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.

This policy does not apply to information stored on Removable Media for data releases to external clients. The dissemination of data to external clients is subject to the *Secure Information Transfer 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 to CIHI Staff, including but not limited to any Mobile Device.

CIHI Staff means all full-time, part-time and contract employees of CIHI, individuals working at CIHI on secondment, students, temporary workers and certain external professional services consultants or providers who require and are authorized to access CIHI data or information systems as defined in CIHI's *Acceptable Use Policy*.

Confidential Information, for the purposes of this policy, means information that is highly sensitive in nature and that must be secured against loss or theft, as well as against unauthorized access, disclosure, copying, use or modification throughout its life cycle, ensuring the confidentiality, integrity and availability of information. Confidential Information includes but is not limited to Personal Health Information, Personal Information, Health Workforce Personal Information, De-Identified Data and Technical Information.

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.

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.

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.

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.

Personal Information means any factual or subjective information, regardless of its format, that can be used, either alone or in combination with other information, to identify an individual, including photographs and videos. Personal Information does not include information that relates to an individual's business position or function (e.g., position or title, business address, business telephone number or email address).

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

- Specific technologies in use at CIHI;
- Log files and dump files;
- Network and application topologies/diagrams;
- Operating systems, software or hardware systems and versions;
- Application development tools and technologies;
- Information about CIHI's information security controls;
- Application code;
- System configuration files;
- Data models and database schema information; and
- Results of information security audits assessing CIHI's information processing systems.

Policy

1.0 CIHI Staff are to perform work either on CIHI's premises or over its secure networks, using CIHI-issued computing devices/media and in keeping with CIHI's privacy and security policies, procedures, standards and guidelines, subject only to any specific and exceptional circumstances as set out below.

Specifically,

1.1 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 as set out in the *Secure Information Transfer Standard*;
- Shall not be stored on Mobile Devices or Removable Media; and
- Shall not be accessed using CIHI's VPN from outside of Canada.

1.2 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 as set out in the *Secure Information Transfer Standard*;
- Shall not be stored on Mobile Devices or Removable Media; and
- Shall not be accessed using CIHI's VPN from outside of Canada.

1.3 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 as set out in the *Secure Information Transfer Standard*;
- Shall not be stored on Mobile Devices or Removable Media; and
- Shall not be accessed using CIHI's VPN from outside of Canada.

1.4 Technical Information

- Shall not be removed from CIHI's premises in paper form;
- Shall not be sent by email externally, unless authorized and with appropriate safeguards as set out in the *Third-Party Technical Information Disclosure Standard*;
- 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.

2.0 **Conditions or restrictions on the retention of Personal Health Information on a Mobile Device**

- Not applicable; CIHI prohibits the retention of Personal Health Information, Health Workforce Personal Information and De-Identified Data on Mobile Devices.

3.0 **Remote access**

CIHI Staff are permitted to work remotely using CIHI's VPN on CIHI-provided encrypted laptop computers. CIHI Staff are prohibited from remotely accessing Personal Health Information if other information, such as de-identified and/or aggregate information, will serve the purpose, and from remotely accessing more Personal Health Information than is reasonably necessary for the identified purpose.

Only authorized CIHI-owned devices are allowed to connect to CIHI's networks over VPN. CIHI Staff are responsible for adhering to conditions and restrictions as set out in CIHI's *Acceptable Use Policy* including but not limited to the following:

- The user must safeguard the device's physical security;
- The device may be used for CIHI-related work only and may not be used by anyone other than the authorized user; and
- Storage of data on CIHI-issued laptops and workstations is prohibited.

All laptops and workstations capable of accessing CIHI's networks over VPN must employ whole-disk encryption in addition to all information security controls employed for on-site devices.

The approval process for accessing Personal Health Information, whether over VPN or through on-site devices, is found in Section 10 of CIHI's internal *Privacy Policy Procedures*.

Compliance, audit and enforcement

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 Staff to comply with the code and all of CIHI's policies, protocols and procedures. Compliance with security policies, protocols and procedures is monitored through CIHI's Privacy and Information Security Audit Program. Violations of the code are referred to Human Resources as appropriate and may result in disciplinary action up to and including dismissal.

Notification of breach

Instances of non-compliance with privacy and security policies are managed through CIHI's *Privacy and Security Incident Management Protocol*, which requires Staff to immediately report incidents and breaches by emailing incident@cihi.ca.

For more information:

security@cihi.ca

privacy@cihi.ca

How to cite this document:
Canadian Institute for Health Information. *Policy on the Security of Confidential Information and Use of Mobile Devices/Removable Media*. Ottawa, ON: CIHI; 2023.