Policy on Privacy and Security Risk Management

Purpose

This *Policy on Privacy and Security Risk Management* sets out the requirements for CIHI to identify, assess, treat and monitor privacy and security risks, as well as associated roles and responsibilities.

Scope

All staff at CIHI play a role in identifying and managing privacy and security risks.

Definitions

Impact: A measurement of the severity of a risk.

Likelihood: A measurement of the chance that a risk might occur.

Mitigating action: The action to be taken to reduce the likelihood and/or impact of a risk.

Privacy and security risk: The possibility that an event may occur that

- Results in non-compliance with privacy laws and regulations or CIHI's privacy and information security policies or procedures;
- Results in a failure to safeguard or prevent unauthorized collection, use or disclosure of personal information, or more generally the confidentiality, integrity and availability of CIHI's data holdings; or
- Otherwise jeopardizes CIHI's status under the *Personal Health Information Protection Act, 2004* (PHIPA).

All of these would adversely affect the achievement of CIHI's strategic goals.

Privacy and security risk management (PSRM): A formal, repeatable process for identifying, assessing, treating and monitoring risks in order to minimize the probability of such risks materializing and/or their impact should they occur.

Privacy and Security Risk Register: A consolidated list of CIHI's current identified privacy and security risks.

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

Risk treatment: The modification of risk by mitigation, transfer, avoidance or acceptance of the risk.

Risk treatment plan: The identified process and implementation of options to mitigate, transfer, avoid or accept a risk.

Policy

CIHI shall establish a Privacy and Security Risk Management (PSRM) Program and associated processes that

- Ensure privacy and information security risks are properly identified, assessed, treated and monitored;
- Integrate with CIHI's Corporate Risk Management Program;
- Ensure CIHI meets its legal obligations and regulatory expectations with respect to privacy and information security; and
- Contribute to CIHI's culture of privacy and security risk awareness.

Roles and responsibilities

1. **CIHI's Executive Committee** (EC) is responsible for
   - Accepting on behalf of the corporation risks that are higher than CIHI's risk tolerance level.
2. **CIHI's Senior Management Committee** is responsible for PSRM across CIHI and for
   - Providing input on potential additional mitigation strategies for risks that are higher than CIHI's risk tolerance level prior to bringing risks to EC for acceptance; and
   - Reviewing and resolving any escalations from the chief privacy officer (CPO) and/or chief information security officer (CISO) with respect to privacy and security risk treatment.
3. The **Privacy, Confidentiality and Security Committee** is responsible for
   - Overseeing CIHI's Privacy and Security Risk Register.
4. **Senior managers or other identified owners** are responsible for PSRM within their area and for
   - Collaborating with the CPO and CISO to identify possible privacy and security risks that exist or may arise in their area;
   - Assisting the CPO and CISO in developing a plan to treat privacy and security risks;
   - Monitoring all privacy and security risks applicable to their area; and
   - Reporting quarterly to the CPO and CISO on the status of all risk treatment plans within their area.

5. The **CPO and CISO** are responsible for CIHI's PSRM processes and for
    - Developing and implementing a PSRM strategy, including but not limited to this policy and a PSRM Framework that aligns with CIHI's Corporate Risk Management Program and supports the Information Security Management System Risk Management Program;
    - Collaborating with CIHI's senior managers to identify privacy and security risks throughout CIHI and recommending risk treatment in accordance with the PSRM Program;
    - Assessing privacy and security risks, in accordance with the PSRM methodology;
    - Maintaining the Privacy and Security Risk Register, in accordance with the PSRM Framework;
    - Reporting to senior managers or other identified owners any privacy and security risks that are applicable to their area;
    - Assisting senior managers or other identified owners with developing a risk treatment plan for their risks;
    - Monitoring all privacy and security risks in the Privacy and Security Risk Register, including an annual review of the assessments and risk treatment plans;
    - Recommending for possible inclusion in CIHI's Corporate Risk Register any privacy and security risks that may meet the definition of a corporate risk, as set out in the Corporate Risk Management Program;
    - Providing quarterly risk mitigation progress reports to the Senior Management Committee; and
    - Reviewing this policy and the PSRM Framework on an annual basis.

Related policies and procedures/ supporting documents

Privacy and Security Risk Management Framework

For more information, please contact

security@cihi.ca

privacy@cihi.ca

How to cite this document:
Canadian Institute for Health Information. *Policy on Privacy and Security Risk Management*. Ottawa, ON: CIHI; 2022.