Privacy and Security Framework

2010

Updated October 2022

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
cihi.ca
copyright@cihi.ca

How to cite this document:
Canadian Institute for Health Information. *Privacy and Security Framework, 2010 — Updated October 2022*. Ottawa, ON: CIHI; 2022.

Cette publication est aussi disponible en français sous le titre *Cadre de respect de la vie privée et de sécurité, 2010 — mise à jour en octobre 2022*.

Table of contents

Introduction to privacy and information security at CIHI

This Privacy and Security Framework provides a coherent and comprehensive approach to enterprise privacy and information 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 information security officers, and entire governance structure, with a holistic view of the organization's privacy and information security practices. The framework is updated as CIHI's Privacy and Information Security programs evolve over time. It can also be used for the purposes of communicating CIHI's commitment to privacy and information 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

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 information 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 information 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, executive directors and the CPO/GC
- Senior Management Committee
  - Chaired by the vice president of Corporate Services; includes vice presidents, executive directors and all directors, including the CPO/GC and CISO
- IT Leadership Team
  - Chaired by the vice president and chief information
- 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 manager of Information Security and
    of CIHI's ISMS

CIHI is committed to the principles of openness, transparency and accessibility by making this framework and its suite of privacy and security policies available to the public on cihi.ca. Other documentation that must be made available includes the following:

- CIHI's Privacy Policy and other information (including brochures and/or frequently asked questions) related to the privacy and security policies, procedures and practices implemented by CIHI;
- A list of CIHI's data holdings of personal health information;
- PIAs;
- The mailing address and contact information for CIHI's CPO/GC and CISO, to whom people may direct inquiries, concerns or complaints regarding compliance with the privacy and security policies, procedures and practices implemented, and regarding compliance with the act and its regulations;
- A description of the Information and Privacy Commissioner of Ontario's role in reviewing and approving CIHI's policies, practices and procedures; and
- A notice that documentation in respect of these reviews and approvals is publicly available on the Information and Privacy Commissioner of Ontario's website.

At a minimum, the information made available (including in brochures and/or frequently asked questions) must include

- A description of CIHI's status as a prescribed entity under PHIPA, as well as of the duties and responsibilities arising from this status and the policies implemented;
- The types of personal health information collected and from whom the personal health information is typically collected;
- The purposes for which personal health information is collected and used, and if identifiable information is not routinely used, the nature of the information that is used;
- The circumstances in which and the purposes for which personal health information is disclosed and the persons or organizations to which it is typically disclosed;
-

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 information security risks.

a. Privacy and Security Risk Management Program

CIHI has implemented its PSRM Program in alignment 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 information 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, privacy and security incidents, vulnerability assessments and penetration tests ("ethical hacks"). PIAs ensure that privacy and security principles are taken into account during the design, implementation and evolution of a program, initiative, process or system (privacy and security by design).

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 information security risk assessments 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 information 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 information 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 information 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 information security policies are accessible, transparent and comprehensive. In 2005, 2008, 2011, 2014, 2017 and 2020, 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 determines whether amendments and/or new policies, procedures and practices are necessary. Updates or changes to CIHI's privacy and information security policies, procedures and practices 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 regulations;
- Evolving industry privacy and information security standards and best practices;
- Amendments to the act and its regulations relevant to CIHI as a prescribed entity;

- Recommendations arising from privacy and information security audits, privacy impact assessments and investigations into privacy complaints, privacy and information security breaches or incidents;
- Whether the privacy policies, procedures and practices of the prescribed person or prescribed entity continue to be consistent with its actual practices; and
- Whether there is consistency between and among the privacy and information security

  - 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 Information 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.

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 and information security 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.

Corporate-wide awareness of the incident management protocol is addressed as part of CIHI's privacy and security training program.

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(waren32ro)TjEMC[ApEMC121.99169929D 661BDCBT0 0 0 rg/TT0 154rly n1 for example, CIH

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, an agreement must be signed requiring recipients 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 supplier management

All outsourcing and supplier arrangements involving confidential information or information systems are formally documented in written contracts that contain privacy and information security requirements, confidentiality obligations and service-level objectives.

a. Privacy Audit Program

The CPO/GC is responsible for CIHI's Privacy Audit Program, which is designed to monitor compliance with legislative or regulatory requirements, internal policy and contractual obligations pertaining to privacy. The *Privacy Audit Program* is anchored by CIHI's Privacy Audit Policy and the related Multi-Year Privacy Audit Plan, the latter being approved annually by the Governance and Privacy Committee of CIHI's Board of Directors. CIHI conducts 2 types of privacy audits:

- Internal privacy audits assess internal staff compliance with CIHI's Privacy Policy and privacy best practices, or focus on how a particular issue is managed across the organization. Internal privacy audits are initiated as the need arises and often occur within the context of CIHI's internal incident and breach response processes. Internal privacy audits may also be performed in response to external factors such as an investigation, recommendation or order from a privacy commissioner or ombudsman.
- Third-party audits focus on external recipients of CIHI data. The audits evaluate compliance with the terms of the agreement governing the use of CIHI data. The audits also make recommendations to address any issues identified. In order to determine which audits will be performed in a given year, CIHI considers a range of criteria, including sensitivity of data, complexity of the research data management plan and risk intelligence derived from the Privacy and Legal Services department's ongoing compliance monitoring activities (e.g., annual data recipient compliance certification process).

b. Information Security Audit Program

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 privacy and/or security 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 2020, 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 information 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 updated as privacy and information security practices evolve.

For more information

Information about CIHI's Privacy and Information Security programs is available on CIHI's website.