Privacy and Security Framework, February 2010

Updated May 2017

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

Production of this document is made possible by financial contributions from Health Canada and provincial and territorial governments. The views expressed herein do not necessarily represent the views of Health Canada or any provincial or territorial government.

Canadian Institute for Health Information
495 Richmond Road, Suite 600
Ottawa, Ontario K2A 4H6

Phone: 613-241-7860
Fax: 613-241-8120
www.cihi.ca
copyright@cihi.ca

Table of contents

Introduction to privacy and security at CIHI

This Privacy and Security Framework provides a coherent and comprehensive approach to enterprise privacy and security management for the Canadian Institute for Health Information (CIHI). The framework is designed to enable the effective integration and coordination of CIHI's privacy and security policies and to provide CIHI's decision-makers, privacy and security officers, and entire governance structure with a holistic view of the organization's privacy and security practices. It is a living document, updated as CIHI's Privacy and Information Security programs evolve over time. The framework can also be used for the purposes of communicating CIHI's commitment to privacy and security to regulators, federal, provincial and territorial governments, the public and other stakeholders.

The framework has been informed by best practices for privacy and secure information management across the public, private and health sectors. The framework is modular and provides CIHI the flexibility to share accountability across lines of business, to identify areas for improvement and to develop action plans specific to particular components of the framework.

CIHI's Privacy and Security Framework

Drivers	Legal and statutory drivers	Ontario's *Personal Health Information Protection Act* (PHIPA) and regulations and any other applicable federal, provincial or territorial privacy legislation
	Trust and confidence	Confidence of the Canadian public and of federal, provincial and territorial governments, including ministries of health, health care providers and other stakeholders
	Vision/mandate	Vision, mandate and foundation outlined in CIHI's 2016 to 2021 Strategic Plan and specific goals and priorities Mandate and core functions set out in CIHI's Privacy Policy

Governance	Organizational structure	Board of Directors Governance and Privacy Committee Board of Directors Finance and Audit Committee President and CEO Chief privacy officer and general counsel (CPO/GC) Chief information security officer (CISO) Vice president/chief information officer (VP/CIO) Extensive committee structure supports privacy and security vision and commitments External privacy advisor
	Accountability, shared responsibilities and transparency	Individual accountabilities for privacy and security and written mandates for the various committees

Risk management	Privacy and Security Risk Management Program	Privacy and Security Risk Management Program aligned with the corporate Risk Management Program Risk tools: Privacy impact assessment (PIA), threat risk assessment (TRA), vulnerability assessment and penetration testing
	Benchmarking	Environmental scans and best practices
	Compliance	Information Security Management System (ISMS) in accordance with ISO/IEC 27001:2013 Code of Business Conduct
	Business continuity/ disaster recovery	CIHI business continuity plan Technology recovery plan

(cont'd on next page)

Program controls	**Policies**	Comprehensive suite of privacy and security policies
	Standards, procedures and protocols	Standards, procedures and protocols supporting privacy and security policies
	Training and awareness	*Privacy and Security Training Policy* Mandatory and traceable privacy and security orientation for all new employees and ongoing training at least annually for current employees Internal website Privacy and Security Awareness programs established Privacy Awareness Month in January and Information Security Awareness Month in September Ongoing, regular staff education sessions based on new and emerging trends in privacy and information security
	Secure information life cycle	A suite of standards and guidelines for the protection of the confidentiality, integrity and availability of information throughout its life cycle — creation and collection, retention and storage, access, use, disclosure and disposition
	Incident Management Protocol	*Privacy and Security Incident Management Protocol*
	Agreements	Internal agreements, including CIHI Employee Confidentiality Agreement and Annual Renewal Third-Party Non-Disclosure/Confidentiality Agreement
	Third-party provider management	Accountability framework for procurement
	External communication	Privacy and Security Framework and other key policy instruments publicly available at cihi.ca

Audits, compliance and reporting	**Privacy Audit Program**	Terms of reference for the Privacy Audit Program
	Information Security Audit Program	Number of mandatory and additional audits for the Information Security Audit Program
	External review of CIHI	Information and Privacy Commissioner of Ontario review every 3 years pursuant to Section 45 of PHIPA
	Compliance monitoring/reporting	Annual privacy report to the Board of Directors, reporting topically on an ad hoc basis and pursuant to the Audit and PIA programs

1 Drivers

a. Legal and statutory drivers

CIHI is a prescribed entity under Section 45 of Ontario's *Personal Health Information Protection Act* (PHIPA) and is authorized to collect, use and disclose personal health information for prescribed purposes. As a prescribed entity, CIHI is subject to oversight by the Information and Privacy Commissioner of Ontario and must have its practices and procedures, with respect to privacy and the protection of health information, reviewed and approved every 3 years. The last such review was completed in October 2014. The renewal of CIHI's prescribed entity status is viewed by stakeholders in jurisdictions across Canada as evidence of the soundness of CIHI's Privacy and Information Security programs.

PHIPA and all privacy codes generally are based on the 10 fair information principles set out in the Canadian Standards Association's *Model Code for the Protection of Personal Information*:

Principle 1: Accountability

Principle 2: Identifying purposes

Principle 3: Consent

Principle 4: Limiting collection

Principle 5: Limiting use, disclosure and retention

Principle 6: Accuracy

Principle 7: Safeguards

Principle 8: Openness

Principle 9: Individual access

Principle 10: Challenging compliance

These principles are the basis for CIHI's self-regulatory efforts. CIHI also adheres to other provincial and territorial privacy legislation as applicable to CIHI's mandate and core functions.

b. Trust and confidence

Home to 30+ databases (see CIHI's *Products and Services Guide*), CIHI is a leading source of unbiased, credible and comparable information. Maintaining the trust and confidence of stakeholders — including federal, provincial and territorial government bodies, health care providers and institutions, health professional colleges and associations and, ultimately, the public — is critical to the success of CIHI and the achievement of its goals. All its activities must be conducted, and all partnerships established and maintained, in a manner that reflects these expectations.

c. Vision/mandate

Our vision

CIHI's vision — Better data. Better decisions. Healthier Canadians. — portrays how better data can lead to better decision-making and improve the health of Canadians. A rigorous and effective privacy and security framework is fundamental to the realization of CIHI's vision.

Our mandate

CIHI's mandate is to deliver comparable and actionable information to accelerate improvements in health care, health system performance and population health across the continuum of care.

Our foundation

CIHI bases its work on 4 foundational elements that are critical to its success as an organization and in meeting its strategic goals:

- Our people
- Stakeholder engagement and partnerships
- Privacy and security
- Information technology

Privacy and security management and a robust IT infrastructure are 2 of the 4 foundational elements and, as such, are an embedded part of CIHI's culture. They are used strategically when making decisions in day-to-day interactions with employees, customers and stakeholders.

2 Governance

a. Organizational structure

CIHI's information governance structure reflects the organization's information management practices. The information governance structure provides assurance that the strategies, policies, standards, processes and resources to manage privacy and security risks are aligned with CIHI's objectives and are consistent with applicable laws, standards and best practices.

The Governance and Privacy Committee of CIHI's Board of Directors presides over the organization's Privacy Program. The Finance and Audit Committee of the Board presides over the organization's Information Security Program. In addition to the president and chief executive officer, the governance structure also includes a chief privacy officer and general counsel (CPO/GC) and a chief information security officer (CISO).

Both the CPO/GC and the CISO hold senior positions within the organization and, importantly, provide representation for their respective functions on senior decision-making and oversight bodies. These include the Governance and Privacy Committee of the Board, the Finance and Audit Committee of the Board, the Senior Management Committee and the Privacy, Confidentiality and Security Committee. Both the CPO/GC and the CISO are supported by a number of specific functional committees.

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

- Executive Committee
  - Chaired by the president and CEO; includes the president and CEO, vice presidents and executive directors
- Senior Management Committee
  - Chaired by the president and CEO; includes Executive Committee members and all directors
- IT Leadership Team
  - Chaired by the vice president and chief information officer (VP/CIO)
- Privacy, Confidentiality and Security Committee
  - Chaired by the CPO/GC
- Information Security Management System (ISMS) Steering Committee
  - Chaired by the VP/CIO; includes all Information Technology Services (ITS) directors and key ISMS personnel

- ISMS Working Group
  - Chaired by the senior program consultant, Information Security; includes senior ITS staff in support of CIHI's ISMS

The CPO/GC's and CISO's responsibilities are closely linked. Open and constant communication between the 2 functions is recognized as vital to a successful information governance model. Consequently, the CPO/GC and CISO coordinate their efforts in areas such as training and awareness and policy development.

To further ensure that CIHI's Privacy Program is representative of best practices, CIHI retains an external chief privacy advisor whose primary focus is to provide CIHI with timely advice about emerging privacy trends and issues, best practices, new developments in legislation, and the approaches and perspectives of the external privacy community.

b. Accountability, shared responsibilities and transparency

All CIHI employees play a significant role in the privacy and security of the data holdings at CIHI. The accountabilities set out in this document specifically relate to those committees and individuals who play leadership roles and carry specific accountability for privacy and security.

CIHI's Board of Directors recognizes the importance of the organization's privacy obligations and therefore established the Governance and Privacy 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 significant changes to CIHI's Privacy Policy and any other issue deemed relevant by the president and CEO and/or the CPO/GC.

Accountability for privacy and security ultimately resides with the president and CEO of CIHI, who has formally delegated these functions at an operational level to the CPO/GC and CISO, respectively.

The CPO/GC heads Privacy and Legal Services and is responsible for managing the Privacy Program, providing privacy advice and support to program areas, ensuring that the suite of privacy policies and procedures is comprehensive and up to date, providing privacy training and awareness, conducting privacy impact assessments (PIAs) and audits, monitoring compliance and benchmarking. The CPO/GC is also responsible for ensuring that appropriate data-sharing and other agreements are in place and for monitoring legal and other developments in the privacy arena.

The CISO heads Information Security and has overall day-to-day accountability for the confidentiality, integrity and availability of the data holdings within CIHI's custody and control and for ensuring that the Information Security Program and policy suite are robust and up to date. The CISO is also responsible for providing information security training and awareness, conducting risk assessments and audits, benchmarking and monitoring industry best practices in information security. The CISO reports all significant audit findings to the Finance and Audit Committee of the Board of Directors.

CIHI is committed to the principles of openness, transparency and accessibility by making this framework and its privacy and security policies available to the public on cihi.ca. Other documentation is also made available, including brochures, a description of CIHI's data holdings of personal health information, PIAs and documentation related to the Information and Privacy Commissioner of Ontario's review of CIHI's privacy and security practices.

3 Risk management

The CPO/GC and CISO maintain the Privacy and Security Risk Management (PSRM) Program. This program enables the organization to properly identify, evaluate, assess and manage privacy and security risks.

a. Privacy and Security Risk Management Program

CIHI has implemented its PSRM Program that aligns with the corporate Risk Management Program. Privacy and security risk management is a formal, repeatable process for identifying, assessing, treating and monitoring risks in order to minimize the probability of such risks materializing and/or the impact of such risks should they occur.

The PSRM Program informs and aligns with corporate risk management activities through

- Adopting a similar methodology, terminology and governance structure; and
- Identifying privacy and security risks for potential inclusion on the Corporate Risk Register.

CIHI employs a number of different privacy and security risk identification tools that inform the PSRM Program. Examples include PIAs, threat risk assessments (TRAs), vulnerability assessments and penetration tests ("ethical hacks"). PIAs and TRAs ensure that privacy and security principles are taken into account during the design, implementation and evolution of a program, initiative, process or system.

CIHI has effectively integrated PIAs into its business processes. CIHI's *Privacy Impact Assessment Policy* makes PIAs a shared responsibility between the program area staff or project manager and Privacy and Legal Services staff. PIAs are conducted in the design stage of new programs or when significant changes to existing programs occur, where such activity involves the collection, access, use or disclosure of personal information.

CIHI conducts TRAs to identify, assess and manage information security risks. In addition, vulnerability assessments and penetration tests are conducted or commissioned on a regular basis to identify risks to CIHI's information and information systems.

b. Benchmarking

CIHI's CPO/GC and CISO regularly assess the Privacy and Information Security programs' attributes and controls at CIHI against those of peer organizations, emerging trends and current national and international best practices. This activity informs the development of strategic, operational and tactical privacy and information security plans.

c. Compliance

The CPO/GC actively monitors the legislative and regulatory landscape to ensure CIHI continues to comply with all relevant legislation. Similarly, the CISO monitors the IT security environment to identify emerging trends and best practices.

CIHI has implemented an ISMS in accordance with ISO/IEC 27001:2013 and is subject to regular audits against this international standard.

Internally, CIHI's Code of Business Conduct requires that personnel comply with all privacy and security policies, procedures, standards and protocols, and that they reaffirm their commitment to an understanding of their obligations on a biennial basis. Violations of the Code of Business Conduct and the policies and practices it represents may result in disciplinary action up to and including dismissal.

d. Business continuity/disaster recovery

CIHI has implemented a comprehensive business continuity plan, which includes a supporting technology recovery plan. This plan is critical to the protection of CIHI's data holdings and vital records in the event of an emergency or a disruption in normal business operations. The CPO/GC and CISO are members of the Business Continuity Management team and ensure that privacy and information security concerns are considered and addressed during the recovery process.

4 Program controls

CIHI maintains a comprehensive suite of privacy and security policies, procedures, standards and guidelines. These policy instruments inform all information practices within the organization.

a. Policies

CIHI's *Privacy Policy on the Collection, Use, Disclosure and Retention of Personal Health Information and De-Identified Data, 2010* (Privacy Policy) and its *Information Security Policy* set the overall direction for other privacy and security policies, standards and guidelines.

CIHI's Privacy Policy is based on the Canadian Standards Association's *Model Code for the Protection of Personal Information* and is the foundation for the Privacy Program at CIHI. It embodies the internationally accepted privacy principles of minimal collection, identification of use, disclosure and retention, and the right of access and correction.

CIHI's *Information Security Policy* outlines CIHI's commitment to information security and the roles and responsibilities of all staff in the protection of information.

CIHI's privacy and security policies communicate, at a high level, the goals and directions set by the Board of Directors and senior management and reflect legislative requirements and best practices for the protection of information. CIHI's privacy and security policies are accessible, transparent and comprehensive. In 2005, 2008, 2011 and 2014, the Information and Privacy Commissioner of Ontario found that CIHI continued to have in place practices and procedures that sufficiently protect the privacy of the individuals whose personal health information it receives and that sufficiently maintain the confidentiality of that information. CIHI implements all recommendations made by the Information and Privacy Commissioner of Ontario as part of these reviews.

An ongoing policy review process ensures that all policies remain current and up to date.

b. Standards, procedures and protocols

CIHI has a comprehensive set of privacy and security standards, procedures and protocols to support the goals in the policies; examples include those on secure information life cycle, incident management and acceptable use of information systems.

c. Training and awareness

CIHI's Privacy and Security Framework is supported by an internal Training and Awareness Program that includes a number of key initiatives:

- CIHI's internal website includes comprehensive information about CIHI's Privacy and Information Security programs as well as links to policies, standards, guidelines and other privacy- and security-related instruments.
- CIHI's *Privacy and Security Training Policy* mandates documented and traceable privacy and security training, including
  - Privacy and security orientation for all new employees;
  - Ongoing privacy and security training at least annually for current employees; and
  - Ad hoc training and information sessions delivered on a regular basis to highlight new and emerging trends in privacy and information security.
- CIHI's annual Privacy and Security Awareness programs established September as Information Security Awareness Month and January as Privacy Awareness Month. Both of these awareness initiatives include crossover training and referring employees to both privacy and information security information.
- The InfoSec newsletter is published several times per year and includes information about CIHI's Information Security and Privacy programs, current and emerging privacy and security issues, and links to useful resources.

d. Secure information life cycle

CIHI has implemented administrative, technical and physical safeguards to protect personal information throughout its life cycle: creation and collection, access, retention and storage, use, disclosure and disposition. A comprehensive suite of policies and associated standards, guidelines and 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. This includes, for example, CIHI's *Policy on the Security of Confidential Information and Use of Mobile Devices/Removable Media* that specifies the necessary controls for protecting information stored on mobile or removable devices and requirements for strong encryption of personal information.

e. Incident Management Protocol

CIHI's *Privacy and Security Incident Management Protocol* requires a coordinated, orderly and timely response to privacy and security events and incidents in order to minimize the potential harm to CIHI or individuals whose information may be compromised.

All CIHI employees are expected to protect CIHI's data holdings and have an obligation to report privacy or security incidents, including any perceived deficiencies in privacy and security procedures and controls.

The CPO/GC and CISO provide ongoing joint communication and awareness to ensure corporate-wide compliance with the incident management protocol.

f. Agreements

CIHI is a leading source of credible health information and data in Canada. Hospitals, regional health authorities, health care practitioners and governments all entrust sensitive data to CIHI. Accordingly, CIHI is committed to maintaining the trust of its data suppliers by entering into information-sharing agreements that require CIHI to maintain the privacy and ensure the security of its data holdings.

In addition, CIHI administers a Third-Party Data Request Program for research purposes and other purposes consistent with CIHI's mandate. Prior to receiving data, a Non-Disclosure/ Confidentiality Agreement must be signed by all third parties who have been granted access to data for research purposes. This agreement requires individuals to comply with the conditions and restrictions imposed by CIHI relating to the collection, purpose, use, security, disclosure and return or disposal of data. It also permits CIHI to audit compliance upon reasonable notice.

g. Third-party provider management

All outsourcing and supplier arrangements involving confidential information or information systems are formally documented in written contracts with standard terms and conditions and require the execution of a confidentiality agreement. These contracts contain privacy and security requirements, confidentiality obligations and service-level objectives.

Access to data holdings or any other business information by service providers is conducted strictly in accordance with CIHI's privacy and security policies and procedures.

h. External communication

CIHI makes information about its privacy and security practices and programs readily available on its public website, including an overview of its Privacy and Information Security programs, key policies and standards, featured reports and publications, and contact information for the CPO/GC. PIAs and the statements of purpose for each data holding are also publicly available at cihi.ca.

CIHI values the role of the privacy regulators in Canada at the federal, provincial and territorial levels and actively seeks out their views and feedback where appropriate.

5 Audits, compliance and reporting

a. Privacy Audit Program

Privacy and Legal Services carries out CIHI's Privacy Audit Program, which is designed to monitor compliance with legislative or regulatory requirements, internal policy and contractual obligations pertaining to privacy and security. The *Privacy Audit Program — Terms of Reference* sets out 3 types of privacy compliance monitoring:

- Internal program audit: Internal program compliance with CIHI's Privacy Policy and privacy practices, which includes comparing internal practices against best practices;
- External data recipient audit: Data recipients' compliance with their obligations under their agreements with CIHI, including the Non-Disclosure/Confidentiality Agreement; and
- Topic audit: Corporate-level compliance with a focus on a particular subject area; priority is given to highly sensitive, visible or generally high-risk enterprise-wide activities.

b. Information Security Audit Program

The office of the CISO is responsible for CIHI's Information Security Audit Program. This program specifies a number of mandatory audits, including

- Compliance with ISO/IEC 27001:2013;
- Internal employee access to personal health information; and
- Vulnerability assessment and penetration testing of CIHI's physical and network infrastructure.

In addition to the mandatory audits, the CISO performs a number of ad hoc audits each year.

CIHI may perform additional audits as a result of

- An order/ruling from a privacy commissioner;
- A privacy or security incident or breach; and/or
- A request from CIHI's Board of Directors, senior management, CPO/GC or CISO.

c. External review of CIHI

CIHI's Privacy and Information Security programs are subject to a review every 3 years by the Information and Privacy Commissioner of Ontario. This review provides CIHI and its stakeholders with independent and objective verification that CIHI continues to have in place practices and procedures that sufficiently protect the privacy of individuals whose personal health information it receives and that sufficiently maintain the confidentiality of that information. The last review was conducted in 2014, and CIHI's status as a prescribed entity under Section 45 of Ontario's PHIPA was renewed.

d. Compliance monitoring/reporting

Recommendations arising from CIHI's privacy and security audits are tracked and monitored by senior management in a corporate-wide recommendation log. Responsibility for implementing recommendations rests with the relevant director or vice president.

The CPO/GC is responsible for submitting an annual privacy report to CIHI's Board of Directors that documents the accomplishments of the Privacy Program, including PIAs, privacy audits, policy development, training and other significant developments.

Under the Privacy Audit Program, CIHI prepares reports on all audits for the Governance and Privacy Committee of CIHI's Board of Directors. Under the Security Audit Program, the CISO reports all findings from external audits to the Finance and Audit Committee of the Board.

The CPO/GC and/or CISO may also be required to prepare additional presentations to the Board on sensitive privacy or security issues on an ad hoc basis.

Review of CIHI's Privacy and Security Framework

This framework is designed to be a living document and will be updated as privacy and information security practices evolve. CIHI will formally review this document and relevant policies at least yearly.

On an ongoing basis, the CPO/GC and CISO coordinate the review of all privacy and security policies, as well as any related procedures and practices, to ensure that they remain current and up to date and reflect evolving industry best practices.

Material changes to the Privacy Policy require approval from CIHI's Board of Directors. In other cases, the approval process and the extent of internal and external communication depend on the nature of the document and may require approval, for example, by the Executive Committee, Senior Management Committee or other internal committees.

Updates or changes to CIHI's privacy and security policies, procedures and practices reflect orders, guidelines, fact sheets and best practices issued by privacy commissioners and new or amended privacy and personal health information legislation relevant to CIHI.

For more information

CIHI's Strategic Plan, 2016 to 2021

Privacy Policy on the Collection, Use, Disclosure and Retention of Personal Health Information and De-identified Data, 2010 (Privacy Policy)

Information Security Policy

Privacy Policy on the Collection, Use, Disclosure and Retention of Health Workforce Personal Information and De-identified Data, 2011 (Health Workforce Privacy Policy)

Policy on the Security of Confidential Information and Use of Mobile Devices/Removable Media

Policy on Health Facility Identifiable Information

Privacy Impact Assessment Policy

Acceptable Use of Information Systems Policy

Privacy and Security Training Policy

Privacy and Security Incident Management Protocol

Privacy and Security Risk Management Framework

Privacy and Security Risk Management Policy

Privacy and Security Risk Management Methodology

help@cihi.ca

CIHI Ottawa
495 Richmond Road
Suite 600
Ottawa, Ont.
K2A 4H6
613-241-7860

CIHI Toronto
4110 Yonge Street
Suite 300
Toronto, Ont.
M2P 2B7
416-481-2002

CIHI Victoria
880 Douglas Street
Suite 600
Victoria, B.C.
V8W 2B7
250-220-4100

CIHI Montréal
1010 Sherbrooke Street West
Suite 602
Montréal, Que.
H3A 2R7
514-842-2226

cihi.ca

15206-0517