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-

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.

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.