

# Privacy and Security Training Policy

## Purpose

The purpose of this policy is to set out the requirements for traceable, mandatory privacy and security training for all Canadian Institute for Health Information (CIHI) staff.

Staff training is essential to the development and maintenance of a culture of privacy and security within the organization. It is also an essential preventive measure against unauthorized collection, access, use and disclosure of personal health information. Training efforts will be focused on reducing risk for the organization and supporting staff in fulfilling CIHI's mandate, in compliance with its policies and applicable legislation.

## Scope

This policy applies to all CIHI staff, including all full-time, part-time and contract employees of CIHI, individuals working at CIHI on secondments, students and certain external professional services (EPS) consultants who require access to CIHI data or information systems as defined in CIHI's Acceptable Use Policy. Any exceptions to mandatory privacy and security training requirements must be approved by the chief privacy officer (CPO) and/or the chief information security officer (CISO).

## Policy

### Interpretation

1. This policy will be interpreted with the following 2 guiding principles:
  - a. Privacy and security training is mandatory; and
  - b. Privacy and security training is traceable to ensure compliance.

## Mandatory privacy and security onboarding (orientation) training

2. All new CIHI staff must successfully complete CIHI's mandatory privacy and security onboarding training within 15 days of commencement of employment and prior to gaining access to any personal health information. The training includes content on privacy and security fundamentals, acceptable use of information systems at CIHI, risks associated with social engineering/phishing and incident management.
3. The effective date in the letter of employment or the contract with CIHI is deemed to be the commencement of employment.

## Mandatory ongoing training

4. All CIHI staff must successfully complete CIHI's mandatory privacy and security annual renewal training prior to January 31, starting the year following the year of commencement of employment. Ongoing training will also include role-based training in order to
  - a. Ensure that employees understand how to apply the privacy and security policies, procedures and practices in their day-to-day employment, contractual or other responsibilities;
  - b. Address any new privacy and security policies, procedures and practices, as well as significant amendments to existing privacy and security policies, procedures and practices; and
  - c. Address any recommendations about privacy and security training made in privacy impact assessments, privacy and security audits, and the investigation of privacy and security breaches and privacy and security complaints.
5. All CIHI staff must also complete the online *Annual Renewal of CIHI Agreement Respecting Confidential Information and Privacy*.

## Content of the Privacy and Security Training Program

6. The CPO is responsible for determining the content of privacy training, and the CISO is responsible for determining the content of security training.
7. The following elements must be included in CIHI's Privacy and Security Training Program in order to ensure its accuracy and relevance:
  - CIHI's status under the Ontario *Personal Health Information Protection Act* (PHIPA) and the duties and responsibilities that arise as a result of this status;
  - The nature of the personal health information collected and from whom this information is typically collected;

- The purposes for which personal health information is collected and used, and how this collection and use is permitted by PHIPA;
- Limitations placed on access to and use of personal health information by employees;
- The procedure that must be followed in the event that an employee is requested to disclose personal health information;
- An overview of CIHI’s privacy and security policies, procedures and practices and the obligations arising from them;
- The consequences of a breach of the privacy and security policies, procedures and practices implemented;
- An explanation of the Privacy Program, including the key activities of the program and the CPO;
- An explanation of the Security Program, including the key activities of the program and of the CISO and the manager of Information Security;
- The administrative, technical and physical safeguards implemented by CIHI to protect personal health information against theft, loss and unauthorized use or disclosure and to protect records of personal health information against unauthorized copying, modification or disposal;
- The duties and responsibilities of employees in implementing the administrative, technical and physical safeguards put in place by CIHI;
- A discussion of the nature and purpose of the confidentiality agreement that employees must execute and the key provisions of the confidentiality agreement; and
- An explanation of the *Privacy and Security Incident Management Protocol* and the duties and responsibilities imposed on employees in terms of identifying, reporting, containing and participating in the investigation and remediation of privacy and security incidents.

## Privacy and security awareness

8. CIHI is committed to ensuring a culture of privacy and security at CIHI through an ongoing awareness program in addition to its formal training program, and has consequently adopted a multi-pronged approach to raising awareness. This includes
  - Articles on CIHighway (CIHI’s intranet-based communication mechanism);
  - Staff presentations and special presentations at departmental meetings;
  - The “January is Privacy Awareness Month at CIHI” campaign;
  - The “September is Information Security Awareness Month at CIHI” campaign;
  - Small Talks (lunch and learns);
  - Privacy and security awareness posters and mouse pads;

- A summary of investigations completed by privacy commissioners and ombudsmen across Canada, where orders have been issued, that are health care–related and could have implications for CIHI with respect to managing its Privacy and Security Program;
  - An incident management desktop tool provided to all staff;
  - All-staff emails; and
  - Technical training for specific positions.
9. The CPO and CISO will determine the frequency, method and nature of the above communications.

## **Responsibility for tracking completion of mandatory privacy and security training**

10. Privacy and Legal Services (PLS) is responsible for maintaining a log and tracking the completion of onboarding and annual renewal training, as well as any additional mandatory privacy and security training that may be identified by the CPO and/or the CISO. PLS will report rates of completion to the Senior Management Committee.

## **Consequences of non-compliance**

11. The training requirements set out above must be met prior to gaining initial access to data and on an annual basis thereafter in order to retain access privileges.
12. Failure to successfully complete mandatory privacy and security training may result in denial or revocation of access to data or other components of CIHI's infrastructure (e.g., the CIHI network).
13. The decision to deny or revoke access will be made by the CISO and CPO in consultation with the director of Human Resources, in the case of CIHI staff, or with the director/manager of the contracting area in the case of EPS.
14. In addition to denial or revocation of access, failure to successfully complete mandatory training may result in disciplinary action, including the termination of employment or other relationship with CIHI.

## Compliance, audit and enforcement

15. 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 CIHI's *Privacy and Security Incident Management Protocol*. Violations of the code, including violations 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.

## Related policies/procedures and supporting documents

- *Procedure: Privacy and Security Training*
- *CIHI Code of Business Conduct*
- [Privacy and Security Incident Management Protocol](#)

**For more information, please contact**



[privacy@cihi.ca](mailto:privacy@cihi.ca)

How to cite this document:

Canadian Institute for Health Information. *Privacy and Security Training Policy*. Ottawa, ON: CIHI; September 2022.