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.

-

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.