Standard: Health Data Collection

1994 • 2019

Canadian Institute for Health Information

Institut canadien d'information sur la santé

Canadian Institute for Health Information
495 Richmond Road, Suite 600
Ottawa, Ontario K2A 4H6
Phone: 613-241-7860
Fax: 613-241-8120
cihi.ca
copyright@cihi.ca

How to cite this document:
Canadian Institute for Health Information. *Standard: Health Data Collection*. Ottawa, ON: CIHI; 2019.

Cette publication est aussi disponible en français sous le titre *Norme relative à la collecte de données sur la santé*.

Table of contents

Purpose

Collecting health data from data providers is an integral part of the information life cycle. When collecting health data, the Canadian Institute for Health Information (CIHI) must ensure the confidentiality and integrity of the data while it is in transit and upon receipt.

Scope

This standard applies to the collection of health data by CIHI. For the purpose of this document, health data includes personal health information, health workforce personal information and de-identified data. This standard does not apply to aggregate data — as defined in the Privacy Policy, 2010 or Health Workforce Privacy Policy, 2011 — or to information that is already publicly available that CIHI may acquire from external sources.

Definitions

Note: Unless otherwise stated, the source of the definition is CIHI's Privacy Policy, 2010 and/or Health Workforce Privacy Policy, 2011.

Aggregate data: Data that has been compiled from record-level data to a level of aggregation that ensures that the identity of individuals cannot be determined by reasonably foreseeable methods. Aggregate data with units of observation less than 5 may constitute either de-identified data or personal health information/health workforce personal information.

Confidential information: 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, health workforce personal information and de-identified data.

De-identified data: 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: 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.

Personal health information (PHI): Health information that identifies an individual or could identify an individual by a reasonably foreseeable method, as defined in CIHI's Privacy Policy, 2010 and as may be amended by CIHI from time to time.

Staff: Any worker at CIHI, including all full-time or part-time employees, secondments, temporary workers, students and contract employees, including external consultants or other third-party service providers.

Standard

Security considerations and data provider engagement

CIHI does not collect PHI in paper format. Staff should always encourage data providers to use 1 (or more) of the data submission methods outlined in this standard. When arranging for collection of confidential information from a data provider, it is important to notify the data provider of CIHI's preferred methods of acquisition.

Before receiving health data from a data provider using any other method, staff must consult Information Security at CIHI (security@cihi.ca).

Preferred data acquisition methods

CIHI has identified 3 preferred methods of receiving health data from its data providers. These methods, in order of preference, are as follows:

Web-based applications or CIHI's server-to-server application

The preferred and most secure means of data acquisition is through CIHI's approved methods of electronic submission. These applications use industry standard, encrypted, secure methods to transfer the data.

Wherever possible, data providers should submit health data to CIHI using our existing electronic methods. Please email Central Client Services (CCS) at ccs_data_trans@cihi.ca to determine whether an existing electronic method can be used for your request. CCS will consult with the Information Security team to select the most secure data acquisition method if an electronic method cannot be used.

Courier

Confidential information contained on an electronic medium should be encrypted and password-protected using approved methods. For more information about approved methods, please email security@cihi.ca. If the data provider includes a record layout or data dictionary, these documents must be sent to CIHI, either as part of the encrypted files or separately from the data via any medium (e.g., email). Passwords to decrypt the information should be provided separately using an alternative medium (e.g., phone).

When sending any confidential information by courier, data providers should prepare a double-wrapped (e.g., 2 envelope or equivalent double wrapping) courier package as follows:

Inner envelope:

- Destination address: CIHI's address
- Return address: Data provider's address
- Label: Suggested text: "Contains confidential data. To be opened by the addressee only."

Outer envelope:

- Destination address: CIHI's address
- Return address: Data provider's address

When sending encrypted electronic media via courier, data providers should include a cover letter to accompany the data indicating that the contents are encrypted and password-protected and providing contact information, including a name and phone number, which the recipient can use to confirm receipt of the information and obtain the necessary password(s). Suggested text: "These files are encrypted and password-protected. Upon receipt, please contact <data provider name> at <data provider telephone number> to obtain the password."

A service that allows for electronic tracing and confirmation of receipt should be used for all courier submissions of health data.

Email

CIHI will accept data via email when no other safe alternative is available. Electronic confidential information should be encrypted and password-protected using approved methods before it is sent. For more information about approved methods, please email security@cihi.ca.

If the data provider includes a record layout or data dictionary, these documents must be sent to CIHI, either as part of the encrypted files or separately from the data via any medium (e.g., email). Passwords to decrypt the information should be provided separately using an alternative medium (e.g., phone). In the email text accompanying the data, data providers should include the following information:

- Indication that the files are encrypted and password-protected.
- Information about what to do upon receipt, including the name and phone number of the person to contact to obtain the necessary password(s). Suggested text: "Please contact <data provider name> at <data provider telephone number> to obtain the password."
- Information about what to do if the email is misdirected. Suggested text: "IMPORTANT NOTICE: This email may contain confidential information. If you have received it in error, please delete. Thank you."

Compliance

The *CIHI Code of Business Conduct* describes the ethical and professional behaviour related to work relationships, information — including PHI — 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 the *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 and procedures/ supporting documents

Privacy Policy, 2010

Health Workforce Privacy Policy, 2011

For more information

For more information, please email security@cihi.ca.

help@cihi.ca

CIHI Ottawa
495 Richmond Road
Suite 600
Ottawa, Ont.
K2A 4H6
613-241-7860

CIHI Toronto
4110 Yonge Street
Suite 300
Toronto, Ont.
M2P 2B7
416-481-2002

CIHI Victoria
880 Douglas Street
Suite 600
Victoria, B.C.
V8W 2B7
250-220-4100

CIHI Montréal
1010 Sherbrooke Street West
Suite 602
Montréal, Que.
H3A 2R7
514-842-2226

cihi.ca

21166-1119