Production of this document is made possible by financial contributions from Health Canada and provincial and territorial governments. The views expressed herein do not necessarily represent the views of Health Canada or any provincial or territorial government.

Unless otherwise indicated, this product uses data provided by Canada's provinces and territories.

Table of contents

Quick facts about the Primary Health Care Database

1. Primary health care is often a patient's first point of contact with the health care system

1 Introduction

The Canadian Institute for Health Information (CIHI) collects and analyzes information on health and health care in Canada. Its mandate is to deliver comparable and actionable information to accelerate improvements in health care, health system performance and population health across the continuum of care. CIHI obtains data from hospitals and other health care facilities, long-term care homes, regional health authorities, medical practitioners and governments. This data includes information about health services provided to individuals, the health professionals who provide those services and the cost of the health services.

The purpose of this privacy impact assessment (PIA) is to examine the privacy, confidentiality and security risks associated with the Primary Health Care Database. This PIA, which is CIHI's first primary health care PIA, includes both a review of the 10 privacy principles set out in the Canadian Standards Association's *Model Code for the Protection of Personal Information* and how the principles apply to the Primary Health Care Database, as well as a look at the application of CIHI's *Privacy and Security Risk Management Framework*.

The primary driver for this PIA is compliance with CIHI's *Privacy Impact Assessment Policy*.

2 Background

2.1 Introduction to the Primary Health Care Database

Primary health care

Primary health care is often a patient's first point of contact with the health care system and the central point of coordination between health care providers. It puts the patient at the centre of care, focusing on the comprehensive and interrelated aspects of physical, mental and social health, and well-being. Primary health care incorporates primary care services as well as the broader spectrum of services that can play a part in health, such as education, income, housing, environment and other social determinants of health.

Primary Health Care Database

For the purposes of the Primary Health Care Database, CIHI collects data on primary health care services provided to patients and on patients' socio-demographic attributes. CIHI uses the database to produce information that can be used to manage primary health care services, monitor population health, examine screening and immunization rates and identify gaps in access to primary health care.

Beginning in 2018, CIHI and the Alliance for Healthier Communities — an Ontario network of primary health care organizations and community health centres — began a collaboration to demonstrate the value of collecting primary health care data from electronic medical records. As of 2022, CIHI had collected data from the Alliance network that represents nearly 17 million visits by more than 1 million patients to 73 community health centres in Ontario. CIHI is pursuing similar primary health care data in provinces and territories beyond Ontario where legislative authority exists for the disclosure of primary health care data to CIHI.

2.2 Data collection

For the purposes of the Primary Health Care Database, CIHI collects patients' health card numbers, demographic information, information about their health and administrative data such as primary health care organization identifers and health service provider identifers. CIHI uses

3.2 Authorities governing Primary Health Care Database data

General

CIHI adheres to its *Privacy Policy, 2010* and to any applicable privacy legislation and/or legal agreements.

Privacy legislation

CIHI is a secondary data collector of health information, specifically for the planning and management of the health system, including statistical analysis and reporting. Data providers are responsible for meeting the statutory requirements in their respective jurisdictions, where applicable, at the time the data is collected.

People and organizations that provide private-practice primary health care services are currently authorized to disclose PHI to CIHI without consent under provincial health information privacy legislation in Newfoundland and Labrador, Nova Scotia, New Brunswick and Ontario. For example, health information custodians in Ontario — including those in private practice — have authority to disclose PHI to CIHI without consent given CIHI's status as a prescribed entity under Ontario's *Personal Health Information Protection Act, 2004* (PHIPA).

Agreements

At CIHI, the Primary Health Care Database data is governed by CIHI's *Privacy Policy, 2010*, by legislation in the jurisdictions and by data-sharing agreements with data providers. The data-sharing agreements set out the purpose, use, disclosure, retention and disposal requirements of PHI provided to CIHI, as well as any subsequent disclosures that may be permitted. The agreements also describe the legislative authority under which PHI is disclosed to CIHI.

3.3 Principle 1: Accountability for PHI

CIHI's president and chief executive officer is accountable for ensuring compliance with CIHI's *Privacy Policy, 2010*. CIHI has a chief privacy officer and general counsel, a corporate Privacy, Confidentiality and Security Committee, and a Governance and Privacy Committee of its Board of Directors.

Organization and governance

The following table identifies key internal senior positions with responsibilities for the Primary Health Care Database data in terms of privacy and security risk management:

Table Key positions and responsibilities

3.4 Principle 2: Identifying purposes for PHI

CIHI's mandate is to deliver comparable and actionable information to accelerate improvements in health care, health care system performance and population health across the continuum of

An example is the number assigned to each service provider (e.g., health professional) who contributed to the person's care. CIHI uses this information to determine the types of human resources involved in the individual's care.

Free (open) text fields are general fields that can accept any type of data in the form of text or numbers, such as clinical notes and fill-in-the-blank "Other: _____" fields. Semi-structured text fields are fields that contain a menu of options that can be modified by individual users. For example, for spoken language, a semi-structured field might contain "English," "French" and "Unknown" as pre-defined values, with the option for users to add values, such as "Spanish," "Mandarin" and "Arabic."

The Primary Health Care Database currently collects data in semi-structured text fields, including reason for visit, issue addressed and medication prescribed. These semi-structured fields allow users to add options or modify pre-defined values when the existing list does not meet their needs. CIHI would not expect a user to enter a patient's name, for example, into semi-structured text fields; however, there is a risk that this could occur. T ' E

3.7 Principle 5: Limiting the use, disclosure and retention of PHI

Limiting use

Clients

CIHI limits the use of the Primary Health Care Database data to authorized purposes, as described in Section 3.4. These include comparative analyses within and among jurisdictions; trend analyses to assess and monitor the impact of differences in policy, practices and service delivery; and the production of statistics to support planning, management and quality improvement.

CIHI staff are permitted to access and use data on a need-to-know basis only, including for data processing and quality management, producing statistics and data files, and conducting analyses. All CIHI staff are required to sign a confidentiality agreement at the commencement of employment, and they are subsequently required to renew their commitment to privacy yearly.

Staff access to CIHI's secure analytical environment is provided through CIHI's centralized data access process. This environment is a separate, secure space for analytical data files, including general use data (GUD) files, where staff are required to conduct and store the outputs from their analytical work.

The GUD files are pre-processed files that are designed specifically to support internal analytical users' needs, including the removal of the original health care number (replaced with an encrypted health care number), and full date of birth and full postal code, which are replaced by a set of standard derived variables. The production of primary health care GUD files is completed annually, to incorporate new data.

The process ensures that all requests for access, including access to Primary Health Care Database data, are traceable and authorized, in compliance with Section 10 of CIHI's *Privacy Policy, 2010*. Access to CIHI's secure analytical environment is subject to an annual audit to ensure that staff are accessing data on a need-to-know basis. Section 3.9 includes additional information about how the various procedural and technical measures are deployed to prevent unauthorized access and otherwise secure the Primary Health Care Database.

Data linkage

Data linkages are performed between the Primary Health Care Database and other CIHI data sources. While this potentially causes greater risk of identification of an individual, CIHI undertakes mitigating steps to reduce the risks.

Sections 14 to 31 of CIHI's *Privacy Policy, 2010* govern the linkage of records of PHI. Pursuant to this policy, CIHI permits the linkage of PHI under certain circumstances. Data linkage within a single data holding for CIHI's own purposes is generally permitted. Data linkage across data holdings for CIHI's own purposes and all third-party requests for data linkage are subject to an internal review and approval process. When carrying out data linkages, CIHI will generally do so using consistently encrypted health care numbers. The linked data remains subject to the use and disclosure provisions in the *Privacy Policy, 2010*.

Criteria for approval of data linkages are set out in sections 23 and 24 of CIHI's *Privacy Policy, 2010*, as follows:

Section 23 The individuals whose personal health information is used for data linkage have consented to the data linkage; or

Section 24 All of the following criteria are met:

a) The purpose of the data linkage is consistent with CIHI's mandate;

b) The public benefits of the linkage significantly offset any risks to the privacy of individuals;

c) The results of the data linkage will not be used for any purpose that would be detrimental to the individuals that the personal health information concerns;

d) The data linkage is for a time-limited specific project and the linked data will be subsequently destroyed in a manner consistent with sections 28 and 29; or

e) The data linkage is for purposes of an approved CIHI ongoing program of work where the linked data will be retained for as long as necessary to meet the identified purposes and, when no longer required, will be destroyed in a manner consistent with sections 28 and 29; and

f) The data linkage has demonstrable savings over other alternatives or is the only practical alternative.

Client linkage standard

CIHI has implemented a corporate-wide client linkage standard to be used for the linkage of records created in 2010–2011 or later, where the records include the following data elements: encrypted health care number, and the province/territory that issued the health care number. For the linkage of records that do not satisfy these criteria, the linkage mechanism is determined on a case-by-case basis.

Destruction of linked data

Section 29 of CIHI's *Privacy Policy, 2010* further requires that for time-limited specific projects, the secure destruction of linked data will occur within 1 year after publication of the resulting analysis, or 3 years after the linkage, whichever is sooner, in a manner consistent with CIHI's

Where CIHI has provided researchers and other approved users with access to record-level data by extracting the relevant data into files and sending the files to the users, CIHI has adopted a complete life cycle approach. As part of that life cycle, Privacy and Legal Services (PLS) has developed and is responsible for the ongoing compliance monitoring process whereby all data sets that are disclosed to third-party data recipients are tracked and monitored for secure destruction at the end of their life cycle. Prior to disclosing data, third-party recipients sign a data protection agreement and agree to comply with the conditions and restrictions imposed by CIHI relating to the collection, purpose, use, security, disclosure and return or disposal of data.

Data requesters are required to complete and submit a data request form. They must also sign an agreement wherein they agree to use the data for only the purpose specified. All data protection agreements with third parties specify that receiving organizations must keep record-level data strictly confidential and not disclose such data to anyone outside the organization. Moreover, CIHI imposes obligations on these third-party recipients, including

- Secure destruction requirements;
- CIHI's right to audit;
- Restriction on the publication of cell sizes less than 5; and
- Strong encryption technology that meets or exceeds CIHI's standards where mobile computing devices are used.

In addition to the ongoing compliance monitoring process, whereby all data sets that are disclosed to third-party data recipients are tracked and monitored for secure destruction at the end of their life cycle, PLS contacts third-party data recipients on an annual basis to certify that they continue to comply with their obligations as set out in the data request form and data protection agreement signed with CIHI.

As noted in Section 3.4 of this PIA, CIHI collects Indigenous identifiers for purposes of the Primary Health Care Database. The disclosure of this identifier is governed by CIHI's *Policy on the Release and Disclosure of Indigenous-Identifiable Data*, which requires that any request for Indigenous-identifiable data at CIHI be accompanied by approvals from appropriate Indigenous authorities. For more information, see *A Path Forward: Toward Respectful Governance of First Nations, Inuit and Métis Data Housed at CIHI*.


help@cihi.ca

CIHI Ottawa