Primary Health Care Database

Privacy Impact Assessment

March 2023

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

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.

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. *Primary Health Care Database Privacy Impact Assessment, March 2023*. Ottawa, ON: CIHI; 2023.

Cette publication est aussi disponible en français sous le titre *Base de données sur les soins de santé primaires : évaluation des incidences sur la vie privée, mars 2023*.

The Canadian Institute for Health Information (CIHI) is pleased to publish the following privacy impact assessment in accordance with its *Privacy Impact Assessment Policy*:

- *Primary Health Care Database Privacy Impact Assessment, March 2023*

Approved by

Brent Diverty
Vice President, Data Strategies and Statistics

Rhonda Wing
Executive Director, Chief Privacy Officer and General Counsel

Ottawa, March 2023

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 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.
2. 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.
3. For the purposes of the Primary Health Care Database, the Canadian Institute for Health Information (CIHI) collects data on primary health care services provided to patients and on patients' socio-demographic attributes.
4. 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.
5. 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.
6. As of 2022, CIHI had collected data from the Alliance network representing nearly 17 million visits by more than 1 million patients to 73 community health centres in Ontario.
7. For the purpose of fulfilling its mandate, 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.
8. 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 identifiers and health service provider identifiers.
9. CIHI uses this data in a de-identified format to create information that supports the activities of the Primary Health Care Program.

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 identifiers and health service provider identifiers. CIHI uses this data to support the activities described above relating to the Primary Health Care Program.

Information about the data CIHI collects for Primary Health Care Database purposes can be found on CIHI's website.

2.3 Access management and data flow for the Primary Health Care Database

Access to CIHI's secure applications is managed by CIHI's Product Management and Client Experience (PMCE) department. PMCE manages access to CIHI's secure applications using established access management system (AMS) processes for granting and revoking access.

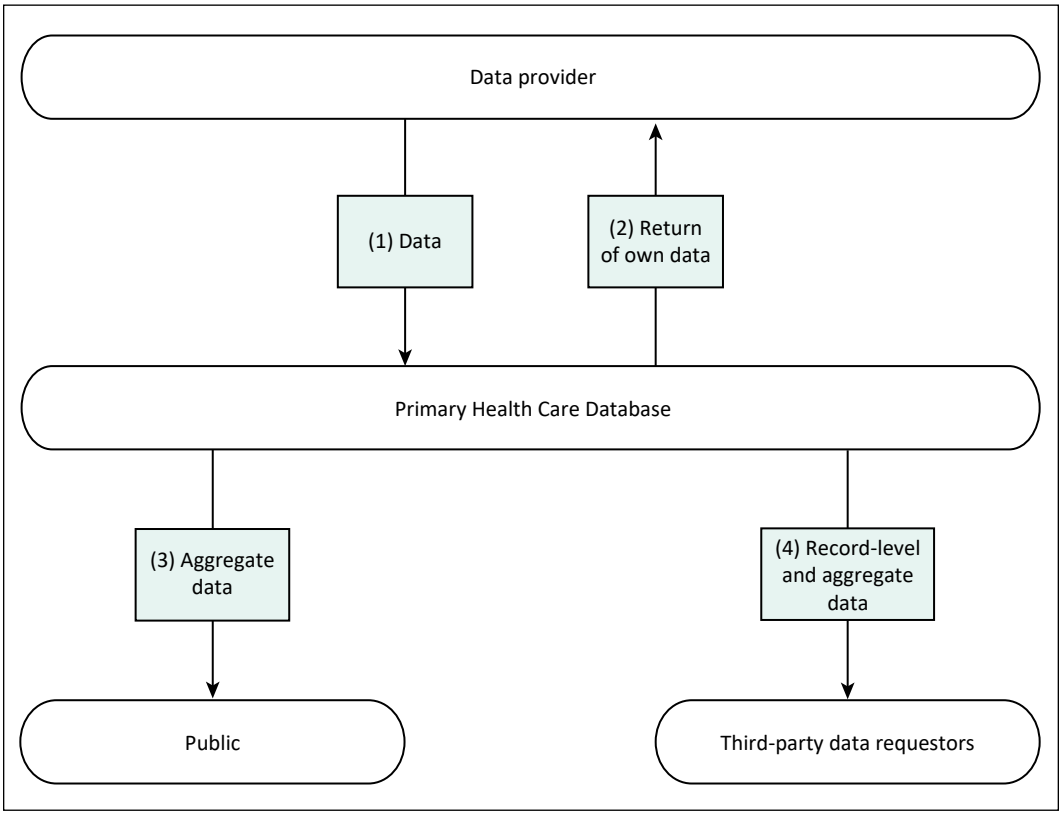
Once authenticated through CIHI's AMS, primary health care data providers submit record-level data that is electronically captured using specialized software, through CIHI's secure web-based electronic Data Submission Services (eDSS) or server-to-server (SFTP) application.

Primary Health Care Database data flows are as follows:

1. Data providers such as organizations that provide primary health care services (e.g., primary health care clinics, community health centres) submit data to the Primary Health Care Database.
2. Upon request, a copy of the records (after they have been processed by the Primary Health Care Database) is made available to the data provider.
3. CIHI releases aggregate data to the public.
4. CIHI provides personal health information (PHI), de-identified record-level and aggregate data to third-party data requestors in accordance with CIHI's Privacy Policy and CIHI's agreements with its data providers.

The following figure illustrates the Primary Health Care Database data flows.

Figure Primary Health Care Database data flows



3 Privacy analysis

3.1 Privacy and security risk management

Privacy and security risk management is 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. CIHI has implemented a *Privacy and Security Risk Management Framework* and the associated *Policy on Privacy and Security Risk Management*. CIHI's chief privacy officer and general counsel, and chief information security officer, in collaboration with senior managers, are responsible for identifying, assessing, treating, monitoring and reviewing privacy and security risks.

Privacy and security risks may be identified from a variety of sources, including PIAs. Once identified, risks are entered into the Privacy and Security Risk Register and categorized as **high**, **medium** or **low**, based on the likelihood and impact of a risk event:

- **High:** High probability of risk occurring, and/or controls and strategies are not reliable or effective;
- **Medium:** Medium probability of risk occurring, and/or controls and strategies are somewhat reliable or effective; or
- **Low:** Low probability of risk occurring, and/or reliable, effective controls and strategies exist.

The likelihood and impact of the identified risk are used to create a risk score. The risk assessment score of low, medium or high defines the seriousness of a risk. A higher risk ranking indicates a more serious threat and a greater imperative for treatment. Once an initial risk treatment is applied, the residual risk (the new calculation of the likelihood and impact of the risk, given the treatment) is assessed and compared against CIHI's privacy and security risk tolerance statement, which indicates that CIHI's privacy and security risk tolerance is low. If the risk score for the residual risk is still greater than low, additional risk treatment is necessary until the risk is low or the untreated/residual risk is accepted by CIHI's Executive Committee, on behalf of the corporation.

As indicated in Section 3.4, CIHI is currently undertaking a privacy and security risk management process regarding free text and semi-structured text fields.

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

Position/group	Roles/responsibilities
Vice president, Data Strategies and Statistics	Responsible for the overall strategic direction of the Primary Health Care Database.
Director, Spending and Primary Care	Responsible for the overall operations and strategic business decisions of the Primary Health Care Database.
Chief information security officer	Responsible for the strategic direction and overall implementation of CIHI's Information Security Program.
Chief privacy officer and general counsel	Responsible for the strategic direction and overall implementation of CIHI's Privacy Program.

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 care. In order to fulfill these goals, CIHI collects the following types of primary health care data for the purposes indicated.

Patient personal identifier

This refers to an individual's health care number. CIHI uses this information to develop a complete picture of the continuum of care by linking together records describing the different types of care provided to the individual, at different times, by different health care providers and facilities.

Patient demographic information

Examples include birthdate, postal code, sex, gender, language, education, and racial, ethnic and Indigenous identifiers. CIHI uses age calculated from the date of birth, geographic information derived from postal code, as well as sex, gender, language and racial, ethnic and Indigenous identifiers for demographic analysis of health care services and outcomes.

Patient health characteristics

Examples of patient health characteristics collected include diagnoses and treatments, related comorbidities, clinical measurements and immunizations. CIHI uses this information to analyze disease prevalence and interventions provided to a defined population, evaluate the types of conditions requiring treatment or rehabilitation, assess the quality of care provided to the individual and calculate the costs associated with treatment.

Administrative information

Examples include dates when the patient visited a primary health care centre to seek care, the date a patient began a treatment and the date a patient was referred for care. CIHI uses this information to evaluate wait times for care, care coordination, continuity of care and resources consumed in providing care.

Organization identifiers

This refers to the names/codes of the organization that provided care to an individual, or where an individual was referred for care. CIHI uses this information to support analysis regarding the care provided by different providers or types of providers.

Health service provider identifiers

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 and semi-structured text fields

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. To mitigate this risk, CIHI conducts manual and automated checks in semi-structured fields to identify and remove PHI.

The privacy risks associated with free text and semi-structured text fields are currently being evaluated using CIHI's Privacy and Security Risk Management Program, as discussed in Section 3.1.

3.5 Principle 3: Consent for the collection, use or disclosure of PHI

CIHI is a secondary collector of data and does not have direct contact with patients. CIHI relies on data providers to abide by and meet their data collection, use and disclosure rules and responsibilities, including those related to consent and notification, as outlined in jurisdiction-applicable laws, regulations and policies.

3.6 Principle 4: Limiting the collection of PHI

CIHI is committed to the principle of data minimization. Under sections 1 and 2 of CIHI's *Privacy Policy, 2010*, CIHI collects from data providers only the information that is reasonably required for health system uses, including statistical analysis and reporting, in support of the management, evaluation or monitoring of the health care system.

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

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 28 of CIHI's *Privacy Policy, 2010* sets out the requirement that CIHI will destroy PHI and de-identified data in a secure manner, using destruction methodologies appropriate to the format, media or device such that reconstruction is not reasonably foreseeable.

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 *Secure Destruction Standard*. For linked data resulting from an ongoing program of work, secure destruction will occur when the linked data is no longer required to meet the identified purposes, in a manner consistent with CIHI's *Secure Destruction Standard*. These requirements apply to data linkages both for CIHI's own purposes and for third-party data requests.

Return of own data

CIHI returns records from the Primary Health Care Database to the data provider, upon request.

Third-party data requests

Customized record-level and/or aggregated data from the Primary Health Care Database may be requested by a variety of third parties.

CIHI administers the Third-Party Data Request Program, which establishes privacy and security controls that must be met by the recipient organization. Furthermore, as set out in sections 37 to 57 of CIHI's *Privacy Policy, 2010*, CIHI discloses health information in a manner consistent with its mandate and core functions, and CIHI data disclosures are made at the highest degree of anonymity possible while still meeting the research and/or analytical purposes of the requester. This means that, whenever possible, data is aggregated. When aggregated data is not sufficiently detailed for the intended purpose, record-level de-identified data or PHI (in limited circumstances, e.g., with individual consent) may be disclosed to the recipient on a case-by-case basis, when the recipient has entered into a data protection agreement or other legally binding instrument with CIHI. Only those data elements necessary to meet the intended purpose may be disclosed.

As the preferred means of record-level data access available to third-party data requestors, CIHI uses a secure access environment (SAE) (which is separate from CIHI's secure analytical environment that CIHI staff access, as indicated above). CIHI's SAE is an encrypted, secure environment hosted in CIHI's data centre. Consistent with CIHI's existing policies and procedures, approved researchers, who are subject to stringent agreement terms, access data extracts that have been prepared and vetted by CIHI staff for an approved research project. Record-level data cannot be copied or removed from the SAE; only aggregate results can be extracted from the SAE. Further information about CIHI's SAE is available on CIHI's website (Make a data request; *Secure Access Environment Privacy Impact Assessment*).

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*.

Public release

As part of its mandate, CIHI publicly releases aggregated data only in a manner designed to minimize any risk of re-identification and residual disclosure. This generally requires a minimum of 5 observations per cell in accordance with Section 33 of CIHI's *Privacy Policy, 2010*. CIHI expects aggregated statistics and analyses regarding primary health care to be made available in publications and on CIHI's website through tools such as Your Health System: In Depth and Quick Stats.

Limiting retention

The Primary Health Care Database forms part of CIHI's data holdings and, consistent with its mandate and core functions, CIHI retains such information for as long as necessary to meet the identified purposes.

3.8 Principle 6: Accuracy of PHI

CIHI has a comprehensive data quality program. Any known data quality issues will be addressed by the data provider or documented in data limitations documentation, which CIHI makes available to all users.

Similar to other CIHI data holdings, the Primary Health Care Database is subject to data quality assessment on a regular basis, based on *CIHI's Information Quality Framework*. The process of completing the framework includes numerous activities to assess the various dimensions of quality, including the accuracy of Primary Health Care Database data.

3.9 Principle 7: Safeguards for PHI

CIHI's Privacy and Security Framework

CIHI has developed a *Privacy and Security Framework* to provide a comprehensive approach to enterprise privacy and security management. Based on best practices from across the public, private and health sectors, the framework is designed to coordinate CIHI's privacy and security policies and to provide an integrated view of the organization's information management practices. Key aspects of CIHI's system security with respect to the Primary Health Care Database data are highlighted below.

System security

CIHI recognizes that information is secure only if it is secure throughout its entire life cycle: creation and collection, access, retention and storage, use, disclosure and destruction. Accordingly, CIHI has a comprehensive suite of policies that specify the necessary controls for the protection of information in both physical and electronic formats, up to and including robust encryption and secure destruction. This suite of policies and the associated standards, guidelines and operating procedures reflect best practices in privacy, information security and records management for the protection of the confidentiality, integrity and availability of CIHI's information assets.

System control and audit logs are an integral component of CIHI's Information Security Program. CIHI's system control and audit logs are immutable. Analysis at CIHI is generally conducted with the use of de-identified record-level data, where the health care number has been removed or encrypted upon first receipt. In exceptional instances, staff will require access to original health care numbers. CIHI's internal *Privacy Policy and Procedures, 2010* sets out strict controls to ensure that access is approved at the appropriate level and in the appropriate circumstances, and that the principle of data minimization is adhered to at all times. CIHI logs access to data as follows:

- Access to health care numbers and patient names (rarely collected) within CIHI's operational production databases;
- Access to data files containing PHI extracted from CIHI's operational production databases and made available to the internal analytical community on an exceptional basis; and
- Changes to permissions in access to operational production databases.

CIHI's employees are made aware of the importance of maintaining the confidentiality of PHI and other sensitive information through the mandatory Privacy and Security Training Program and through ongoing communications about CIHI's privacy and security policies and procedures. Employees attempting to access a CIHI information system must confirm, prior to each logon attempt, their understanding that they may not access or use the computer system without CIHI's express prior authority or in excess of that authority.

CIHI is committed to safeguarding its information technology ecosystem, securing its data holdings and protecting information with administrative, physical and technical security safeguards appropriate to the sensitivity of the information. Audits are an important component of CIHI's overall Information Security Program; they are intended to ensure that best practices are being followed and to assess compliance with all information security policies, procedures and practices implemented by CIHI. Audits are used to assess, among other things, the technical compliance of information-processing systems with best practices and published architectural and security standards; CIHI's ability to safeguard its information and information-processing systems against threats and vulnerabilities; and the overall security posture of CIHI's technical infrastructure, including networks, servers, firewalls, software and applications.

An important component of CIHI's Audit Program is regular third-party vulnerability assessments and penetration tests of its infrastructure and selected applications. All recommendations resulting from third-party audits are tracked in the Corporate Action Plan Master Log of Recommendations, and action is taken accordingly.

3.10 Principle 8: Openness about the management of PHI

CIHI makes information available about its privacy policies, data practices and programs relating to the management of PHI. Specifically, CIHI's *Privacy and Security Framework* and *Privacy Policy, 2010* are available to the public on cihi.ca.

3.11 Principle 9: Individual access to, and amendment of, PHI

PHI held by CIHI is not used by CIHI to make any administrative or personal decisions affecting individuals. Requests from individuals seeking access to their PHI will be processed in accordance with sections 60 to 63 of CIHI's *Privacy Policy, 2010*.

3.12 Principle 10: Complaints about CIHI's handling of PHI

As set out in sections 64 and 65 of CIHI's *Privacy Policy, 2010*, questions, concerns or complaints about CIHI's handling of information are investigated by the chief privacy officer and general counsel, who may direct an inquiry or complaint to the Information and Privacy Commissioner of the jurisdiction of the person making the inquiry or complaint.

4 Conclusion

CIHI's assessment of the Primary Health Care Database did not identify any privacy or security risks.

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

30761-0423