Canadian Institute for Health Information

Information Security Policy

Introduction

The Canadian Institute for Health Information (CIHI) is committed to protecting the privacy of individuals and ensuring the security of their personal health information.

CIHI is a secondary collector of personal health information. To receive this information, CIHI has entered into bilateral and data-sharing agreements with most provinces/territories and other health care stakeholders across Canada. Pursuant to these agreements, CIHI has contractual obligations to protect the security and the confidentiality of the information that it receives from its data providers. As well, CIHI is a prescribed entity under Section 45 of the Ontario *Personal Health Information Protection Act* (PHIPA). As a prescribed entity, CIHI is subject to independent oversight by the Office of the Information and Privacy Commissioner of Ontario and must have its information practices reviewed and approved by the commissioner's office every 3 years. This review process provides our stakeholders with the assurance that CIHI's information management practices comply with PHIPA and with privacy and security standards of practice expected from that office. As a result, CIHI adheres to this and any other applicable privacy legislation.

CIHI is committed to safeguarding its IT (information technology) 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.

Purpose

The purpose of the *Information Security Policy* is to

- Provide CIHI Staff with direction and support for information security in accordance with business requirements and relevant laws and regulations; and
- Outline the responsibilities of CIHI Staff with respect to information security.

Scope

This policy and all related standards, guidelines and procedures apply to all CIHI Staff, contractors, consultants, temporary workers and students.

Policy

CIHI management supports the development and maintenance of the Information Security Program in accordance with business, legal and privacy requirements. This program must address, at minimum, the following control objectives and practices:

- A security governance framework;
- Privacy and Security Risk Management;
- Ongoing review of the security policies, procedures and practices implemented;
- An information security awareness and training program for all employees;
- Policies, standards, practices and/or procedures for ensuring the physical security of the premises, the security of information processing facilities and the protection of information throughout its life cycle (creation, acquisition, retention and storage, use, disclosure and disposition), including policies and procedures related to mobile devices, remote access and security of data at rest;
- An access management process for information and information processing facilities;
- Secure systems acquisition, development and maintenance;
- Technical vulnerability management;
- A cybersecurity program;
- Security audits;
- Acceptable use of information technology;
- Security in backup and recovery;
- Business continuity and disaster recovery;
- Information security incident management;
- Protection against malicious and mobile code; and
- Continuous improvement of the Information Security Program.

CIHI is committed to ensuring that reasonable steps are taken to ensure that personal health information is protected against loss or theft as well as unauthorized access, disclosure, copying, use, modification and disposal.

Responsibilities

The following CIHI individuals/groups have specific responsibilities for the Information Security Program:

- All CIHI Staff
- Senior Management
- Vice President and Chief Information Officer
- Chief Information Security Officer
- Chief Privacy Officer and General Counsel
- Director, People and Workplace Operations
- Senior Consultant, Cybersecurity
- Manager, Information Security

All CIHI Staff

All information under the care and control of CIHI is a corporate asset and must be securely managed throughout its life cycle. The protection of CIHI's information assets is a responsibility of all Staff, and Staff must understand and agree to their obligation to protect such assets throughout the information life cycle — creation, acquisition, retention and storage, use, disclosure and disposition. CIHI Staff shall create, acquire, retain, store, use, disclose, transfer or dispose of information only in accordance with CIHI's policies, standards and guidelines.

CIHI Staff must at all times engage in practices that are consistent with published information security policies, procedures, standards and guidelines. Additionally, CIHI Staff are obliged and expected to report all information security incidents and suspected information security incidents immediately upon learning of them. (For more information, refer to the *Privacy and Security Incident Management Protocol*.)

Senior Management

Senior Management shall provide the necessary guidance and support for the development and maintenance of the Information Security Program, in line with privacy and legal requirements and business strategy objectives.

This support includes, but is not limited to, the following:

- Integrating information security goals into relevant processes;
- Providing clear direction and visible management support for information security initiatives;
- Providing the resources required for information security; and
- Approving assignment of specific roles and responsibilities for information security across the organization.

Vice President and Chief Information Officer (VP/CIO)

The VP/CIO has overall responsibility for information security and represents CIHI's Executive Committee. They shall ensure that information security goals are identified, meet organizational requirements and are addressed within the Information Security Program.

Chief Information Security Officer (CISO)

Reporting to the VP/CIO, the CISO is responsible and accountable for leading CIHI's Information Security Program, which includes defining goals, objectives and metrics consistent with the corporate Strategic Plan and CIHI's Privacy Program to ensure that the organization's security principles, policies, procedures and practices support the protection of the organization's information. The CISO shall manage and coordinate the design, implementation, operation and maintenance of CIHI's Information Security Management System (ISMS).

In addition, the CISO shall actively foster a culture of information security by leading and supporting activities both internally and externally to increase awareness of CIHI's information security principles, policies and procedures.

Chief Privacy Officer and General Counsel (CPO/GC)

The CPO/GC is responsible for informing the CISO of relevant legislative, regulatory and contractual obligations. In addition, the CPO/GC shall collaborate with the CISO on key aspects of the privacy and security program, including but not limited to

- Privacy and security risk management;
- Privacy and security incident management; and
- Training and awareness.

Director, People and Workplace Operations

The Director, People and Workplace Operations, is responsible for the following in support of CIHI's information security objectives:

- The physical security of the premises;
- Records and information management policies, procedures and practices; and
- Security in Human Resources processes.

Senior Consultant, Cybersecurity

The Senior Consultant, Cybersecurity, is responsible for oversight of CIHI's Information Security Program. Specifically, they shall create and maintain

- A cybersecurity program aligned with CIHI's information security objectives; and
- A suite of information security policies, procedures, standards and guidelines to protect the confidentiality, integrity and availability of CIHI's information assets.

The Senior Consultant, Cybersecurity, is also responsible for the continued compliance and certification of CIHI's information security practices, including the requirements pursuant to Ontario's PHIPA.

Manager, Information Security

The Manager, Information Security, oversees the implementation and maintenance of CIHI's security architecture in alignment with CIHI's Information Security Program.

Compliance, audit and enforcement

CIHI's Code of Business Conduct describes the ethical and professional behaviour related to work relationships, information — including personal health information — and the workplace. The code requires all employees to comply with the code and all CIHI's policies, procedures and practices. Instances of non-compliance with privacy and security policies are managed through CIHI's *Privacy and Security Incident Management Protocol*, which requires Staff to immediately report incidents and breaches to incident@cihi.ca, including non-compliance with this policy. Policy owners are responsible for ensuring compliance with the policies, procedures and practices. Violations of the code — including violation of privacy and security policies, procedures and practices — are referred to People and Workplace Operations, as appropriate, and may result in disciplinary action up to and including dismissal, in accordance with the CIHI Employee Discipline Guidelines. Compliance is monitored through either CIHI's *Privacy Audit Policy* or CIHI's Information Security Audit Program, as applicable.

Glossary

Business record

Business records comprise any information created, received or maintained as evidence and information by CIHI, in the transaction of business or in the pursuance of legal obligations.

Business records may be in physical or electronic form and include, but are not limited to,

- Information collected from data providers, clients and stakeholders;
- Official organizational records;
- Transitory records; and
- Records in the public domain owned by CIHI.

CIHI Staff

Any worker at CIHI, including all full-time or part-time employees, secondments, temporary workers, students and contract employees, including external consultants or other third-party service providers whose role includes responsibility for the secure storage of personal health information.

Information asset

For the purposes of this policy, information or information assets shall include the following:

- All health information maintained by CIHI for the purposes of meeting our mandate; and
- All business records of the organization, regardless of the security classification.

Information may be in physical or electronic format.

Information security

The concepts, techniques, technical measures and administrative measures used to protect information assets from deliberate or inadvertent unauthorized acquisition, damage, disclosure, manipulation, modification or loss.

For more information
security@cihi.ca

How to cite this document:
Canadian Institute for Health Information. *Information Security Policy*. Ottawa, ON: CIHI; 2024.