit, including criteria for selecting the subject matter, when notification occurs, the content and recipient of the notification, and all documentation required at the outset and conclusion of the audit and to whom it must be provided.

CIHI's Privacy Audit schedule is approved on an annual basis by the Privacy and Data Protection 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.

In order to close the loop on risk management, the Terms of Reference contain a process for managing the recommendations arising from a privacy audit. The Terms of Reference require that Privacy and Legal Services maintain a log of privacy audits, recommendations and relevant information to ensure proper follow-up including complete and timely implementation.

This information is subsequently fed into CIHI's master inventory of corporate 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 Operations Committee. Regular updates will continue to be provided to the Operations Committee chaired by the Director, Corporate Planning and Accountability, until such time as the recommendations are fully implemented.

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

28. Log of Privacy Audits

CIHI's Privacy and Legal Services Secretariat 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
- The status of the audit and subsequently, the date the audit was completed
- The employee(s) responsible for completing the audit.

CIHI's Privacy and Legal Services Secretariat also 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 audit
- The 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.

Both logs above are cross-referenced at all times.

Privacy Breaches, Inquiries and Complaints

29. Policy and Procedures for Privacy Breach Management

PHIPA does not define per se "privacy breaches". It does, however, impose security obligations on health information custodians as contemplated in subsection 12(1) of PHIPA. It reads as follows:

> 12. (1) A health information custodian shall take steps that are reasonable in the circumstances to ensure that personal health information in the custodian's custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the

information are protected against unauthorized copying, modification or disposal. 2004, c. 3, Sched. A, s. 12(1)

Subsection 12(2) further imposes an obligation on health information custodians to notify individuals at the first reasonable opportunity in instances where the information is stolen, lost or accessed by unauthorized persons.

While there are no statutory notification obligations imposed on prescribed entities, CIHI takes a proactive position in this regard. In 2008, CIHI adopted and implemented a *Privacy Breach Management Protocol* that addresses in detail the steps to be taken with respect to the identification, reporting, containment, notification, investigation and remediation of privacy breaches. This is an internal management tool which is intended to enable CIHI to respond to and resolve breaches promptly and effectively. It is also available on CIHI's external website (www.cihi.c) and follows the approach recommended by the British Columbia and Ontario Privacy Commissioners.

The Protocol defines a privacy breach as occurring when personal health information in CIHI's custody or control is accessed, used, copied, modified, disclosed or disposed of in an unauthorized fashion, be it deliberately or inadvertently. A privacy incident is defined as any occurrence that impacts or has the potential to impact or compromise personal health information held by CIHI.

CIHI's *Privacy Breach Management Protocol* makes it mandatory for CIHI employees to immediately report all privacy breaches or suspected privacy breaches or incidents. Moreover, it has been designed to make it easy for employees to do so. CIHI has established a centralized mailbox (Incident@cihi.ca) to which employees are directed to report real or suspected privacy and security incidents or breaches. This ensures that both the Chief Privacy Officer and the Senior Program Consultant, Information Security are informed immediately of any such incident or breach.

The *Privacy Breach Management Protocol* tells employees to include a description of the compromised data, when the privacy breach or suspected privacy breach was discovered, how it was discovered, the location, the cause of the privacy breach or suspected privacy breach (if known), the individuals involved and any other relevant information, and any immediate steps taken to contain the breach or suspected privacy breach.

Upon being notified of a breach or suspected breach, the Breach Response Team is assembled and, working in collaboration with the areas affected by the breach, or suspected privacy breach, implements the Protocol. The Breach Response Team is comprised of the Chief Privacy Officer, the Vice President and Chief Technology Officer, designated Vice-President(s), and others as required. The composition of the Breach Response Team may differ from time to time depending on the circumstances.

The Breach Response Team identifies the compromised data and the affected individuals and/or organizations and jurisdictions. The Breach Response Team notifies the President and CEO of the Breach, or suspected privacy breach, at the earliest opportunity. The President and CEO, in consultation with the Breach response team, determine whether a privacy breach has occurred.

CIHI's *Privacy Breach Management Protocol* also addresses containment in a comprehensive fashion, ensuring that it is clear that containment must begin immediately, where possible.

The following steps are intended to illustrate the actions that may be required to contain the breach or suspected breach (but they are not exhaustive). Individual circumstances will dictate the next steps:

- Ensure that additional privacy breaches cannot occur through the same means (e.g., change passwords, identification numbers, and/or temporarily shut down a system).
- Determine what, if any, data have been stolen, lost or accessed, used, disclosed, copied, modified or disposed in an unauthorized manner.
- Securely retrieve the data to ensure that they are protected against theft and loss and are protected against further unauthorized access, use, disclosure, copying, modification or disposal, or have securely destroyed all or as much of the breached data as possible in order to ensure that reconstruction of the records is not reasonably foreseeable in the circumstances.
- Ensure no copies of the data have been made or retained by the individual or organization involved in the privacy breach or suspected privacy breach.
- Where the data have been securely destroyed rather than being returned to CIHI, obtain confirmation in writing from the individual or organization that the secure destruction has taken place, including the date, time and method of secure destruction employed.
- Determine whether the privacy breach or suspected privacy breach would allow unauthorized access to any other data (e.g., an electronic information system involving multiple databases where other PHI could be compromised) and take whatever steps are necessary and appropriate**.**

The *Privacy Breach Management Protocol* clearly defines CIHI's notification requirements. It is not CIHI's role to notify the individual(s) to whom the breached personal health information belongs. In keeping with its pan-Canadian mandate, where appropriate, CIHI will notify (a) the Privacy Commissioner(s); and/or (b) the Ministry of Health or other data providers of the affected jurisdictions, including health information custodians in Ontario.

The Breach Response Team will discuss notification with the President and Chief Executive Officer. The notification process (i.e., when to notify, how to notify, who should notify, who should be notified, and what should be included in the notification) will be determined 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 Agreements with data providers.

Under the leadership of the CPO, the Breach Response Team is responsible for the investigation of privacy breaches or suspected privacy breaches. Subsequently, the Breach Response Team's investigative reports (which refer to document reviews, interviews, site visits, inspections as the case may be) are submitted to the Senior Management Committee and to any other internal body as deemed necessary. These privacy breaches are also reported to the Privacy and Data Protection Committee of the Board and ultimately to the overall CIHI Board of Directors.

In order to close the loop on remediation and risk management, section 4 of CIHI's *Privacy Breach Management Protocol* contains a process for managing the recommendations arising from a privacy breach. The Vice President of the relevant program area is responsible for ensuring that a plan to implement the recommendations is drafted. The implementation plan shall include prioritized action items with responsibilities and time lines.

CIHI's Privacy and Legal Services Secretariat maintains a log of all privacy breaches and related recommendations. This information is subsequently fed into CIHI's master inventory of corporate 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 Operations Committee. Regular updates will continue to be provided to the Operations Committee until such time as the recommendations are fully implemented.

As indicated above, CIHI's *Privacy Breach Management Protocol* only applies to CIHI. That said, CIHI is committed to safeguarding its data when in the custody and control of external third-party recipients. Third-party data recipients and data-sharing partners who obtain data from CIHI are prompted to notify CIHI at the earliest opportunity of real or suspected breaches through contractual obligations in Data Protection Agreements, Data Sharing Agreements or other legally-binding instruments. CIHI has an unfettered right to audit recipients. CIHI, therefore, monitors compliance by conducting privacy audits of external recipients. The Chief Privacy Officer will determine if a privacy breach has occurred where the privacy of individuals has been compromised, and in all instances regardless of the determination, the Chief Privacy Officer will issue a report containing recommendations in the form of corrective measures when and where required.

When CIHI developed its *Privacy Breach Management Protocol*, it simultaneously developed an *Information Security Incident Management Protocol* which adopts the same four steps to managing security breaches. CIHI's *Information Security Incident Management Protocol* is discussed in greater detail in Part 2 of this Report.

30. Log of Privacy Breaches

CIHI's Privacy and Legal Services Secretariat maintains a log of privacy breaches. The log contains the following elements:

- The date of the breach
- The date that the privacy breach was identified or suspected;
- 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;

- The date that the health information custodian or other Organization that disclosed the personal health information to the prescribed person or prescribed entity was notified;
- The date that the investigation of the privacy breach was completed;
- The employee(s) responsible for conducting the investigation.

CIHI's Privacy and Legal Services Secretariat also 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 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.

Both logs above are cross-referenced at all times.

31. Policy and Procedures for Privacy Questions, 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 questions, concerns or complaints. Questions, 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.

To date, CIHI has never received a privacy complaint.

32. Log of Privacy Complaints

Not applicable – no privacy complaints received. Should CIHI receive a complaint, it would set up a log and document same accordingly.

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 Vice President and Chief Technology 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.

Finally, CIHI is implementing a formalized risk management program within Information, Technology and Services (ITS) that will require regular threat-risk assessments of the Information Security Program. An initial threat-risk assessment has been scheduled in the fourth quarter of 2010/11 to provide CIHI with a baseline for future activities. This will enable ITS management to:

- Prioritize and plan work activities;
- Align ITS risk management activities with enterprise risk management initiatives; and
- Assist with definition of scope for the development of an Information Security Management System aligned with ISO 27001.

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

CIHI's *Information Security Document Management Standard* requires 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. These yearly reviews are conducted on the anniversary of the last review.

The *Standard* requires 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 the Privacy and Legal Services Secretariat as necessary, considers the following, as appropriate:

- 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.

The *Standard* indicates that Document Owners will be 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 Senior Program Consultant, Information Security, 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. Internal communication to staff is guided by the *Privacy and Security Training Policy* which clearly stipulates at sections 4 and 5 that the CPO and CTO 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 Vice President and Chief Technology Officer's portfolio. The inherent benefit to this consolidation is that the organization is better able to identify inconsistencies, gaps or instances of non-conformance to the Senior Program Consultant, Information Security and to document owners.

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 three offices in Ontario (two in Ottawa and one in Toronto), one in British Columbia, one in Quebec and one in Newfoundland and Labrador. 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 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 employees who routinely require such access for their employment, contractual or other responsibilities.

Policy, Procedures and Practices with Respect to Access by 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 employees, including long-term consultants and students. Full access (24/7) to CIHI offices is granted to CIHI employees, long-term consultants and students. Short-term consultants are issued security access cards with restricted access (8:30 a.m. to 5 p.m., Monday to Friday) unless otherwise requested/authorized in writing by the Manager or Director. Short-term consultants are required to complete a Non-Disclosure Agreement setting out their confidentiality obligations in respect of the service they are providing.

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 4:45 p.m. will be provided with a temporary security access card at Reception. Contractors are required to complete a Non-Disclosure Agreement setting out their confidentiality obligations in respect of the service they are providing.

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. 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 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 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 *Departure Checklist* for Managers identifies the necessary steps the Manager must complete before the 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 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 and long-term consultants are programmed to deactivate on the last day of the employment or contractual arrangement with CIHI.

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

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

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

- The name of the employee granted approval to access the premises;
- The name of the employee granted specific approval to access data centres/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 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*, demonstrates 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. One of those administrative safeguards is a clean desk policy in addition to a comprehensive suite of policies, and associated procedures, standards and guidelines that reflect best practices in privacy, information security and records management to ensure the confidentiality, integrity and availability of CIHI's information assets.

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 *Information 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.

In addition, 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 through the use of one of its template agreements, namely an *Independent Contractor Agreement*, a *Master Services Agreement* or a *Standing Offer Agreement*, all of which are consistent with the *Template Agreement for All Third Party Service Providers*.

CIHI's *Information Security Policy* provides that records are transferred and retrieved in the documented secure manner in compliance with CIHI's *Secure Information Transfer Standard*. The requirements for secure transfer are detailed in section 7, below. Information Technology Services maintains a detailed inventory of all electronic information media that are retained by and retrieved from a third party service provider.

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

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

CIHI's *Privacy Policy on the Use of Mobile Computing Equipment* governs, amongst other things, the storage of personal health information on mobile computing equipment. It defines mobile computing equipment as laptops, Universal Serial Bus (USB) flash drives, external hard drives, CDs, DVDs, and other mobile and mass storage devices.

The *Privacy Policy on the Use of Mobile Computing Equipment* is consistent with orders issued under the Act and its regulation, as well as with the various guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner of Ontario and others in Canada[2].

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 risk 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

1. In particular, see sections 19 and 20 – *Agreements with Third Party Service Providers*.
2. See "Protecting Personal Information Outside the Office", February 2005, Office of the Information and Privacy Commissioner for British Columbia

> 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 *Privacy Policy on the Use of Mobile Computing Equipment* sets out as a general rule that work performed by employees is to be done on CIHI premises and/or over its secure networks. The *Policy* states that personal health information will not be stored on mobile computing equipment except for specific and exceptional circumstances. Personal health information temporarily stored on mobile computing equipment will be done on CIHI issued mobile computing equipment, de-identified to the fullest extent possible, and encrypted and password protected.

Approval Process

Prior approval is required by a Vice-President before personal health information can be temporarily stored on mobile computing equipment. 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. This includes a requirement that only the minimum amount of personal health information needed is to be stored on mobile computing equipment and that it is de-identified to the fullest extent possible. 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 computing equipment.

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

In accordance with the *Privacy Policy on the Use of Mobile Computing Equipment*, Information Technology Services is responsible for ensuring that all mobile devices 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 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 computing equipment 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

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

approved requests are documented and tracked by the Privacy and Legal Services Secretariat to ensure secure destruction of the personal health information on mobile computing devices occurs.

Remote Network Access

CIHI's workforce is made up of employees in six offices across the country in addition to Location Independent Workers who work from a home office with an encrypted workstation. As such, CIHI's networks can be accessed remotely through a virtual private network by Location Independent Workers and by other staff who have been assigned a CIHI encrypted laptop computer.

Approval Process

CIHI allows its staff to work remotely over its virtual private network (VPN) under controlled circumstances. All staff requests for personal laptop computers include VPN access and are subject to Director approval. This approval process is managed and documented through the IT Service Management process.

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 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 non-employees;
- The user must connect to CIHI's VPN network as soon as internet connectivity is established;
- The user must ensure they have properly logged off of CIHI's VPN network and the laptop at the end of their working session;
- The user must turn the device off at the end of their working session;
- 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 has developed a *Secure Information Transfer Standard* to ensure appropriate safeguards are implemented for the secure transfer of records of personal health information in both paper

and electronic format. CIHI took into account the 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.

All transfers of personal health information must include the safeguards set out below:

- For electronic transmission including email, only where authorized by the relevant authority and according to CIHI's current encryption standards;
- For information on electronic media, only where authorized by the relevant authority and according to CIHI's current encryption standards;

For paper records, transfer between CIHI offices or to an approved third party service provider, only where authorized by the relevant authority. The authorized employee who is responsible for carrying-out the electronic transfer of personal health information must ensure that CIHI's current encryption standards are followed. For paper records, the Distribution Teams located in the various CIHI offices are responsible to ensure that the packages containing personal health information are double-wrapped, and notification of transfer and confirmation of receipt is documented. Otherwise, CIHI does not permit paper records of personal health information to be sent outside of CIHI.

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

CIHI has mandatory procedures for authorized transfers of personal health information. These procedures set out the conditions under which such transfers are permitted and define the nature and content of the required documentation.

Pursuant to the *Secure Information Transfer Standard*, the employee responsible for transferring records of personal health information is required to document the following elements:

- Date and method of transfer;
- Recipient;
- Nature of the records; and
- Confirmation of receipt.

More specifically, CIHI's *Privacy Policy Procedures* -- Preferred Methods of Dissemination ensure that all transfers of personal health information obtain prior approval at the Manager or Director level.

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 *Information 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 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 media contained in the device has been securely wiped of all information in accordance with CIHI's *Information 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 *Information 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 centres 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.

In the event that electronic media must be transported to a different location for destruction, CIHI ensures that care is taken to guard against loss or theft, as well as unauthorized access, disclosure, copying, use or modification. All electronic media destined for transport is first degaussed using approved methods.

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

1. Physical Destruction
2. Degaussing
3. Complete secure data wipe of hard drive
4. Selected secure data wipe of individual files and folders

Destruction by a Designated 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:

- Physical destruction of removable media such as CDs, DVDs;
- Complete wipe of desktop or laptop hard drive prior to resale or repair
- Degauss hard drive prior to transfer to a 3rd party for physical destruction
- Selective wipe of hard drive upon request for destruction of specific electronic files

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:

- 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 *Information 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 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.

There are two instances where CIHI receives personal health information in paper form. They are submissions to the Canadian Organ Replacement Register (CORR) and the Canadian Joint

Replacement Registry (CJRR). These paper records are not placed in the general locked shredding bins for destruction as described above nor are they destroyed along with other confidential information. Specifically, personal health information contained in paper form related to both the CORR and CJRR are stored in access-controlled areas within CIHI premises and CIHI tracks and keeps a description of the records to be securely destroyed.

When such documents are no longer required, they are gathered by the designated CORR/CJRR employee who also notifies the Records Management team that they have such records ready for destruction. These records are kept in the departmental secure area until the third party service provider is on site to perform regular paper destruction services (typically every two weeks). These services are provided on-site. The CORR/CJRR personnel accompanies the records and witnesses the destruction process. In these instances, a Certificate of Destruction is used which documents the level of detail required by the IPC as set out in the IPC Manual.

Destruction of Electronic Information by a Third Party Service Provider

At CIHI, physical destruction of hard drives is performed by a third party service provider. Prior to transport to the service provider, all hard drives are degaussed according to CIHI's *Information Destruction Standard*. 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*. A Certificate of Destruction is not required in this particular instance because information is securely destroyed prior to turning over the hard drives to the third party service provider for destruction.

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. Its *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 3 different categories. Moreover, the Standard also establishes the default password periodicity, for example, passwords must be changed 45 days after the previous password has been registered, and passwords must be different from the previous 24 passwords that have been registered. CIHI systems will automatically reject passwords that do not comply with the Standard where technology permits. In addition, other measures in place include locked access after 3 failed attempts to input the correct password, and Password access is required to access the system after10 minutes of inactivity because a system-wide locked screen-saver is automatically

triggered. Passwords are specific to an individual and traceable to that individual. 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.

The *Standard* mandates the following administrative, technical and physical safeguards to be implemented by employees:

- Passwords may not be written down;
- Passwords may not be shared with anyone under any circumstances – and 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 *Information 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 recognizes that system control and audit logs are a critical component of its Information Security Program. CIHI's system control and audit logs are immutable. CIHI's system control and audit logs are applied uniformly to all data holdings across the organization. CIHI logs the nature and scope of the information accessed in addition to the following:

- All externally-facing applications involving personal health information (for example, CIHI Portal, CIHI's e-Reporting applications such as e-CHAP, e-NACRS, e-NRS, etc.)[4];
- Employee access to sensitive data elements such as health card number, chart number, date of birth, name (where applicable) and full postal code within CIHI's operational production databases; and
- Employee access to data files extracted from CIHI's operational databases and made available to the internal analytical community.

The Vice President and Chief Technology Officer is responsible for ensuring that the types of events that are required to be audited are in fact audited and that the nature and scope of the information that is required is in fact logged. Also, at CIHI the most recent 18 months of system control and audit logs are immediately accessible, and the past 7 years are retained on tape back-up. The *InfoSec Audit Policy* and the related procedures govern, amongst other things, the following:

[4] e-CHAP (electronic Comparison of Hospital Activity Program), e-NACRS (National Ambulatory Care Reporting System web-based comparative reporting), e-NRS (electronic National Rehabilitation Reporting System) are e-tools whereby CIHI clients can securely access CIHI data and generate reports in a controlled environment.

- the review of the system control and audit logs;
- the findings arising from the review;
- the nature of documentation following the review;
- how the findings are communicated; and
- how the findings are tracked.

For the most part, analytical activities are performed using encrypted health card numbers. CIHI's Privacy Policy Procedures 10.10 to 10.19 set out the limited and exceptional circumstances where access to unencrypted health card numbers is permitted.

11. Policy and Procedures for Patch Management

CIHI has a Patch Management Policy pursuant to which designated owners of information processing assets monitor the availability of patches on behalf of CIHI and are responsible for maintaining 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 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 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:

- Very High – next business day
- High – 2 business days
- Medium – 5 business days
- Low – Scheduled in next available maintenance window
- Very Low – Scheduled in future maintenance window.

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 approval 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).

Change Managers and the CAB follow a detailed, documented process for arriving at a determination to approve or deny a request for a change. Requestors must complete a Request for Change (RFC) and provide it to the Change Analyst. The Change Analyst reviews the RFC, validates that it can be accomplished as requested, determines the category and priority using the Change Management Categorization Model and the Change Management Prioritization Model, and updates the request with additional required information. The RFC contains the following:

- 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.

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 Change Analyst is identified in CIHI's *Global Process Policies for Change Management* as 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.

At CIHI, implementation of changes to the operational environment is governed by the Technology Change Management (TCM) process. The Change Analyst is responsible for ensuring

all changes are tested. Testing protocols are dependent on the nature and scope of the change and are executed according to the deployment instructions in the TCM request.

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

- A description of the change;
- The name of the employee who requested the change;
- The date the change was implemented;
- The employee responsible for implementing the change;
- The date, if any, the change was tested;
- The 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 Standard* and associated 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 Standard* and associated 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. Pursuant to it, the Manager of Infrastructure Technology is designated as responsible for these processes. The *Secure Information Backup Standard* also requires that such back-up storage devices are encrypted and are stored and transported securely. At CIHI, the Senior Network Analyst is responsible to ensure that all transfers and retrievals of backed-up records are carried out in the documented secure manner as set out in both CIHI's *Secure Information Backup Standard* and its *Secure Information Transfer Standard as described in section 7, above*, and that 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 also 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 Technology is responsible for auditing backup tape validity, backup tape integrity and completeness in accordance with the procedures contained therein.

CIHI contracts with a third party service provider to retain backed-up files, 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 *Template Agreement for All Third Party Service Providers*.

14. Policy and Procedures on the Acceptable Use of Technology

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

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, 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

Security audits are a key component of CIHI's overall security program. In accordance with CIHI's *Information Security Audit Policy*, CIHI has developed and implemented an audit program based on the following criteria that assesses:

- 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 access to information or information processing systems;
- Inappropriate use of 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.

In addition to the specified audits, the Policy also states that CIHI may, from time-to-time, perform additional audits 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 Vice President and Chief Technology Officer.

CIHI's *Information Security Audit Procedure Manual* includes a list of all audits that must be performed. This list acts as a form of internal notification. In addition, for each mandatory audit, it includes the following:

- 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;
- All audit activities are ultimately reported to the Vice President and Chief Technology Officer on a quarterly basis in the form of audit summaries which may or may not include recommendations, as the case may be;
- All recommendations are logged and tracked, action plans are developed within 30 days.

The Vice President and Chief Technology Officer will report, from time to time, the findings of security audits. Security audits that are commissioned and conducted by external third parties are reported in every instance to CIHI's Senior Management Team headed by the President and Chief Executive Officer, in addition to CIHI's Finance and Audit Committee.

The Senior Program Consultant, Information Security is responsible for providing oversight to the Information Security Audit Program, and ensuring the results of information security audits are reported to the Vice President and Chief Technology Officer. Recommendations contained in audit reports are tracked in the *InfoSec Recommendation Log* and an action plan is defined to address each recommendation within 30 days of the audit report. In all cases where CIHI elects not to accept a recommendation, justification and formal acceptance of risks must be documented.

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 fed into CIHI's master inventory of corporate action plans that are monitored and reported on at the corporate level to CIHI's Operations Committee. The Senior Program Consultant, Information Security is responsible for documenting the recommendations and the actions taken (or planned) to address each recommendation and to provide regular updates to the Operations 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 employee(s) responsible for completing the audit; and
- The recommendations arising from the audit.

The *Information Security Recommendation Log* includes:

- The 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 Information Security Breach Management

CIHI has an *Information Security Incident Management Protocol* to address the identification, reporting, containment, notification, investigation and remediation of information security incidents and breaches. The *Protocol* defines an information security incident as "*any occurrence that impacts or has the potential to impact the confidentiality, integrity or availability of CIHI's electronic information assets OR any occurrence that compromises, or has the potential to compromise, CIHI's information security controls."* The *Protocol* defines an information security breach as "*any occurrence that results in the compromise of CIHI's information security controls."* If a breach of policy, procedures or practice has "*the potential to impact the confidentiality, integrity or availability of CIHI's electronic information assets or CIHI's information security controls*" – this would amount to a information security incident and the Protocol would be triggered. Furthermore, CIHI's *Information Security Policy* makes it mandatory to report all information security incidents.

Employees are required to report any information security incident immediately. As described in Part 1 of this Report, section 29, *Policy and Procedures for Privacy Breach Management*, CIHI has established a centralized mailbox (Incident@cihi.ca) to which employees are directed to report real or suspected privacy and security incidents or breaches. This ensures that both the Chief Privacy Officer and the Senior Program Consultant, Information Security are informed immediately of any such incident or breach.

Furthermore, the *Protocol* instructs staff involved in any step of Information Security Incident Management to maintain a concise record of all communications and activities, including details of the incident, dates, times, actions, decisions, and so on.

Upon being notified of an incident, the Incident Response Team is assembled and, working in collaboration with the areas affected by the incident implements the Protocol. The Incident Response Team will:

- Determine whether or not the Privacy Breach Management Protocol should be invoked;
- Advise the Incident Owner on matters of incident containment and management;
- Determine internal and external communication requirements, including reporting the incident to the President and CEO.

The specific composition of the Incident Response Team will depend on the nature of the incident, however at minimum, the following staff (or their designates) are typically included:

- Vice President and Chief Technology Officer
- Chief Privacy Officer
- Senior Program Consultant, Information Security
- Management / Senior Management representation from all affected program areas within CIHI
- Management / Senior Management representation from all affected ITS departments or branches

It bears repeating that immediately upon being assembled, the Incident Response Team shall determine whether or not to invoke the *Privacy Breach Management Protocol*. In all cases where personal health information is at risk, the Privacy Breach Protocol must be invoked.

The Senior Program Consultant, Information Security is assigned initial ownership of all Information Security incidents, however, any member of the ITS management team or the Incident Response Team may act as designated owner. The Incident Response Team or the Incident Owner may identify the need for an extended response team. This team may comprise various subject matter experts and others who may assist with decision making, containment or communication activities. Employees are expected to cooperate fully with the Incident Response Team.

CIHI's *Information Security Incident Management Protocol* requires that containment and preliminary assessment begin immediately. The goal of assessment is to determine what immediate actions, if any, are required in response to the incident and will consider extent of actual damage, potential for damage and communication requirements. Containment measures may include shutting down applications or services.

The Incident Response Team, along with others as deemed necessary, determines internal and external communication requirements.

An investigation is commenced at the earliest opportunity. The incident owner is responsible for managing the necessary activities to determine the root cause of the incident. Once the root cause of the incident has been ascertained, the incident owner, with the support of the Incident Response Team, manages the remediation activities. An Information Security Incident report is produced (which refers to document reviews, interviews, site visits and inspections, as the case may be) for all Information Security incidents where security controls have been compromised or any time the Incident Response Team deems it necessary. The Information Security Incident report recommendations are presented to the Incident Response Team and to any affected stakeholders within 45 days of the completion of the analysis and remediation activities.

All recommendations are entered and tracked in the *Information Security Recommendation Log*. The Senior Program Consultant, Information Security is responsible for tracking all recommendations entered in the *Log*, and for ensuring appropriate lessons-learned activities are undertaken with the participation of all relevant staff.

CIHI is committed to fully understanding the events that contribute to information security incidents in order to take permanent remediation steps and to continually improve CIHI's privacy and security posture.

The *Information Security Incident Management Protocol* is an internal management tool which is intended to enable CIHI to respond to and resolve breaches promptly and effectively. It is also available on CIHI's external website (www.cihi.ca). In the case of external third-party data recipients and third-party service providers, these parties are prompted to notify CIHI at the earliest opportunity of real or suspected breaches through contractual obligations, amongst other things. CIHI also reserves the right to audit third-parties as a means of monitoring compliance.

18. Log of Information Security Incidents

CIHI's Senior Program Consultant, Information Security maintains a log of information security incidents. The log contains the following elements:

- The date of the incident;
- The date that the information security incident was identified or suspected;
- The nature and extent of the incident;
- The date that the information security incident was contained and the nature of the containment measures;
- The date that the investigation of the information security incident was completed;
- The employee(s) involved in conducting the investigation;
- The recommendations arising from the investigation;
- The 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.

Part 3 - Human Resources Documentation

Privacy and Security Training and Awareness

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

CIHI's *Privacy and Security Training Policy* sets out the requirements for traceable, mandatory privacy and security training for all CIHI staff. Pursuant to the *Policy*, new 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*. Currently, the initial mandatory privacy and security orientation training comprises the following modules:

- Privacy and Security Fundamentals;
- CIHI Privacy Breach and InfoSec Incident Management Protocols.

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 Vice President and Chief Technology 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 employees on their first day of employment. The mandatory privacy and security training is referenced and explained within this session. The mandatory privacy and security training is tracked by the business process management workflow tool CIHI uses to initiate and manage the on-boarding process for all new hires.

CIHI is in the process of upgrading its on-boarding and off-boarding process for all new hires as well as for external professional services consultants who must also meet mandatory training

1. New-hires include all full-time, part-time and contract employees of CIHI, individuals working at CIHI on secondment, students and external professional services consultants.

requirements, to ensure that the training is completed within the timeframe set out in CIHI's *Privacy and Security Training Policy*. This upgrade is expected to be operational as of April 2011.

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 employees;
- The procedure that must be followed in the event that an 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 Vice President and Chief Technology Officer and Senior Program Consultant, Information Security
- 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 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 employees must execute and the key provisions of the Confidentiality Agreement; and
- An explanation of the *Privacy Breach Management Protocol* and the duties and responsibilities imposed on employees in identifying, reporting, containing and participating in the investigation and remediation of privacy breaches.
- An explanation of the *Information Security Incident Management Protocol* and the duties and responsibilities imposed on employees in identifying, reporting, containing and participating in the investigation and remediation of information security breaches.

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 Vice President and Chief Technology 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 CTO 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. The Privacy and Legal Services Secretariat is responsible for maintaining the log, and for ensuring compliance across the organization. CIHI's on/off-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. Tracking functionality also forms part of the upgrade that will be in place as of April 2011.

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 *CIHIway* (CIHI's intranet-based employee communication mechanism);
- staff presentations and special presentations at departmental meetings;
- "*January is Privacy Awareness Month at CIHI*" campaign;
- "*September is Information Security Awareness Month at CIHI*" campaign;
- SmallTalks (lunch and learns);
- privacy and security awareness posters and mouse pads;
- 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

The Privacy and Legal Services Secretariat maintains an electronic log of the completion dates for all employees of new mandatory privacy and security training. The upgraded system will be in place as of April 2011.

Confidentiality Agreement

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

CIHI requires all 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, for the first time in January 2010, employee renewal was recorded electronically. One hundred per cent completion by the end of January is required and is ensured by monitoring and direct follow-up with employees. Amongst other things, the renewal states that 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 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, in fact, executed for each new employee. For example, a checklist is followed and is sent to new employees. The Human Resources Generalist follows up with a reminder to the employee, if necessary, to sign and return the Confidentiality Agreement. Finally, the Human Resources Generalist 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 employee file.

4. Template Confidentiality Agreement with 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 as previously indicated at page 34 of this Report; 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 the following template Certificate of Destruction based on the Commissioner's requirements[2], to be used where appropriate:

[2] Dr. Ann Cavoukian, Robert Johnson, *Best Practices for the Secure Destruction of Personal Health Information*, October 29, 2009, http://www.ipc.on.ca/images/Resources/naid.pdf

Canadian Institute for Health Information

Institut canadien d'information sur la santé

Certificate of Destruction

I hereby certify that the **original media containing** CIHI STAFF INSERT HOLDING, YEARS FROM DATA REQUEST DOCUMENTATION provided to me by CIHI, have been duly and securely destroyed such that reconstruction is not reasonably foreseeable.

In addition to the destruction of the original media containing CIHI STAFF INSERT HOLDING, YEARS FROM DATA REQUEST DOCUMENTATION I hereby certify that **all copies** of the data obtained from CIHI, reproduced, located, stored or found on servers, hard drives, CDs/DVDs, USB keys, laptops, paper, and any other format, device or media regardless of location, have also been duly and securely destroyed such that reconstruction is not reasonably foreseeable.

The description of destruction methodologies employed contained in **Schedule A and Schedule B, forms part of this Certificate of Destruction**.

Where the destruction of data has been executed by an external third party, that party's Certificate of Destruction is appended hereto and forms part of this Certificate of Destruction.

Note: Double-click form box (_____) to type or paste response.

Name (Researcher/Title)	Organization
Signature	Date
Name/Title (Information or Chief Technology Officer or equivalent senior position)	Organization
Signature	Date

5. Log of Executed Confidentiality Agreements with Employees

CIHI does not maintain a separate log of executed Confidentiality Agreements. As described in section 3 above, Human Resources has a process in place to ensure that a properly executed Confidentiality Agreement is obtained and placed in the every employee's file. With respect to the annual renewal of Confidentiality Agreements, tracking is recorded electronically and 100% completion ensured by monitoring and direct follow-up with 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.

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 employees are aware of the Act and its regulation and their duties thereunder;
- Ensuring 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 Breach Management Protocol*; and
- Conducting privacy audits pursuant to the Privacy Audit Program – Terms of Reference.

7. Job Description for the Vice President and Chief Technology Officer

At CIHI, the Vice President and Chief Technology Officer has overall responsibility for Information Security and ensures that information security goals are identified, that they meet organizational requirements and that they are addressed within the Information Security Program. The Vice President and Chief Technology Officer has delegated responsibility for the day-to-day management of the organization's Information Security Program to the Senior Program Consultant, Information Security. The Senior Program Consultant, Information Security, ensures that all Information Security practices and procedures comply with CIHI's policies and legislative requirements, and follow current best practices in Information Security management. The Vice President and Chief Technology Officer reports directly to the President and CEO.

The job description for the Vice President and Chief Technology 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 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 *Information Security Incident Management Protocol*; and
- Conducting security audits pursuant to the *Information Security Audit Policy*.

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 BPM team are notified of any 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 sending out a last day email to the above-mentioned teams to notify them that an employee is leaving CIHI, as well as submitting a Service Desk request to inform the Information Technology team of the employee's last day in the office.

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

The on/off-boarding process sets out the Manager's roles and responsibilities to ensure the effective termination of their employee. A *Departure Checklist* for managers forms part of the process and sets out the necessary steps that the Manager must complete before the employee's last day. Should CIHI property not be duly returned by the departing employee, the Director of Human Resources and Administration[3] 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 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 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 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 employees. This Division has a set of policies and procedures that ensure such employment-related issues within the organization are dealt with effectively.

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

Part 4 - Organizational and Other Documentation

Governance

1. Privacy and Security 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 Vice President and Chief Technology Officer, who reports to the President and CEO, has been delegated day-to-day authority to manage the security program and describes the responsibilities and obligations of the Chief Technology Officer. It illustrates that both CIHI's Chief Privacy Officer and Chief Technology 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 Privacy and Data Protection Committee of the Board. This committee represents accountability at the highest possible level, overseeing the privacy program and reviewing 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 Technology Officer.

The Privacy and Data Protection 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 comprised of the President and CEO, Vice-Presidents, Executive Directors and the Vice President and Chief Technology Officer
- Senior Management Committee
  - Chaired by the President and CEO, and comprised of Executive Committee members and all Directors
- IT Operations Committee
  - Chaired by the Vice President and Chief Technology Officer
- Privacy, Confidentiality and Security Team
  - Chaired by the Chief Privacy Officer
- Security Management Group
  - Chaired by the Senior Program Consultant, Information Security

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

2. 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

3. Corporate Risk Management Framework

CIHI has developed and implemented a Corporate 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, as well as 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 Corporate 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.

4. Corporate Risk Register

CIHI's corporate risk register identifies each risk that may negatively affect CIHI's ability to deliver on its strategic directives.. 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;
- Employee responsible for the implementation

5. 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 Secretariat 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 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 inventory of corporate 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 CIHI's Operations Committee[1]. Regular updates will continue to be provided to the Operations Committee until such time as the recommendations are addressed.

The Vice President and Chief Technology Officer, through the office of the Senior Program Consultant, Information Security, 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. A monthly report is tabled by the Senior Program Consultant, Information Security, at the Security Management Group[2]. Recommendations resulting from security audits conducted by an independent third party (e.g. vulnerability assessments and penetration testing) are included in the master inventory of corporate action plans, are monitored and reported on at the corporate level.

6. 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 inventory of corporate 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

1. Operations Committee is chaired by the Director of Corporate Planning and Accountability, and is comprised of CIHI's Vice Presidents, the Director of ITS Applications and Web Services, the Manager of Publications and Translation and the Manager, Planning and Project Management Office.
2. Security Management Group is chaired by the Senior Program Consultant, Information Security and is comprised of senior technical resources from ITS.

- The employee responsible for addressing the recommendation.

Business Continuity and Disaster Recovery

7. 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:

i) Notification of the Interruption – roles and responsibilities, the contact list, timeframes, and form of notification

ii) Assessment of the Severity of the Interruption – roles and responsibilities, criteria for assessment and documentation, initial impact assessment, a detailed damage assessment

iii) Resumption and Recovery – activation of the business continuity and disaster recovery plan, an inventory of all critical applications and business functions, procedures for recovery of every critical application and business function, prioritization of recovery activities, recovery time objectives, roles and responsibilities

iv) Governance During an Event – the procedure by which decisions are made by the Business Continuity Management Team

v) 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 employees.

The Business Continuity Coordinator is responsible for managing all communications to employees during an interruption or threat event.

PHIPA Review – Indicators

(Current as of October 31, 2011)

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 and Confidentiality of Health Information at CIHI: Principles and Policies for the Protection of Personal Health Information, 3rd Edition – Revoked March 2010 ▪ New *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 December 2010 and March 2011 ▪ Privacy Policy Procedures first adopted July 2010; reviewed December 2010 and March 2011 ▪ *Privacy and Security Framework* first adopted February 2010; reviewed December 2010 and March 2011 ▪ *Privacy and Security Training Policy* first adopted September 2009; reviewed December 2010 ▪ *Privacy Impact Assessment Policy* first adopted April 2009; reviewed December 2010 ▪ *Privacy Breach Management Protocol* first adopted June 2008; reviewed December 2010 ▪ *Privacy Policy on the Use of Mobile Computing Equipment*, first adopted February 2008; reviewed December 2010
	▪ Whether amendments were made to existing privacy policies and procedures as a result of the review, and if so, a list of the amended privacy policies and procedures and, for each policy and procedure amended, a brief description of the amendments made.	▪ *Privacy Policy, 2010*, amended December 2010 and March 2011 ▪ Privacy Policy Procedures amended December 2010, March 2011 and July 2011 ▪ *Privacy and Security Framework*, amended December 2010 and March 2011 ▪ *Privacy and Security Training Policy, amended*

Categories	Privacy Indicators	CIHI Indicators
		December 2010 ▪ *Privacy Impact Assessment Policy*, amended December 2010 ▪ *Privacy Breach Management Protocol*, amended December 2010 and March 2011 ▪ *Privacy Breach Management Protocol, amended October 2011* Documents available on request.
	▪ 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.	▪ Yes, see above.
	▪ 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, SmallTalks, targeted presentations and the like. The communication strategy for all documents that have been amended or created as a result of this review is in progress and will be completed by October 31, 2011. To date, the following communications have been delivered: ▪ *Privacy Policy, 2010*, general communication to CIHI staff in March 2010, followed-up with training sessions given by the CPO for managers and for all staff ▪ Three on-line mandatory training modules for all employees – (1) *Privacy and Security Fundamentals (January 2010); (2)* CIHI *Privacy Breach and InfoSec Incident Management Protocols* (October/November 2010); and (3) *Privacy and Security Framework –Privacy Awareness Month Training Module (*January 2011*);* ▪ Developed and circulated to all staff two Privacy Interpretation Bulletins: (1) Use of Data for Educational Material (September 2010) and (2) Return of Own Data (February 2011) ▪ *Privacy Breach Management Protocol* - email to CIHI Senior Managers and Managers to advise them of a change to the definition of a privacy breach to include

Categories	Privacy Indicators	CIHI Indicators
		unauthorized copying or modification of personal health information ▪ *Privacy Breach Management Protocol* – email to all staff to advise them of a change to the definition of a privacy breach to include unauthorized copying or modification of personal health information, including examples ▪ *Privacy Policy Procedures* – article in CIHiway notifying CIHI staff of availability of amended procedures and a general description of those changes ▪ *Privacy Breach Management Protocol* – article in CIHiway notifying all staff of the addition of a definition of a privacy incident to the Protocol and their responsibility to report privacy incidents to Incident@cihi.ca
	▪ 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 Breach Management Protocol*, *Privacy Impact Assessment Policy*, *Privacy and Security Training Policy*, and *Privacy Policy on the Use of Mobile Computing Equipment* 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 has 15 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 data holdings are made publically available on CIHI's external website
	▪ 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 October 2008, CIHI has updated 12 PIAs for data holdings containing personal health information ▪ CIHI renews annually its *Products and Services Guide* which includes a description of data holdings containing personal health information
	▪ 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. CIHI collects, uses and discloses personal health information in a manner consistent with section 45(1) of PHIPA and its mandate and core functions as described in sections 1 and 2 of its Privacy Policy, 2010.
Use	▪ The number of agents granted approval to access and use personal health information for purposes other than research.	▪ As of October 2011, 338 agents have approval to access and use personal health information at CIHI.
	▪ The number of requests received for the use of personal health information for research since the prior review by the Information and Privacy Commissioner of Ontario.	▪ N/A
Disclosure	▪ 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.	▪ N/A
	▪ 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 (1) Statistics Canada (2) Cancer Care Ontario (3) ICES (4) The Registry of the Canadian Stroke Network ▪ Ontario facilities - return of own data
	▪ 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.	▪ For requests granted, see above.
	▪ 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.	▪ Three (1) Bloorview Research Institute (consent based) (2) Hospital for Sick Children (Electrolyte Study (consent based)

Categories	Privacy Indicators	CIHI Indicators
		(3) Hospital for Sick Children (Eating Disorder Study (section 44).
	▪ 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.	▪ All three requests above are currently in progress.
	▪ 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.	▪ None. The three requests are currently being processed and none of the three Research Agreements referenced above has yet been executed.
	▪ 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.	▪ 2008-09: 314[1] ▪ 2009-10: 336[1] ▪ 2010-11: 413[1] ▪ 2011-12: (Q1 – Q2) 236[1]
	▪ The number of acknowledgements or agreements executed by persons to who 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.	▪ See above.
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.	▪ Cancer Care Ontario (August 2010)
	▪ 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.	▪ Statistics Canada (February 2011) ▪ Cancer Care Ontario (January 2009) ▪ ICES (July 2009) ▪ Registry of the Canadian Stroke Network (November 2008)
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.	▪ None

1. Data requests are not exclusive to Ontario data. Also, numbers do not include requests for aggregate data available to the public through Quick Stats on CIHI's website.

Categories	Privacy Indicators	CIHI Indicators
Data Linkage	▪ The number and a list of data linkages approved since the prior review by the Information and Privacy Commissioner of Ontario.	▪ 43 linkages ▪ See attached log of *Approved Data Linkages*
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 2008, 12 Privacy Impact Assessments have been completed ▪ See attached *Privacy Impact Assessment Log* and *Summary of Recommendations*
	▪ 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.	▪ Six (1) Primary Health Care Voluntary Reporting System (New) 2011/12 (2) National Trauma Registry/Ontario Trauma Registry (Update) 2011/12 (3) Clinical Administrative Databases (Update) 2011/12 (4) MS Monitoring System (New) 2012/13 (5) Patient Cost Database (New) 2011/12 (6) Continuing Care Reporting System (Update) 2011/12
	▪ 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.	▪ See attached *Privacy Impact Assessment Log*.
	▪ 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.	▪ One – PIA for Therapeutic Abortions Database: As there is no longer a requirement to maintain a discrete database of therapeutic abortion data, a separate privacy impact assessment is not required. No further updates to the *2003 Privacy Impact Assessment of the Therapeutic Abortions* Database, therefore, will be reported. Should the situation change in the future, CIHI will address the requirement for a privacy impact assessment in accordance with its *Privacy Impact Assessment Policy*.

Categories	Privacy Indicators	CIHI Indicators
	▪ 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.	▪ Two (1)2008 CIHI Portal Services PIA: 2008/09 Addendum and 2010/11 Addendum (in progress) (2) 2009 Canadian Organ Replacement Registry PIA: CORR WAVE Addendum (in progress)

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.
	▪ 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 2008, CIHI has completed ten privacy audits. ▪ See attached *CIHI's Privacy Audit Program*
Privacy Breaches	▪ The number of notifications of privacy breaches or suspected privacy breaches received by the prescribed person or prescribed entity since the prior review by the Information and Privacy Commissioner of Ontario.	▪ None
	▪ With respect to each privacy breach or suspected privacy breach: – The date that the notification was received, – The extent of the privacy breach or suspected privacy breach, – Whether it was internal or external, – The nature and extent of personal health information at issue, – The date that senior management was notified, – The containment measures implemented, – 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,	▪ N/A

Categories	Privacy Indicators	CIHI Indicators
	– 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.	▪ 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 – The date of the letter to the individual who made the privacy complaint and a brief description of the content of the letter.	▪ N/A

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, last reviewed September 2011 ▪ *Acceptable Use of Information Systems Policy*, first adopted December 2008, last reviewed September 2011 ▪ *Secure Destruction Policy,* first adopted March 2010, last reviewed September 2011 ▪ *Patch Management Policy,* first adopted March 2010, last revised May 2011 ▪ *InfoSec Audit Policy,* first adopted December 2010 ▪ *Security and Access Policy*, first adopted March 2008, last revised December 2010 ▪ *InfoSec Audit Procedure Manual,* first adopted December 2010 ▪ *File Encryption Standard,* first adopted May 2008, last reviewed June 2011 ▪ *Username and Password Standard,* first adopted October 2008, last reviewed November 2010 ▪ *Information Security Incident Management Protocol,* first adopted November 2008, last reviewed December 2010 ▪ *Information Security Document Management Standard,* first adopted October 2010 ▪ *Information Destruction Standard,* first adopted May 2009, last reviewed December 2010 ▪ *Third Party Technical Information Disclosure Standard*, first published September 2009, last reviewed June 2011 ▪ *COTS Product Technical Requirements Standard,* first published February 2010, last reviewed July 2011 ▪ *Manual Changes to Production Data*, first published October 2010 ▪ *Health Data Collection Standard,* first published November 2010

Categories	Security Indicators	CIHI Response
		▪ Document Management Standard, first published December 2010 ▪ *Secure Storage Standard,* first published November 2010 ▪ *Secure Transfer Standard,* first published November 2010 ▪ *Secure Information Backup Standard*, first published November 2010 ▪ *Anti-Malware Strategy*, first published December 2010 ▪ *Responding to Malware Procedure*, first published October 2009, last reviewed September 2011 ▪ *Safe Email and Browsing Guideline*, first published December 2008, last revised February 2010, last reviewed September 2011 ▪ *Email Etiquette Guidelines, first published December 2008, last reviewed September 2011* ▪ *FAQ – Acceptable Use Policy*, first published December 2008, last reviewed September 2011
	▪ 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.	▪ See above. Documents available on request.
	▪ 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.	▪ See above
	▪ 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 to those staff that are impacted by the change. Communication mechanisms include CIHI's intranet, SmallTalks, targeted presentations and the like. The communication strategy for all documents that have been amended or created as a result of this review is in progress and will be completed by October 31, 2011. To

Categories	Security Indicators	CIHI Response
		date, the following communications have been delivered: ▪ *Acceptable Use of Information Systems Policy* – presentation to CIHI Privacy Practice Group, November 2008 ▪ *Acceptable Use of Information Systems Policy* – presentation to Architecture and Standards Department January 2009 ▪ *Acceptable Use of Information Systems Policy* – presentation to Analytical Systems Department February 2009 ▪ *Information Security Policy* and *Acceptable Use of Information Systems Policy* – presentation to Continuing and Specialized Care Information Services Department (Toronto), July 2009 ▪ *Information Security Policy* and *Acceptable Use of Information Systems Policy* – presentation to Continuing and Specialized Care Information Services Department (Ottawa), August 2009 ▪ *Technical Information Disclosure Standard* – email to all ITS staff, September 2009 ▪ *Acceptable Use of Information Systems Policy* – email to all staff regarding "pirated" internet content provisions, July 2010 ▪ *Acceptable Use of Information Systems* – SmallTalk as part of Information Security Awareness Month, September 2010 ▪ *Privacy Breach Management* and *Information Security Incident Management* - SmallTalk as part of Information Security Awareness Month, September 2010 ▪ On-line mandatory training to all staff – October/November 2010 on CIHI *Privacy Breach and InfoSec Incident Management Protocols* ▪ Intranet communication to all staff with regard to updated policies, procedures and standards as a result of the PHIPA Review process, March 2011 ▪ *Introduction to the Secure Information Lifecycle* –

Categories	Security Indicators	CIHI Response
		SmallTalk as part of Information Security Awareness Month, September 2011 ▪ *Secure Lifecycle Phases: Creation/Acquisition and Retention and Storage* – SmallTalk as part of Information Security Awareness Month, September 2011 – Relevant documents: Health Data Collection Standard, Secure Information Backup Standard, Secure Storage Standard, File Encryption Standard, Security and Access Policy (Clean Desk) ▪ *Secure Lifecycle Phase : Access/Use/Disclosure* – SmallTalk as part of Information Security Awareness Month, September 2011 – Relevant documents: File Encryption Standard, Secure Transfer Standard, Security and Access Policy ▪ *Secure Lifecycle Phase – Disposition* – SmallTalk as part of Security Awareness Month, September 2011 – Relevant documents: Secure Destruction Policy, Secure Destruction Standard
	▪ 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 and Security Framework* posted on CIHI's external website (www.cihi.ca)
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.	▪ 2010 *Physical Threat and Risk Assessment* (see attached summary of 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 below for details.
	▪ 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*
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 2008, CIHI has logged 250 information security incidents. (Notes: (1) As defined in CIHI's *Information Security Incident Protocol,* not all incidents necessarily impact data under CIHI's control, and may or may not involve Ontario data. (2) Information Security Incidents are defined broadly and include such circumstances as computer viruses, discovered weaknesses in infrastructure, etc.)
	▪ With respect to each information security breach or suspected information security breach: – The date that the notification was received, – The extent of the information security breach or suspected information security breach, – The nature and extent of personal health information at issue, – The date that senior management was notified, – The containment measures implemented, – The date(s) that the containment measures were implemented, – The date(s) that notification was provided to the health information custodians or any other organizations, – The date that the investigation was commenced,	▪ For any security incident where personal health information is compromised, the Privacy Breach Management Protocol is triggered. See Part 1 – Privacy Indicators.

Categories	Security Indicators	CIHI Response
	– 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.	

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.	▪ 100% completed - mandatory training requirements
	▪ 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 must complete mandatory privacy and security training 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
	▪ 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.	▪ January 2009 – introduction of the Privacy and Security poster campaign "January is Privacy Awareness Month at CIHI" ▪ September 2009 – introduction of the Privacy and Security poster campaign " September is Information Security Awareness Month at CIHI" ▪ Ongoing awareness poster and mouse-pad campaign related to CIHI's Privacy and Security Breach Protocols ▪ Every January and September, CIHI staff receive communication and training, in addition to ad hoc communication and training all year round. For example: ▪ A general communication to CIHI staff in March 2010, on CIHI's new *Privacy Policy, 2010*, followed-up with training sessions given by the CPO for managers and for all staff; ▪ Three on-line mandatory training modules for all employees – (1) *Privacy and Security Fundamentals (January 2010); (2)* CIHI *Privacy Breach and InfoSec Incident Management Protocols* (October/November 2010); and (3) *Privacy and Security Framework* –

Categories	Privacy Indicators	CIHI Response
		*Privacy Awareness Month Training Module (*January 2011*);* ▪ September 2011 – four SmallTalks on the Secure Information Lifecycle as part of Security Awareness Month ▪ Developed and circulated to all staff two Privacy Interpretation Bulletins: (1) Use of Data for Educational Material (September 2010) and (2) Return of Own Data (February 2011).
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.	▪ 100% completed

Categories	Privacy Indicators	CIHI Response
	▪ The date of commencement of the employment, contractual or other relationship for agents that have yet to execute the Confidentiality Agreement and the date by which the Confidentiality Agreement must be executed.	▪ None
Termination or Cessation	▪ The number of notifications received from agents since the prior review by the Information and Privacy Commissioner of Ontario related to termination of their employment, contractual or other relationship with the prescribed person or prescribed entity.	▪ N/A

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 priority risks are reviewed and monitored on a quarterly basis.
	▪ 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.	▪ See above.
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.	▪ Since November 2008, the Business Continuity and Disaster Recovery Plan was tested June 23, 2010.
	▪ 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 and last revised June 2010.

Approved Data Linkages

2011

Fiscal Year	No.	DL - #	Date Approved	Files Linked	Subject	Date of Data Destruction
Nov. 2008-2009	1	300 (2008)	22-Jan-09	DAD-HMDB-NACRS	Impact of minimum drinking age on inpatient and emergency department healthcare utilization in Canada	2012
	2	296 (2008)	22-Jan-09	CORR-DAD	Health Outcomes during Transition to Adulthood in Paediatric Patients with End-Stage Renal Disease	2014

Fiscal Year	No.	DL - #	Date Approved	Files Linked	Subject	Date of Data Destruction
2009-2010	1	152	17-Jun-09	CORR-DAD	Health Outcomes during Transition to Adulthood in Paediatric Patients with End-Stage Renal Disease (additional year of data)	2014
	2	176	29-July-09	DAD-NACRS	Pairing Newborn and Maternal Abstracts	August 2012
	3	248	07-Oct-09	CJRR-HMDB	Examination of the Determinants of Surgical Waiting Times of Joint Replacement in Canada	2012
	4	255	16-Oct-09	CJRR-DAD & HMDB	Data Quality, CJRR Analytical Products	Begins in 2010-11
	5	177	07-Jan-10	DAD-HMDB-NACRS	Linkage of moms and babes records within a single year and across holdings	January 2020
	6	379	23-Mar-09	DAD & Patient-Level Cost Data	Patient-Level Cost Data	November 2013
	7	357	18-Mar-10	CORR-DAD	Major chronic disease affecting organ transplant recipients	March 2013

Approved Data Linkages

2011

Fiscal Year	No.	DL - #	Date Approved	Files Linked	Subject	Date of Data Destruction
2010-2011	1	246	10-May-10	DAD – episodes of care	Residential proximity and hospital level of service: A geospatial epidemiological study of obstetrical outcomes	May 2016
	2	444	10-May-10	DAD, NACRS, NRS, CCRS, HCRS	Pathways of care for stroke patients in Ontario	April 2012
	3	107	10-May-10	Patient-Level cost data, NACRS	Data Quality assessment…continued	November 2013
	4	132	03-Jun-10	OMHRS with DAD & NACRS	Develop mental health indicators for Ontario	June 2013
	5	142	02-Jun-10	DAD, NACRS	Perform newborn-maternal abstract linkage in DAD	June 2013
	6	108	03-Jun-10	DAD	BC Shaken Baby Syndrome Surveillance – to evaluate the incidence of abusive traumatic brain injuries among infants	June 2013
	7	197	16-Aug-10	CCRS with external survey results collected by researchers	Relationships between Quality of Life and Selected Resident and Facility Characteristics in Long Term Care Facilities in Canada	August2013
	8	280	12-Oct-10	Ontario DAD	Evaluation of Fetal Fibronectin Implementation in Ontario	October 2013
	9	306	20-Oct-10	DAD	Effects of coding changes on HSMRs	October 2013
	10	296	21-Oct-10	DAD, NACRS	Alberta Health Services - 7 years of data linkage of DAD and NACRS data	October 2013
	11	311	02-Nov-10	NTR CDS-DAD-NACRS	PHAC Consumer Product Safety Injury Risk Assessment: Unusual and sensitive linkage	November 2013
	12	357	18-Nov-10	CCRS, DAD, NACRS, OMHRS	Patient Safety	November 2013

Approved Data Linkages

2011

Fiscal Year	No.	DL - #	Date Approved	Files Linked	Subject	Date of Data Destruction
2010-2011	13	192	04-Feb-10	DAD, NACRS	DAD_NACRS_IHME at University of Washington	February 2014
	14	374	13-Jan-11	DAD, NRS	Link 4 yrs of DAD & NRS data from all Canadian provinces/territories with the exception of Quebec to evaluate the quality of amputations across hospitals	January 2014
	15	411	04-Feb-11 by PC&S 22-Feb-11 by CEO	DAD	Perform newborn-maternal abstract linkage in DAD; Approval of disclosure of PHI	February 2013
	16	363	18-Feb-11	DAD, NACRS, HMDB	Linkage of data across the CAD databases, within the same year; linkage of newborn and maternal abstracts	2021
	17	389	04-Feb-11	TC's National Collision Database and NTR MDS and NTR CDS	Test linkage of subset of Transport Canada's National Collision Database to the NTR MDS and NTR CDS	April 2014
	18	428	23-Feb-11	DAD	Anti Hip Fracture Medication	February 2014
	19	439	04-Mar-11	DAD	Saskatchewan Patient Level Physician Billing data to DAD	March 2013
	20	473	31-Mar-11	NTR and DAD	Linkage for costing - to obtain RIWs	March 2014

	21	455	09-Mar-11	DAD, NACRS	Severe Combined Immune Deficiency - avoid double counting patients when calculating total number of affected children.	March 2014
	22	493	04-Apr-11	DAD	A population based cohort comparison of post partum haemorrhage incident, risk factors and management between France & Canada	April 2014

Fiscal Year	No.	DL - #	Date Approved	Files Linked	Subject	Date of Data Destruction
2011-2012	1	128	11-May-11	Cost Data to OMHRS, CCRS, NRS	Data quality assessment	November 2013
	2	146	25-May-11	DAD	To produce episodes of care and linkages of moms and babes charts to study regional and tempora variations of critical illness: pregnant and post-partum women and newborns	May 2014
	3	190	27-Jun-11	CJRR, DAD	To assess performance of hip resurfacing procedures – aggregate data only disclosed	July 2014
	4	196	27-Jul-11	HCRS, CCRS, OMHRS to DAD, NACRS & NRS	Neurological Conditions Study	July 2014
	5	218	28-Jul-11	CJRR to CAD	Annual CJRR data quality and reporting activities	July 2014
	6	223	8-Aug-11	DAD, NACRS, Alberta Ambulatory Care	Canadian Partnership Against Cancer Performance Indicators Report	July 2014

	7	228	16-Aug-11	DAD, HMDB	Study examining cardiovascular care in Canada	August 2014
	8	158	29-Aug-11	Patient cost data to DAD, NACRS, OMHRS, CCRS and NRS	Canadian Patient Cost Database	Ongoing program of work
	9	268	28-Sep-11	DAD – Moms & Babes	Defensive Medicine and Caesarean Section Rates: Evidence from Canada	September 2014
	10	265	29-Sep-11	CMDB and CCHS	Unmet Health Care Needs and Adverse Outcomes for Patients with Chronic Disease	December 2012
	11	278	25-Oct-11	Trauma and Dad, NACRS	Costing Analysis of Trauma Cases	October 2014
	12	279	20-Oct-11	DAD, CJRR	Effect of Socioeconomic Status on Access to and Outcomes of Knee and Hip replacement in Select Canadian Provinces	October 2014

Privacy Impact Assessment Log

2011

Data Holding / Information System / Technology / Program	Last Completed	Next Scheduled 3-Yr Review	Comments
Methodologies and Specialized Care			
Hospital Mental Health Database (HMHDB)	2011	2013-14	
Home Care Reporting System (HCRS)	2011	2013/14	
Continuing Care Reporting System (CCRS)	2006	2011/12	In progress
Ontario Mental Health Reporting System (OMHRS)	2011	2014/15	
National Rehabilitation Reporting System (NRS)	2009	2012/13	
Pharmaceuticals and Health Workforce Information Services			
National Prescription Drug Utilization Information System (NPDUIS)	2011	2014-15	
National System Incident Reporting (NSIR)	2009	2012/13	
Acute and Ambulatory Care Information			
Therapeutic Abortions Database (TADB)	2011	N/A	PIA not required
Clinical Administrative Database (DAD, HMDB, NACRS)	2005	2011/12	In Progress
CIHI Portal	2008	2011/12	
➢ Addendum 2008/09	2009		
➢ Addendum 2010/11			In Progress
Primary Health Care and Clinical Registries			
Canadian Joint Replacement Registry (CJRR)	2009	2012/13	
Canadian Organ Replacement Registry (CORR)	2009	2012/13	
➢ CORR WAVE Addendum	New		In Progress
National & Ontario Trauma Reporting Dataset (NTR/OTR)	2005	2011/12	In Progress
Primary Health Care Voluntary Reporting System	New		In Progress
Clinical Data Standards &Quality			
Data Quality Special Studies	2011	2013-14	
ITS			
HMD SRI	2009	2012/13	
e-Reporting	2011	2013-14	

Privacy Impact Assessment Log

2011

Data Holding / Information System / Technology / Program	Last Completed	Next Scheduled 3-Yr Review	Comments
Health Spending & Strategic Initiatives			
MS Monitoring System	New		In Progress
Patient Cost Database	New		In Progress

Fiscal Year: 2008-09

Description of Privacy Impact Assessment	Recommendations	Manner Addressed	Completion Date
CIHI Portal A foundational privacy impact assessment of the privacy, confidentiality and security risks associated with CIHI Portal, an analytical web-based tool designed to provide CIHI's clients, who are also its data providers, with online access to pan-Canadian health care data in a secure environment that safeguards privacy and confidentiality.	1. The threat and risk assessment specific to CIHI Portal scheduled for 2008–2009 to be completed by the end of that fiscal year.	As per recommendation	2008
	2. The service agreements for CIHI Portal have evolved in order to take into account the various needs of CIHI clients and, while some versions are more stringent than others, some privacy or security requirements may have been lost over time. A general review of the requirements of the service agreement relating to confidentiality, privacy and security, therefore, is recommended to be undertaken by CIHI's Privacy and Legal Services Secretariat and completed by the end of 2008–2009. It is further recommended that a revised agreement be phased in over time.	As per recommendation	September 2009
	3. As part of the general review of the confidentiality, privacy and security provisions of the service agreement set out in recommendation 1 above, the service agreement should be amended to include a specific requirement for: a. clients to advise CIHI within five working days of any changes in authorized users; b. clients' users to exit from their accounts at the end of each session; and c. clients' users to sign an acknowledgement of the conditions of use of CIHI Portal to reinforce their understanding of their responsibilities and obligations, including control of passwords.	As per recommendation	September 2009

Description of Privacy Impact Assessment	Recommendations	Manner Addressed	Completion Date
	4. As part of the education process for users, phase into the training materials a clear and easily understood explanation of the acknowledgement and its implications.	As per recommendation	Ongoing
CIHI Portal Addendum 2008 -2009 A privacy impact assessment of the privacy, confidentiality and security risks associated with the following enhancements to CIHI Portal: 1. Expanding the CIHI Portal Community 2. Access to CMG+ variables in CIHI Portal 3. Access to additional provider Service and Provider Type data in CIHI Portal 4. Access to National Ambulatory Care Reporting System (NACRS) data via CIHI Portal 5. Additional/New Functionality: Patient View in CIHI Portal 6. Access to eMIS static reports in CIHI Portal 7. Access to MIS data in CIHI Portal 8. Access to two additional Discharge Abstract Database data elements 9. Updated Termination of Pregnancy Masking in CIHI Portal 10. Ethical hack	No recommendations	n/a	n/a

CIHI'S Privacy Impact Assessment Program – Summary of Recommendations 2011

Fiscal Year: 2009-10

Description of Privacy Impact Assessment	Recommendations	Manner Addressed	Completion Date
Health Master Data Project (HMD) Privacy Impact Assessment A privacy impact assessment of the privacy, confidentiality and security risks associated with Phase 1 of CIHI's Health Master Data Project, with a goal to develop and apply a central methodology that will accurately and efficiently link records across and within CIHI data holdings.	No recommendations	n/a	n/a
National Rehabilitation Reporting System (NRS) A privacy impact assessment of the privacy, confidentiality and security risks associated with NRS, a pan-Canadian information system, designed to collection of inpatient physical rehabilitation patients, including orthopaedic trauma or surgery, stroke and spinal cord dysfunction, from Canadian hospitals to support decision-making and planning of inpatient rehabilitation services.	No recommendations	n/a	n/a
National System for Incident Reporting (NSIR) A privacy impact assessment of the privacy, confidentiality and security risks associated with NSIR, a web-based voluntary reporting system, designed to: (a) capture standardized data related to medication incidents that have occurred within Canadian hospitals; and (b) provide anonymized reporting to encourage voluntary participation and to protect patient, provider and facility information.	No recommendations	n/a	n/a

CIHI'S Privacy Impact Assessment Program – Summary of Recommendations 2011

Fiscal Year: 2010-11

Description of Privacy Impact Assessment	Recommendations	Manner Addressed	Completion Date
Canadian Joint Replacement Registry (CJRR) A privacy impact assessment of the privacy, confidentiality and security risks associated with CJRR, a pan-Canadian information system for hip and knee replacement surgery, with a mandate to record and analyze the level of activity, clinical parameters and outcomes of primary and revision hip and knee replacement surgery over time.	1. CJRR should review the practices around retention of paper questionnaires and, in consultation with Records Management, establish a retention/disposal schedule that takes into account any legal requirements or restrictions and redress mechanisms. CJRR should dispose of documents that no longer have a specific purpose and do so in a way that prevents improper or unauthorized use, access, copying, modification or disclosure and is in accordance with CIHI's policies and procedures.	As per recommendation	September 2011
Canadian Organ Replacement Register (CORR) A privacy impact assessment of the privacy, confidentiality and security risks associated with CORR, a pan-Canadian information system for renal and extra-renal organ failure and transplantation, with a mandate is to record and analyze the level of activity and outcomes of solid organ transplantation and renal dialysis activities.	1. CORR should review the practices around retaining paper questionnaires and, in consultation with Records Management, establish retention and disposal schedule that takes into account any legal requirements or restrictions and redress mechanisms. CORR should dispose of documents that no longer have a specific purpose in a way that prevents improper or unauthorized use, access, copying, modification or disclosure and that is in accordance with CIHI's policies and procedures.	As per recommendation	September 2011
CIHI e-Reporting A privacy impact assessment of the privacy, confidentiality and security risks associated with CIHI's e-Reporting strategy.	1. It is recommended that the agreements for use of the CIHI e-Reporting service (bilateral reports and Portal services) be amended to include a clause requiring devices employed by off-site client users to be owned and managed by the authorized organization. Further, the individual user agreements should contain a clause sensitizing the client users to the need to protect such devices from unauthorized access and the need to appropriately secure hard copy reports outside the authorized organizations' facilities. It is recognized that this safeguard may present a hardship for some smaller client organizations. Alternatively, the e-Reporting organizational service agreement(s) should be amended to include the minimum acceptable device		In progress

Description of Privacy Impact Assessment	Recommendations	Manner Addressed	Completion Date
	configuration for all client organization users who will be accessing the e-Reporting service outside the client organizations' IT environment, i.e., from a home office or other external location. In addition, individual user agreements should be amended to require such external users to confirm that the personal computer used to access CIHI e-Reporting conforms to the stated minimum requirements. 2. It is recommended that CIHI consider the conduct of threat and risk assessments generally on a regular basis. 3. It is recommended that CIHI assess the feasibility of implementing two-factor authentication for all e-Reporting client accounts authorized to access bi-lateral reports and Portal services, in order to strengthen the client authentication process thereby reducing potential risk associated with Secure Socket Layer encryption, that is, a "man-in-the-middle attack", as well as risks associated with malware (keyloggers). 4. It is recommended that CIHI assess the feasibility of implementing a centralized function for initially granting access to all e-Reports at CIHI and for the subsequent management of those permissions.		
Data Quality Special Studies A privacy impact assessment of the privacy, confidentiality and security risks associated with Data Quality Special Studies which are a key component of CIHI's Data and Information Quality Program.	No recommendations.	n/a	n/a
Hospital Mental Health Data Base A privacy impact assessment of the privacy, confidentiality and security risks associated with the Hospital Mental Health Data Base which is a national source of standardized mental health services data in Canada.	No recommendations.	n/a	n/a

Description of Privacy Impact Assessment	Recommendations	Manner Addressed	Completion Date
NATIONAL PRESCRIPTION DRUG UTILIZATION INFORMATION SYSTEM (NPDUIS) A privacy impact assessment of the privacy, confidentiality and security risks associated with the NPDUIS Database which contains health information, in both identified and de-identified form, on drug claimants collected from publicly-financed drug benefit programs in Canada. In addition, the database contains information on drug claims data such as formulary data, drug product information, and information regarding various public drug plan/program administrative policies.	1. Strengthen the terms of use of the current "Operating Principles for Use of NPDUIS Web Reports" and the associated Pop-up Notice to reflect CIHI's most up to date privacy and security practices to ensure the Clients and Authorized users are aware of, and understand their confidentiality and security restrictions and obligations.		In progress
	2. As part of the education process for users, include in the training materials a clear and easily understood explanation of the obligations when accessing the Web Reports and the NPDUIS Analytical Environment.	As per recommendation	September 2011
HOME CARE REPORTING SYSTEM (HCRS) A Privacy Impact Assessment of the privacy, confidentiality and security risks association with the Home Care Reporting System which contains information on home care services provided by provincial and territorial governments. This includes where publicly funded home care programs use private sector agencies to deliver the care.	No recommendations	n/a	n/a
ONTARIO MENTAL HEALTH REPORTING SYSTEM (OMHRS) Privacy impact assessment of the privacy, confidentiality and security risks associated with the Ontario Mental health Reporting System which is designed to capture standardized, patient-specific, clinical, demographic, administrative, and resource utilization information within a single reporting framework. OMHRS is a longitudinal reporting system that captures data on hospital mental health inpatients at multiple points throughout their episodes of care.	No recommendations	n/a	n/a

Fiscal Year: 2008-09

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.	1. That the organization regularly informs CIHI of any modification to the employee access list so that new or additional employees not originally identified in the data request are identified as having access to CIHI data. (Note: this notification must be made in writing and submitted to the CIHI program area that processed the data request.)	As per recommendation	June 2009
	2. That the data be destroyed as opposed to returned once the data become older than 10 years and that the organization uses a generally accepted method to destroy the data and thereafter certify the destruction in writing to CIHI; and that CIHI and the organization documents their decision to amend the agreement so that it is clear that the data will be destroyed as opposed to returned. The organization indicated that it is willing to adopt this recommendation.	As per recommendation	May 2009
	3. That the organization implements the use of a log to record access to the cabinet where the original CIHI data are stored.	As per recommendation	May, 2008
	4. That the organization undertakes in writing that the data breach policy will be triggered should any CIHI data ever be compromised. It is further recommended that part of the above undertaking include notification to CIHI of any unauthorized access, use or disclosure of CIHI data. As recognized and highlighted by several privacy commissioners in Canada, notification of privacy breaches is most effective when provided on a timely basis.	As per recommendation	July 2008

Fiscal Year: 2008-09

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.	1. That on a go-forward basis the organization amends its employee confidentiality agreement so as to recognize, if it does not already, that health data are to be treated as confidential.	As per recommendation	December 2008
	2. That the organization continues to notify CIHI in every incidence of any new hires that have a need and are granted access to CIHI data.	As per recommendation	December 2008
	3. That the organization and CIHI collaborate so as to narrow down and identify the data elements necessary for the research, and only those fields should be disclosed to theorganization.	As per recommendation	December 2008
	4. That the organization, certify to CIHI's Chief Privacy Officer and General Counsel on a yearly basis that the data are destroyed using industry acceptable standards of data destruction.	As per recommendation	December 2008
	5. That the organization undertakes to promptly notify CIHI should any of the record-level data be compromised so as to constitute a privacy breach.	As per recommendation	December 2008
	6. That the organization explores technological solutions that would enable the encryption of its back-up tapes.	As per recommendation	December 2008
	7. That the organization explores the possibility of instituting the required technological solutions that would give access to "read only" data and make it impossible to copy the record-level data on other media.	As per recommendation	December 2008
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.	No recommendations	n/a	n/a
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.	No recommendations	n/a	n/a

Fiscal Year: 2009-10

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.	1. It is recommended that researchers should provide a written certification annually to CIHI that they continue to comply with their obligations under such agreements. This additional requirement could become part of CIHI's third-party data request program and be implemented in CIHI's data request tracking (DaRT) system, as part of a comprehensive life cycle approach to data management.	CIHI has implemented a process to obtain written certification annually from data requestors.	Ongoing

Fiscal Year: 2010-11

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.	1. It is recommended that the clause be amended for those employees involved with CIHI data by including specific reference to CIHI data as being part of the confidential information that the individual will have access to during their employment.	As per recommendation	April 2010
	2. CIHI asks that the organization confirm in writing that the Addendum is amended to include explicit reference to those practices mentioned above that are already in practical effect. a) lock-up procedures employed when employees leave their workstations; b) password settings that ensure adequate security of CIHI data; c) explicit reference to data destruction procedures (each of these issues is further discussed below).	As per recommendation	April 2010
	3. It is further recommended that the terms and conditions for employment be amended to make it clear that the confidentiality with respect to CIHI data is an obligation that survives termination.	As per recommendation	April 2010
	4. The organization's contract with another party be amended to include the obligation to securely destroy all CIHI data upon completion of the project, or at the request of the organization, or at the request of CIHI, or otherwise as obligated by the term in the request form.	As per recommendation	April 2010
	5. It is recommended that the contract with the other partyinclude: - A clause requiring it to consent to a privacy audit by either the organization and/or CIHI. - A clause requiring it to report back to the organization and CIHI if ever there is any unauthorized access to the CIHI data (i.e. a data breach).	As per recommendation	April 2010

Description of Audit	Recommendations	Manner Addressed	Completion Date
	6. It is recommended that the organization implement an editor's checklist that includes references to the organization's obligations to CIHI. For example, the checklist would have the editor ensure that no cell sizes less than five appear in any report and that the report would contain the necessary acknowledgement that the report was based, at least partially, on CIHI data	As per recommendation	April 2010
	7. It is recommended that the practice of ensuring the encryption of the data while in transit on mobile computing equipment and all other mobile devices be explicitly referenced in the Addendum on Health Information that accompanies the organization's privacy policy. It is further recommended that this obligation be made a condition of employment for each employee with access to the CIHI data.	As per recommendation	April 2010
	8. CIHI recommends that the researcher's computer laptop be secured by an alpha-numeric password that is at least 8 characters long.	As per recommendation	April 2010
A compliance audit of an external third-party that received data from CIHI to ensure it and the researchers involved in a consortium, is meeting or has met its contractual obligations, as set out in CIHI's confidentiality agreement.	1. It is recommended that CIHI, the organization and the University enter into a tripartite data-sharing agreement respecting the disclosure of data to the organization, the terms of which would include a clear articulation of the organization's mandate as well as confidentiality and data destruction requirements.	In progress	
	2. It is recommended that the tripartite data-sharing agreement between the parties state that the data may be retained for as long as necessary to meet the identified purposes.	In progress	
	3. It is recommended that the data on the hard drive of the desktop computer at theorganization, and the original CD ROMs, be securely destroyed in accordance with CIHI standards after it is uploaded onto the server.	As per recommendation	October 2011

Description of Audit	Recommendations	Manner Addressed	Completion Date
DaRT A CIHI internal compliance audit with respect to Program Area staff sending to Privacy and Legal Services all required documentation related to record-level data requests prior to disclosing data to the recipient.	No recommendations	N/A	January 2011
Review of Internal Process for Tracking of Mandatory Privacy & Security Training and Annual Renewal of Employee *Confidentiality Agreement* A CIHI internal review of process for tracking the completion of CIHI's first on-line mandatory privacy and security training module and annual renewal of the employee *Confidentiality Agreement*.	No recommendations	N/A	January 2011

Fiscal Year: 2011-12

Description of Audit	Recommendations	Manner Addressed	Completion Date
A compliance audit of an external third-party that received data from CIHI to ensure it is meeting or has met its contractual obligations, as set out in CIHI's confidentiality agreement.	1. That the organization develops a checklist of key procedures for managing CIHI data to ensure continuity of data protection practices in the event of staff changes.	As per recommendation	October 2011
	2. That the organization establishes and maintains a secure method of destroying CDs containing CIHI data. The method of destruction must be an industry acceptable practice to permanently destroy or erase, in an irreversible manner, ensuring that the data records cannot be reconstructed in any way.	As per recommendation	August 2011
	3. That the organization acknowledges formally that all historical data have been securely destroyed by signing a CIHI Data Destruction Certificate.	As per recommendation	October 2011
	4. That a damaged lock to the office where CIHI data is located be repaired or replaced so that there are two physical barriers protecting the network storage device (i.e. one lock for the building and a second lock for the office).	As per recommendation	August 2011
	5. That access to the network storage device (or, alternatively to the file folder containing the data on the network storage device) only be accessible upon entering a different password.	As per recommendation	August 2011
	6. That the file folder on the network storage device used to store CIHI data be encrypted using an industry acceptable solution.	As per recommendation	August 2011
	7. That CIHI data stored on back-up tapes be encrypted using an industry acceptable encryption solution.	As per recommendation	August 2011
	8. That the organization include in the checklist identified in Recommendation #1, the requirement to encrypt any data stored on a mobile computing device.	As per recommendation	October 2011

2010 Physical TRA Assessment

Site	Issue	Recommendation	Status Update
St. John	Employees do not wear their security badges.	Inform employees of the importance of wearing their security badges and review the corporate security policy with employees.	Completed as per recommendation.
	The main door to the office is unlocked during business hours and there is no security system in place.	Install a security system for the main door. In the interim advise staff to lock the main door.(i.e. during lunch hour)	Completed as per recommendation.
Montreal	While the front door to the office is locked at all times, the employee who sits at the front desk is responsible for greeting all visitors. There is no remote entry button so she opens the door for them. At times the employee is unsure if the individuals are CIHI visitors, someone lost in the building or someone who has come to visit the previous tenant. As this employee is alone in the area she does not feel secure.	Install panic button at the reception desk with a chime that sounds in the office space where other employees will hear it and respond. The button would also be wired, via CIHI owned security system, to the building security for rapid response.	Completed as per recommendation.
Ottawa WEP	A potential vulnerability was identified in the Reception Area.	IT to follow up on and provide a recommendation.	Item reviewed by the IT department. After a thorough evaluation of all factors, this was assessed as not a major issue; therefore, no further action is recommended at this time.
Ottawa 495 Richmond	Garage not well lit on 4th and 5th levels	Request enhanced lighting from landlord	Completed as per recommendation.
	Garage - no emergency or panic button in place	Request from landlord that phones or emergency button be installed in the area (to ward off offender)	The landlord has reviewed this request, however, is not willing to act on it. After further review of the matter, a decision has been made that due to low degree of associated risk, no further action is recommended at this time.

2010 Physical TRA Assessment

Site	Issue	Recommendation	Status Update
	Basement corridor on the east and west sides of the building have alcoves	Request from landlord to install convex mirror at each alcove for better visibility	Completed as per recommendation.
	CIHI employees allow individuals to tail gate when entering the secured office space	Reinforce that employees need to ensure that the person following them into the office is an employee and that the individual has a visible security badge. Need to highlight to all staff the potential threat of "tailgating" such as theft and other security breaches. Approach landlord regarding the installation of specific signs for placement outside the elevator advising people to report to the CIHI Reception on the 6th floor.	Completed as per recommendation. Completed as per recommendation. CIHI installed signs by security card readers on 3rd, 4th, 5th, and 7th floors.
Toronto	Employees working on weekends (alone)	Advise all staff to notify security if they are working in the evening or on the weekend	Completed as per recommendation.
	No specific start up procedures for the UPS or A/C after disruptive event.	Refresh current procedures in place with all IT staff on re-setting both systems. To be completed by IT Add signage in the data center on each piece of equipment with emergency contact information for that vendor	Completed as per recommendation. Completed s per recommendation.
	CIHI employees allow individuals to tail gate them while entering the secured office space	Reinforce that employees need to ensure that the person following them into the office is an employee and have a visible security badge. Need to highlight to all staff the potential threat of "tailgating" such as theft and other security breaches.	Completed as per recommendation.

2010 Physical TRA Assessment

Site	Issue	Recommendation	Status Update
Victoria	IT closet door not secure, opens easily	Assess feasibility of installing a bolt on one side of the door and advise employees that the door should be locked at all times.	Completed as per recommendation.
	No temperature or power loss monitoring in place	Install sensors and wire them to the CIHI owned security system	After an on-site review of the situation and current heat dissipation equipment, a decision has been made that no further action is required at this point. The situation will be monitored by the IT department throughout 2011.
	Keys to the office are stored in a secure key box in a lockable filing cabinet but only one person has keys to that cabinet.	Once access to the IT closet is fully secured relocate the key box to the IT closet. In the mean time ensure that someone has a back up key to the filing cabinet.	Completed as per recommendation. Completed as per recommendation.
	CIHI owned security system is to be inspected annually. No inspection was done in 2010.	Test the system.	Completed as per recommendation.
	Employees do not wear their security badges.	Inform employees of the importance of wearing their security badges and review the corporate security policy with employees.	Completed as per recommendation.
	Some employees still use a key and not their badge to access the office. This creates a potential risk of unauthorized access to the office if a key is lost.	Ensure that all badges work to enter the office and educate employees on the importance of using their badges and not a key.	Completed as per recommendation.

Fiscal Year: 2008-09

Description of Audit	Description of Recommendation	Manner Addressed	Completion Date
External Third Party Vulnerability Assessment and Penetration Test Penetration Testing assessments were performed to evaluate the security posture of: ▪ 9 active (7 external and 2 internal) networks, ▪ 15 external IP Addresses, ▪ 25 internal IP Addresses and ▪ 5 Web Applications The purpose and objectives of this audit were to find points of entry, flaws and vulnerabilities that could be used to gain unauthorized access to CIHI's systems. Testing was conducted on site and off-site on the selected systems throughout the month of March 2009 to achieve the following goals: ▪ Determine the current risk exposure and identify vulnerabilities requiring remediation. ▪ Discover and document gaps between the security controls in place and security best practices. ▪ Deliver a prioritized and actionable remediation plan to guide CIHI to improve overall security posture based upon business needs. ▪ Increase security awareness at CIHI.	There were a total of 74 specific technical recommendations related to system configuration and implementation. Due to the confidential nature of these recommendations, the specifics will not be provided here. Of the 74 recommendations: ▪ 67 were addressed as per recommendation or through decommissioning of affected systems ▪ 2 remain open due to the complex nature of the recommendation and ongoing effort ▪ 4 were deemed low risk and/or low impact, and a decision was made to not address the recommendation ▪ 1 was not possible due to technical constraints	See description	See description

Description of Audit	Description of Recommendation	Manner Addressed	Completion Date
External Third Party Vulnerability Assessment and Penetration Test of 3 Web-based Applications The audit comprised the following components: ▪ Software Development Lifecycle Assessment (SDLCA) – a review of the software development process to ensure that security is being included in all phases of the development lifecycle. ▪ Web Application Penetration Test – These exercises were designed to test the application level security controls and specifically identify what vulnerabilities an application may have and what level of effort is needed to exploit these vulnerabilities. ▪ Secure Code Review - The Secure Code review involved reviewing the application code to identify defects that could lead to possible security vulnerabilities in the application.	1. Secure Code Review Recommendations There were a total of 3 recommendations related to coding practices in the 3 subject applications. Due to the confidential nature of these recommendations, the specifics will not be provided here. All recommendations were addressed.	See description	March 2009
	2. Web Application Penetration Test There were a total of 9 recommendations as a result of the penetration testing. Due to the confidential nature of these recommendations, the specifics will not be provided here. Where technically possible, all recommendations were addressed.	See description	March 2009
	3. Software Development Lifecycle Recommendation Security should be considered in all phases of the development lifecycle.	As per recommendation	September 2011

Fiscal Year: 2009-10

Description of Audit	Description of Recommendation	Manner Addressed	Completion Date
External Third Party Vulnerability Assessment and Penetration Test of a web-based application The audit comprised the following components: ▪ A manual code review of key areas of the application code (form processing code, database connectivity, user management, etc.) to identify potential vulnerabilities as a result of coding practices, framework implementation, etc. ▪ Penetration testing of the application to identify vulnerabilities that may exist	There were a total of 3 specific technical recommendations related to the application code. Due to the confidential nature of these recommendations, the specifics will not be provided here.	See description	December 2010

Fiscal Year: 2010-11

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 ▪ Perform a targeted penetration test of up to 12 select systems identified by CIHI. Key activities – Internal: ▪ Perform exploratory vulnerability scanning across multiple internal "Class C" private subnets, ▪ Perform a targeted penetration test of up to 20 select systems identified by CIHI.	1. Ensure adequate end user education and ongoing security awareness.	CIHI regularly reviews its employee and awareness program and updates it based on emerging issues and identified needs. A specific education campaign will be developed to address the risk due to social engineering, to be delivered during FY 2010-2011.	Will be incorporated into Privacy Awareness Month Training January 2012
	2. Review public website content such as organizational charts, email addresses, etc. and sanitizes references to specific personnel names, contact information and business plans where possible.	Remove personal email addresses from external web site except for CEO and VPs.	April 2011
	3. Various configuration changes to systems. A number of specific low-level technical recommendations are presented in the Technical Review portion of the report	ITS staff will assess the feasibility, cost and risk of all such recommendations and address accordingly	September 2011
	4. All internal systems should be assessed, hardened and tested to protect against the potential of internal attack in addition to limiting further penetration by an external attacked should they gain access to systems. Internal technical security assessments and regular vulnerability scans are recommended to detect weak systems that could lead to unauthorized access. Various configuration changes to systems.	Existing procedures for hardening all systems before deployment will be reviewed, and an enhanced audit program is under development that will include internal security and vulnerability assessments.	April 2011

Description of Audit	Description of Recommendation	Manner Addressed	Completion Date
	5. Regular vulnerability scans and application code reviews are recommended to reduce the risk of unauthorized network and application access by immediate identification of system configuration changes such as open ports or newly discovered vulnerabilities affecting <your> systems.	Effective December 2010, ITS implemented a new comprehensive audit policy and procedures	April 2011
	6. Security awareness training for IT professionals	All future divisional education and training plans will include specific and relevant requirements for security training based on roles and responsibilities.	Planned completion date March 2012
	7. Ensure that all administrator level accounts have strong, 15-character or greater passwords.	CIHI has strong password policies and processes. In fact all servers currently employ random generated passwords that exceed CIHI's password policy. To ensure that these policies are adhered to, ITS Management will devise a more robust audit program to verify adherence.	April 2011
	8. Perform server and workstation operating system hardening and verify that settings have been applied.	ITS Management agrees with this recommendation. Currently ITS have rigorous hardening guidelines for all IT based systems and platforms. To ensure that these guidelines are adhered to, ITS Management will devise a more robust audit program to verify adherence to these guidelines.	April 2011

Description of Audit	Description of Recommendation	Manner Addressed	Completion Date
	9. Ensure that antivirus software is installed on every Windows-based computer.	ITS currently employs antivirus on all PC/laptops and outside facing servers. ITS management will investigate the feasibility (cost and resource implications) of deploying antivirus on approximately 175 servers. After IT's review, it was decided that this recommendation would not be implemented. The cost of installing and supporting antivirus software on ALL of CIHI's servers would far exceed the benefit gained. As an alternative, server antivirus software will be considered on a case-by-case basis. The Senior Security Administrator will evaluate each server as it is deployed into production and determine if antivirus software is appropriate.	N/A
	10. Implement an automated patch management system that is capable of deploying patches for Microsoft and non-Microsoft products, such as Adobe Acrobat Reader.	This is the current ITS practice. ITS Management will continue to ensure that additional 3rd party software are automatically patched through a phased in program.	Complete
	11. Implement host intrusion detection and/or active log monitoring to detect malicious activity on key network servers	ITS Management agrees that host intrusion detection should be employed. The next generation of Operating Systems will integrate these capabilities natively within the operating system, For other platforms, CIHI will investigate the feasibility and cost of employing these technologies.	December 2010

Description of Audit	Description of Recommendation	Manner Addressed	Completion Date
	12. Acquire additional network and security scanning tools and develop a vulnerability scanning process to scan the network on a regular basis.	ITS currently uses similar network security scanning tools to those employed by ethical hack vendors. A bi annual audit is performed with these tools. ITS Management feels our internal tools and processes are sufficient when combined with independent external party audits.	Complete
	13. Ensure that passwords and other sensitive information are not stored on the network unless secondary authentication is required for access.	ITS will ensure that our Security Awareness Training and orientation program addresses this issue.	April 2011

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 Ad-hoc (approx. 6-10 times per year) 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
Software Approval Audits Ad-hoc (on-demand) software audits. These audits are designed to evaluate the trustworthiness, vulnerabilities, and security implications of software prior to approval for use on CIHI's networks. Software is classified as approved, conditionally approved, or restricted.	N/A	N/A	N/A

Description of Audit	Description of Recommendation	Manner Addressed	Completion Date
Desktop Software Audit Quarterly desktop software audit to discover unapproved software on user workstations. For any unapproved software that is discovered, an Incident is opened, the software is removed by IT staff, and the employee and their manager receive a notification from Security@cihi.ca. Multiple or serious violations are referred to Human Resources for follow-up.	N/A	N/A	N/A
Network Vulnerability Assessment Annual Internal network vulnerability assessment audit to discover software vulnerabilities within CIHI's network infrastructure, servers, and workstations. Findings are summarized and prioritized and Incident tickets or Change Requests are created to mitigate the vulnerabilities.	N/A	N/A	N/A
New System Security Audit New system security audits are conducted on a per-request basis to uncover vulnerabilities within new servers. A Nessus audit report is produced and the results summarized and sent to the requester to resolve the discovered issues. All issues must be resolved prior to servers being promoted to production.	N/A	N/A	N/A

InfoSec Staff Awareness, Education and Communication Log

Date	Provider	Attendees	Subject
2008.10.30	Internal – Cal Marcoux	Infrastructure Technology Department	Detailed review of CIHI's Security Incident Management Protocol and IT roles within the protocol
2008.11.06	Internal – Cal Marcoux, Mimi Lepage	CIHI Privacy Practice Group	Detailed review of CIHI's Acceptable Use Policy
2008.10.24	Internal – Cal Marcoux, Mimi Lepage	All CIHI Managers invited	Detailed review of CIHI's Privacy Breach Management and Security Incident Management protocols
2009.01.05	Internal – Cal Marcoux, Mary Ledoux	CPHI Division	Detailed review of CIHI's Privacy Breach Management and Security Incident Management protocols
2009.01.12	Internal – Cal Marcoux	Architecture and Standards department	Detailed review of CIHI's Acceptable Use Policy
2009.01.28	Internal – Cal Marcoux and Tony Tomasone	Application Development Branch	Privacy Awareness month, relationship between Privacy and Security, often overlooked coding practices and common errors that impact security
2009.02.02	Internal – Cal Marcoux	Analytical Systems department	Detailed review of CIHI's Acceptable Use Policy
2009.05.13	CIHIlights article	All staff	Connecting to CIHI's network and Acceptable Use Policy
2009.05.13	CIHIlights article	All staff	Changes to desktop and laptop computer configuration
2009.05.13	CIHIlights article	All staff	Laptop encryption software and procedures
2009.06.10	CIHIlights article	All staff	September is security awareness month

InfoSec Staff Awareness, Education and Communication Log

Date	Provider	Attendees	Subject
2009.07.08	CIHIlights article	All staff	Data access audit 2009
2009.07.17	Internal – Cal Marcoux	CSCIS Toronto	Overview of Information Security, CIHI Information Security Policy and Acceptable Use Policy
2009.07.31	Internal – email to ITS staff	ITS staff	A Gentle Reminder - desktop and laptop security – engaging password protected screensaver
2009.08.06	Internal – Cal Marcoux	CSCIS Ottawa	Overview of Information Security, CIHI Information Security Policy and Acceptable Use Policy
2009.08.31	Anne McFarlane	All Staff	September is Information Security Awareness Month at CIHI
2009.09.04	Cal Marcoux	All Staff	Important Information about computer viruses – avoiding malware
2009.09.09	Internal – Cal Marcoux	SmallTalk	Information Security Awareness Month - Information Security in the Workplace
2009.09.15	Internal – Cal Marcoux	Email to ITS staff	Important information about sharing technical information with third parties
2009.09.18	Internal – Hassan Gesso and Jean-Louis Guertin	SmallTalk	Information Security Awareness Month - Information Security in the Home
2009.09.28	Internal – Cal Marcoux	SmallTalk	Information Security Awareness Month - Information Security on the Road
2009.09.28	Internal – Cal Marcoux	HAS Team Meeting	Awareness on how we can build information security into our day-to-day activities, concept of Privacy by Design, importance of knowing and following all privacy and security policies
2009.10.09	Internal – Cal Marcoux	Portal Services team meeting	Awareness on how we can build information security into our day-to-day activities, concept of Privacy by Design, importance of knowing and following all privacy and security policies, review of recent Alberta breach and what lessons we can learn from it (malware infection)
2009.10.09	Cal Marcoux	All Managers	Information Security Awareness Month
2009.10.16	CIHIlights article	All staff	Information Security Awareness Month
2009.10.29	Internal – Cal Marcoux	DSS&AP	InfoSec awareness

InfoSec Staff Awareness, Education and Communication Log

Date	Provider	Attendees	Subject
2009.10.18	Internal – Cal Marcoux	ITS Operations Department	InfoSec awareness
2009.12.10	CIHIlights article	All staff	Passwords and the protection of confidential information
2010.03.10	CIHIlights article	All staff	Technology, Olympic Fever a bad mix for Information Security
2010.03.15	Cal Marcoux	Management	Important Information about EPS and other temporary workers
2010.07.07	Cal Marcoux	All Staff	Important information about downloading movies, videos, music and software on CIHI's computing devices.
2010.03.18	Cal Marcoux	Management	Compliance with Acceptable Use Policy
2010.06.27	Cal Marcoux	DL-IT-IS	Reminder that the use of non-CIHI USB keys on CIHI devices is forbidden
2010.09.09	Cal Marcoux	SmallTalk	Information Security Awareness Month – Acceptable Use
2010.09.24	Cal Marcoux	SmallTalk	Information Security Awareness Month - What to do if you think that a security or privacy breach may have occurred
2010-09-30	Jean-Louis Guertin and Hassan Gesso	SmallTalk	Information Security Awareness Month - All in a Day's Work – IT Security and You!
2010-10-29	Scott Murray	All staff	Important information about storing data on CIHI's network
2011-03-28	CIHIlights article	All staff	Email security advisory
2011-08-12	Cal Marcoux	DL-IT-IS	Database Access Advisory
2011-09-06	Cal Marcoux	SmallTalk	Information Security Awareness Month – Introduction to the Secure Information Lifecycle
2011-09-15	Cal Marcoux	SmallTalk	Information Security Awareness Month – Secure Lifecycle Phases – Creation/Acquisition and Retention/Storage
2011-09-22	Peter Pakeman & Cal Marcoux	SmallTalk	Information Security Awareness Month – Secure Lifecycle Phases – Access/Use/Disclosure
2011-09-29	Cal Marcoux	SmallTalk	Information Security Awareness Month – Secure Lifecycle Phases - Disposition

Affidavit of John Wright, President and CEO of the Canadian Institute for Health Information (CIHI)

I, John Wright of Ottawa, in the Province of Ontario, MAKE OATH AND SAY:

1. I am the President and CEO of the Canadian Institute for Health Information (CIHI).

2. As CIHI's President and CEO, I have formally delegated the supervision and management of day-to-day operations of the privacy portfolio to Mimi Lepage, Chief Privacy Officer and General Counsel, and have also formally delegated the supervision and management of day-to-day operations of the IT security portfolio to Scott Murray, Vice-President and Chief Technology Officer .

3. CIHI has in place privacy and security policies, procedures, protocols, practices, standards, tools, guidelines and other instruments ("Privacy and Security Policies") to protect the privacy of the individuals whose personal health information it receives and to maintain the confidentiality of that information.

4. CIHI is submitting a written report (the "Report") to the Information and Privacy Commissioner of Ontario in compliance with the *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities*, as issued by the Information and Privacy Commissioner of Ontario on April 19, 2010.

5. I have made due inquiries of Mimi Lepage, Chief Privacy Officer and General Counsel and Scott Murray, Vice-President and Chief Technology Officer regarding (i) the contents of the Privacy and Security Policies implemented by CIHI, (ii) the *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities* and (iii) the Report.

6. Based on my knowledge, having exercised reasonable diligence, the Report describes the Privacy and Security Policies implemented by CIHI in an accurate and complete manner as of the date on which the Report is submitted.

7. Based on my knowledge, having exercised reasonable diligence, CIHI has taken steps that are reasonable in the circumstances to: (i) ensure the Privacy and Security Policies implemented comply with the Manual as set out in the Report; (ii) ensure compliance with the Privacy and Security Policies implemented; and (iii) protect personal health information against theft, loss, unauthorized use, disclosure, unauthorized copying, modification or disposal.

SWORN (OR AFFIRMED) BEFORE ME)
)
at the City/Town/Etc. of Ottawa, ~~in~~ the)
)
County/Regional Municipality/Etc. of)
)
_____, in the Province of Ontario,)
on Jan 7th 20 11.)

Commissioner for Taking Affidavits

[SIGNATURE OF DEPONENT]

Talk to Us

CIHI Ottawa
495 Richmond Road, Suite 600
Ottawa, Ontario K2A 4H6
Phone: 613-241-7860

CIHI Toronto
4110 Yonge Street, Suite 300
Toronto, Ontario M2P 2B7
Phone: 416-481-2002

CIHI Victoria
880 Douglas Street, Suite 600
Victoria, British Columbia V8W 2B7
Phone: 250-220-4100

CIHI Montréal
1010 Sherbrooke Street West, Suite 300
Montréal, Quebec H3A 2R7
Phone: 514-842-2226

CIHI St. John's
140 Water Street, Suite 701
St. John's, Newfoundland and Labrador A1C 6H6
Phone: 709-576-7006

October 2011

www.cihi.ca

Canadian Institute for Health Information

Institut canadien d'information sur la santé