Standard: Health Data Collection

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; 2021.

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

Table of contents

Purpose 4

Scope. 4

Definitions 4

Standard 5

Security considerations and data provider engagement 5

Preferred data collection methods 6

Compliance, audit and enforcement. 6

Related policies and procedures/supporting documents 7

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, upon receipt and for as long as CIHI holds the data.

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 de-identified data, personal health information or 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 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.

Personal information: Information recorded about an identifiable individual in any form. Includes, but is not limited to, information related to the individual's race; national or ethnic origin; colour; religion; age; sex; sexual orientation; marital status; education; medical, criminal or employment history; photographs; address; fingerprints; and blood type; as well as any identifying number, symbol or other particular assigned to the individual.

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

Standard

Security considerations and data provider engagement

CIHI does not collect PHI in paper format. CIHI encourages 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 that the data provider be aware of CIHI's preferred methods of collection.

Wherever possible, data providers should submit health data to CIHI using our preferred methods. Questions about CIHI's preferred methods of collection should be sent to dataservices@cihi.ca.

Any other method of receiving health data requires the approval of Information Security at CIHI (security@cihi.ca).

Preferred data collection 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.

Courier

Confidential information contained on an electronic medium should be encrypted and password-protected. For more information, please email security@cihi.ca. Passwords to decrypt the information should be provided separately using an alternative medium (e.g., phone).

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 before it is sent. For more information, please email security@cihi.ca.

Passwords to decrypt the information should be provided separately using an alternative medium (e.g., phone).

Compliance, audit and enforcement

The *CIHI 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 employees to comply with it and all of CIHI's policies, protocols and procedures. Compliance with CIHI's Security Program is monitored through CIHI's Information Security Audit Program, and instances of non-compliance with 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 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

23929-0221