Commitment to Privacy and Security

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 prescribed entity under s. 45 of the Ontario *Personal Health Information Protection Act* (PHIPA) and is authorized to collect personal health information in Ontario, without consent, for the purposes of analysis or compiling statistical information for the planning and management of the health system. As a prescribed entity, CIHI is subject to independent oversight by the Ontario Information and Privacy Commissioner and must have its information practices reviewed and approved by the Commissioner every three years. This review process provides the Canadian public with the assurance that CIHI's information management practices comply with PHIPA, and with recognized privacy and security standards of practice. CIHI adheres to PHIPA and any other applicable privacy legislation.

CIHI recognizes that access to the health data holdings, and in particular the personal health information within those data holdings, is a privilege with corresponding individual and collective responsibilities. Staff training is essential to the development and maintenance of a culture of privacy and security within the organization.

A robust training program is important to ensuring meaningful and well-understood privacy and security policies. It is also an essential preventative 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.

Policy Objective

The purpose of this policy is to set out the requirements for traceable, mandatory privacy and security training for all CIHI staff.

Effective Date and Application

This policy and the training program are in effect as of January 2010 and apply 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 consultants, such as those who require access to CIHI data, or information systems as defined in CIHI's Acceptable Use Policy.

The Director of Human Resources will address any ambiguity as to the application of this policy.

The Policy Custodian

This policy forms part of CIHI's privacy and security program. CIHI's Chief Privacy Officer (CPO) is the custodian of this policy and has the authority and responsibility for its day-to-day implementation.

CIHI Policy

Interpretation

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

Commencement of Employment

2. Commencement of employment is the effective date in the letter of employment or the contract with CIHI.

3. All new CIHI staff must successfully complete CIHI's mandatory privacy and security orientation training within 15 days of commencement of employment and prior to gaining access to any personal health information. The orientation training includes but is not limited to:
   a. Privacy and Security Fundamentals;
   b. Introduction to Information Security at CIHI;
   c. Acceptable Use of Information Systems at CIHI; and
   d. CIHI Privacy Breach and InfoSec Incident management Protocols.

Content of the Privacy and Security Training Program

4. The CPO will be responsible for determining the content of privacy training and the Chief Technology Officer (CTO) will be responsible for determining the content of security training.

5. The following elements must be included in CIHI's privacy and security training program in order to ensure its accuracy and relevancy:

   - 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 these policies, procedures and practices;
- The consequences of 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 Chief Privacy Officer;
- An explanation of the security program, including the key activities of the program and of the Chief Technology Officer and Senior Program Consultant, 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 Breach Management Protocol* and the duties and responsibilities imposed on employees in identifying, reporting, containing and participating in the investigation and remediation of privacy breaches; and
- An explanation of the *Information Security Incident Management Protocol* and the duties and responsibilities imposed on employees in identifying, reporting, containing and participating in the investigation and remediation of information security breaches.

Annual Renewal Training

6. All CIHI staff must successfully complete CIHI's mandatory privacy and security yearly renewal training, prior to January 31, starting the year following the year of commencement of employment, and complete the "Annual Renewal of CIHI Employee Agreement Respecting Confidential Information and Privacy"

Additional Training

7. In addition to the requirements set out above, all CIHI staff is required to successfully complete additional mandatory privacy and security training, as identified by the CPO and the CTO. For example, this additional training may be in response to a privacy breach or security incident, the release of findings from a privacy or security audit, or the adoption and implementation of new policies and procedures.

Responsibility for Tracking Completion of Training

8. The Privacy and Legal Services Secretariat is responsible for tracking the completion of mandatory privacy and security training and for ensuring compliance, and will report rates of completion to the Senior Management Team.

Consequences of Non-Compliance

9. The training requirements set out above must be met prior to gaining initial access to data or other components of CIHI's infrastructure (for example, the CIHI network) and on an annual basis thereafter in order to retain access privileges.

10. Failure to successfully complete mandatory privacy and security training will result in denial or revocation of access to data or other components of CIHI's infrastructure (for example, the CIHI network).

11. 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.

Revocation of Access Privileges

12. The CTO, on the recommendation of the CPO and the Director of Human Resources, will be responsible for revoking access privileges for anyone who has not completed the mandatory training set out above.

Audit

13. The CPO may audit at any time to ensure compliance with this policy and will report his or her findings to CIHI's senior management team.