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 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 the Canadian public 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 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 management and staff with direction and support for information security in accordance with business requirements and relevant laws and regulations; and
- Outline the responsibilities of management and staff with respect to information security.

Security Classification: Public

Scope

This policy and all related standards, guidelines and procedures apply to all employees, contractors, consultants, temporary employees and other workers at CIHI.

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;
- The Privacy and Security Risk Management Framework;
- Ongoing review of the security policies, procedures and practices implemented;
- An information security awareness and training program for all staff;
- 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 lifecycle (creation, acquisition, retention and storage, use, disclosure and disposition);
- An access management process for information and information processing facilities;
- Secure systems acquisition, development and maintenance;
- Technical vulnerability management;
- Security audits;
- Acceptable use of information technology;
- Security in backup and recovery;
- Business continuity and disaster recovery; and
- Information security incident management.

Specific obligations and responsibilities of management and staff in support of the Information Security Program are outlined below.

Responsibilities

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

- All staff
- Senior management
- Chief information officer
- Chief information security officer
- Senior program consultant, Information Security
- Director, Human Resources and Administration

All staff

All information under the care and control of CIHI is a corporate asset and must be securely managed throughout its lifecycle. The protection of CIHI's information assets is a basic responsibility of all staff, and staff must understand and agree to their obligation to protect such assets throughout the information lifecycle — 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, and with applicable legislation.

Staff must at all times engage in practices that are consistent with published information security policies, procedures, standards and guidelines. Additionally, 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.

Chief information officer (CIO)

The CIO has overall responsibility for information security and represents CIHI's Executive Committee. He or she 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 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) within the defined scope.

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.

Director, Human Resources and Administration

The director, Human Resources and Administration, 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 program consultant, Information Security

The senior program consultant, Information Security, is responsible for the day-to-day oversight of CIHI's ISMS and for creating and managing key corporate IT security initiatives. He or she is responsible for developing and maintaining the necessary practices to ensure the ongoing security and integrity of CIHI's data holdings in accordance with CIHI's Privacy and Security Framework and suite of privacy and security policies, procedures, standards and guidelines. He or she shall also ensure that CIHI is employing industry best practices in information security and is meeting the expectations/requirements of key external stakeholders (e.g., the Information and Privacy Commissioner of Ontario).

Compliance

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 of CIHI's policies, protocols and procedures. Compliance with CIHI's privacy and security program is monitored, and instances of non-compliance with privacy and security policies are managed through the *Privacy and Security Incident Management Protocol*. Violations of the code, including violation of privacy and security policies, procedures and protocols, are referred to Human Resources, as appropriate, and may result in disciplinary action up to and including dismissal.

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.

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.

Staff

All full-time, part-time and casual employees of CIHI, including individuals working at CIHI on secondment, students, volunteers, contractors and consultants.

For more information

security@cihi.ca