Canadian Institute for Health Information

Policy on the Security of Confidential Information and Use of Mobile Devices/Removable Media

Purpose

The purpose of this policy is to ensure

a. That Confidential Information is protected and retained only on authorized CIHI computing devices/media and in authorized locations; and

b. That Confidential Information temporarily stored on CIHI's mobile devices and removable media is secured in the event of theft or loss and is protected against unauthorized use, access, copying, modification, disclosure or disposal.

Scope

This policy applies to all CIHI staff (including all full-time or part-time employees, contract employees, secondments, temporary workers and students) and certain external professional services consultants, such as those who require access to CIHI's data or information systems as defined in CIHI's *Acceptable Use of Information Systems Policy*.

This policy does not apply to information burned on CDs or DVDs for data releases to external clients. The dissemination of data to external clients is subject to the *Methods of Dissemination Standard*.

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

Definitions

"CIHI Computing Devices/Media" means any computing device or media in the custody/control of CIHI or issued by CIHI to its staff, including but not limited to any mobile device.

"Confidential Information," for the purposes of this policy, means Personal Health Information, Health Workforce Personal Information, De-Identified Data and Technical Information.

"Personal Health Information" means health information about an individual that identifies the specific individual, may be used or manipulated by a reasonably foreseeable method to identify the individual, or may be linked by a reasonably foreseeable method to other information that identifies the individual.

"Health Workforce Personal Information" means information about a health service provider that identifies the specific individual, may be used or manipulated by a reasonably foreseeable method to identify the individual, or may be linked by a reasonably foreseeable method to other information that identifies the individual.

"De-identified data" means Personal Health Information or Health Workforce Personal Information that has been modified using appropriate de-identification processes so that the identity of the individual cannot be determined by a reasonably foreseeable method.

"Mobile Device" means any electronic device that provides mobile connectivity to CIHI's networks. This includes but is not limited to smart phones, tablets and laptops.

"Privacy and Security Risk Management (PSRM)" means 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.

"Removable Media" means any removable device capable of storing information. This includes but is not limited to CDs, DVDs and USB drives.

"Technical Information" means information about CIHI's networks, servers, applications or computing environments. Technical information includes but is not limited to

- Log files;
- Network topology information;
- Operating systems, software or hardware systems, and versions of same;
- Application development technologies;
- Information about CIHI's hardware or software security controls;
- Application code; and
- System configuration files.

Policy

As a general rule, employees are to perform work on CIHI's premises using CIHI-issued computing devices/media and/or over its secure networks and in keeping with CIHI's privacy and security policies, procedures, standards and guidelines.

Specifically,

Personal Health Information

- Shall not be removed from CIHI's premises in paper form;
- Shall not be sent by email, either internally or externally, unless authorized and with appropriate safeguards; and
- Shall not be stored on mobile devices or removable media except in specific and exceptional circumstances where a PSRM assessment has been undertaken and where prior approval has been given by the relevant vice president.

Health Workforce Personal Information

- Shall not be removed from CIHI's premises in paper form;
- Shall not be sent by email, either internally or externally, unless authorized and with appropriate safeguards; and
- Shall not be stored on mobile devices or removable media except in specific and exceptional circumstances where a PSRM assessment has been undertaken and where prior approval has been given by the relevant vice president.

De-Identified Data

- Shall not be removed from CIHI's premises in paper form;
- Shall not be sent by email, either internally or externally, unless authorized and with appropriate safeguards; and
- Shall not be stored on mobile devices or removable media except in specific and exceptional circumstances where a PSRM assessment has been undertaken and where prior approval has been given by the relevant vice president.

Technical Information

- Shall not be removed from CIHI's premises in paper form;
- May be sent by email internally only; and
- Shall not be stored on mobile devices or removable media unless the mobile device or the media is encrypted according to CIHI's current encryption standards.

CIHI staff are prohibited from retaining Confidential Information on a mobile device or removable media if other information (e.g., de-identified and/or aggregate information) will serve the identified purpose. When using mobile devices or removable media, and the requisite approval has been obtained,

1. Only the minimum amount of Confidential Information required for the identified purpose may be stored on mobile devices and removable media on a temporary basis;
2. Once the identified purpose for temporarily storing the Confidential Information on mobile devices and removable media has been accomplished, the Confidential Information shall be removed or destroyed, where possible, within 5 days of completion; and
3. Confidential Information temporarily stored on mobile devices and removable media will be
    a. Stored on CIHI-issued equipment;
    b. De-identified to the fullest extent possible; and
    c. Encrypted and password protected in keeping with CIHI's current encryption and password standards (see *File Encryption Procedures* and *User Name and Password Standard*). Mobile devices must be password protected.

Compliance

CIHI Code of Business Conduct describes ethical and professional behaviour related to work relationships, information (including personal health information) and the workplace. The code requires all employees to comply with it 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 the *Privacy and Security Incident Management Protocol*. Violations of the code, including violation 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

Acceptable Use of Information Systems Policy

Secure Information Storage Standard

Secure Information Transfer Standard

File Encryption Procedures

User Name and Password Standard

For more information, please contact

security@cihi.ca

privacy@cihi.ca