Health Workforce Databases

Privacy Impact Assessment

October 2024

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.

For permission or information, please contact CIHI:

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. *Health Workforce Databases Privacy Impact Assessment, October 2024*. Ottawa, ON: CIHI; 2024.

Cette publication est aussi disponible en français sous le titre *Bases de données sur la main-d'œuvre de la santé : évaluation des incidences sur la vie privée, octobre 2024*.

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

- *Health Workforce Databases Privacy Impact Assessment, October 2024*

Approved by

Brent Diverty
Vice President, Data Strategies and Statistics

Rhonda Wing
Executive Director, Chief Privacy Officer and General Counsel,
Office of the Chief Privacy Officer and Legal Services

Ottawa, October 2024

Table of contents

Quick facts about the health workforce databases

1. The mandate of the Canadian Institute for Health Information (CIHI) is to deliver comparable and actionable information to accelerate improvements in health care, health system performance and population health across the continuum of care.
2. As part of its mandate, CIHI collects information about health care providers. In the case of certain health care providers — specifically nurses, occupational therapists, pharmacists, physiotherapists and personal support workers — CIHI collects record-level data about their demographic, educational and employment characteristics. CIHI stores this data in its Health Workforce Database (HWDB). CIHI also collects aggregate data about a wide range of other health care providers and stores this data in its HWDB.
3. CIHI also collects data about physicians. Specifically, CIHI collects record-level data about physicians' demographic, payment and service utilization characteristics. CIHI collects this data from ministries of health, which compile the information in the context of paying physicians. CIHI stores this data in its National Physician Database (NPDB).
4. CIHI uses the data about health care providers stored in the HWDB and the data about physicians stored in the NPDB to develop information about Canada's health workforce. This information addresses health workforce demographic, educational, geographic, employment and service utilization characteristics.
5. A range of stakeholders use this information to support workforce planning and policy development and research, and to enable pan-Canadian comparability.

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 care providers who provide those services and the cost of the health services. As part of its mandate, CIHI collects information about selected health care providers in Canada and stores this in its Health Workforce Database (HWDB), and it collects information about physicians and stores this in its National Physician Database (NPDB).

The purpose of this privacy impact assessment (PIA) is to examine the privacy, confidentiality and security risks associated with CIHI's health workforce databases. This PIA replaces *Nursing Database, Health Human Resources Database and Health Workforce Database Privacy Impact Assessment, August 2019*. In addition, this PIA addresses information that CIHI collects about physicians, which was not discussed in the 2019 document. Accordingly, this PIA addresses all health workforce information that CIHI collects (subject to Section 2.1, subsection Out of scope).

This 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 CIHI's health workforce databases, 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*.

All policies referenced in this PIA are available on cihi.ca.

Note regarding terminology:

- "Health workforce databases" refers collectively to the HWDB and NPDB.
- "Health care providers" refers to all health care providers, including physicians.

2 Background

2.1 Data collection

Purpose of collection

CIHI's 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. As part of this mandate, CIHI collects both record-level and aggregate data about selected health care providers and/or the services they provide in Canada. CIHI stores this data in its HWDB or NPDB.

CIHI uses the data in these databases to develop information about Canada's health workforce, addressing its demographic, educational, geographic, employment and service utilization characteristics.

A range of stakeholders use this information to support workforce planning and policy development and research, and to enable pan-Canadian comparability.

Collecting record-level information

Health Workforce Database: Record-level information about selected health care providers

For certain health care providers — specifically nurses, occupational therapists, pharmacists, physiotherapists and personal support workers — CIHI currently collects record-level data about their demographic, educational and employment characteristics. CIHI collects this record-level data from the provincial/territorial regulatory colleges that govern the health care providers in question, or from a national health professional association. In some cases, a provincial/territorial government collects the information from the regulatory college and forwards the information to CIHI.

Each record that CIHI collects reflects the HWDB minimum data set and addresses the following matters:

- Professional registration (e.g., registration province/territory and date, provincial/territorial registration number, concurrent registration province/territory and date);
- Demographics (e.g., birth year, sex at birth, gender, list of languages in which the health care provider is able to provide services, Indigenous identity, racialized group);
- Geography (e.g., residence postal code, employer postal code);
- Education (e.g., graduation province/territory and year); and
- Employment (e.g., full-time/part-time/casual status, employment position, whether the position is publicly or privately funded).

See the HWDB metadata for additional information about the data that CIHI collects for this database.

The record-level data that CIHI collects which addresses the above matters is stored in CIHI's HWDB. In accordance with privacy principles, this record-level health workforce personal information is subject to CIHI's *Privacy Policy on the Collection, Use, Disclosure and Retention of Health Workforce Personal Information and De-Identified Data, 2011* (*Health Workforce Privacy Policy*) and is addressed by this PIA.

National Physician Database: Record-level information about physicians

CIHI also collects data about physicians. Specifically, CIHI collects record-level data about physicians' demographic, payment and service utilization characteristics. CIHI collects this information from ministries of health, which compile the information in the context of paying physicians. Because ministries of health collect the information in this context, it is structured differently from other record-level health workforce data that CIHI collects. Accordingly, it is stored in a separate database: the NPDB.

Each record that CIHI collects reflects the NPDB minimum data set and addresses the following matters:

- Professional registration (e.g., registration province/territory and date, unique physician identifier, registered specialty);
- Demographics (e.g., date of birth, sex at birth);
- Geography (e.g., work postal code); and
- Education (e.g., institution and year of medical school graduation, institution and year of specialty training).

See the NPDB metadata for additional information about the data that CIHI collects for this database.

The record-level data that CIHI collects which addresses the above matters is stored in CIHI's NPDB. In accordance with privacy principles, this record-level health workforce personal information is subject to CIHI's *Health Workforce Privacy Policy* and is addressed by this PIA.

Out of scope

The following health workforce data is not addressed by this PIA:

- As indicated above, CIHI collects aggregate information about many types of health care providers and stores this information in the HWDB. In accordance with privacy principles, aggregate information (which CIHI has confirmed does not identify individuals) is not subject to the rules in CIHI's *Health Workforce Privacy Policy* and is not addressed by this PIA.
- The Patient-Level Physician Billing (PLPB) Repository collects information about services provided by an identifiable physician to an identifiable patient (e.g., it collects patient health care numbers). The presence of personal health information means that information in the PLPB Repository is subject to CIHI's *Privacy Policy on the Collection, Use, Disclosure and Retention of Personal Health Information and De-Identified Data, 2010*. This PIA addresses information subject to CIHI's *Health Workforce Privacy Policy* only and therefore does not address data stored in the PLPB Repository; this data is addressed in a separate PIA available on cihi.ca.
- Scott's Medical Database (SMDB) contains information about the number of physicians in Canada and some of their demographic, educational and migration characteristics. CIHI purchases a copy of Scott's Directories from its publisher, Owen Media Partners (OMP). In accordance with privacy principles, because OMP's database is already publicly available (which includes information for sale), the SMDB is not subject to CIHI's *Health Workforce Privacy Policy* and is not addressed in this PIA.[i]
- In some cases, a data provider submits health workforce information to CIHI on a pilot basis. Pilot data is not subject to this PIA. Instead, CIHI prepares a data management plan that evaluates the application of privacy principles to that particular pilot. If the data provider proceeds to participate in ongoing data submission, this PIA applies to the data submitted going forward.

[i] In addition to information that CIHI purchases from the publisher, the SMDB also relies on publicly available information from provincial/territorial regulatory authorities (e.g., to confirm the physician's practice status or specialization) and publicly available aggregate information from ministries of health (e.g., to confirm total counts of physicians in a certain category). In both cases, in accordance with privacy principles, this additional information is not subject to CIHI's *Health Workforce Privacy Policy* and is not addressed in this PIA.

2.2 Access management and data flow for health workforce databases

Access by data providers to CIHI's secure applications is managed by CIHI's Client Access and Engagement (CAE) department. CAE manages access to CIHI's secure applications using established access management system (AMS) processes for granting and revoking access.

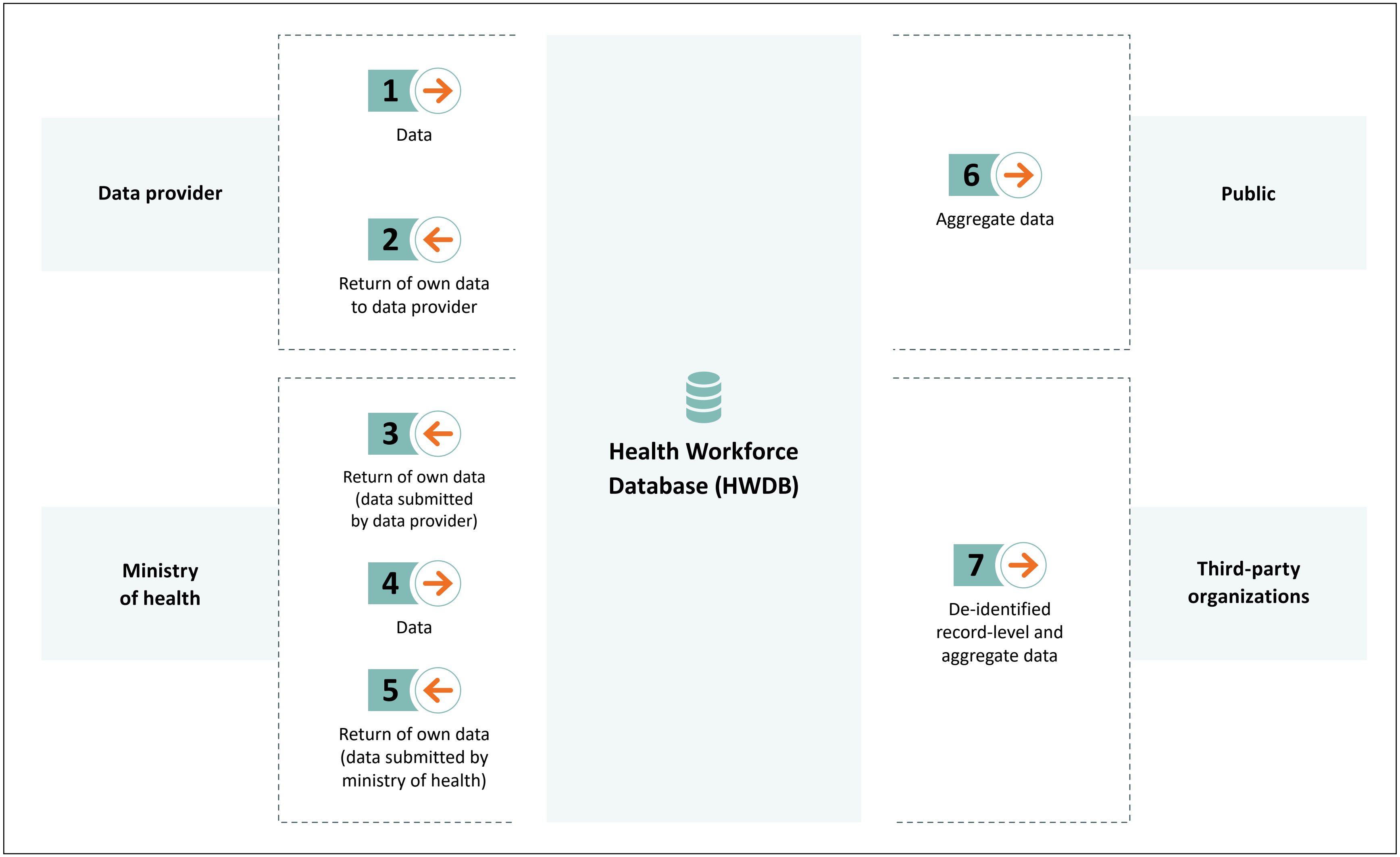
Once authenticated through CIHI's AMS, data providers for CIHI's health workforce databases submit record-level data from facilities that is electronically captured using specialized software, through CIHI's secure web-based electronic Data Submission Services (eDSS) or server-to-server (SFTP) application.

The HWDB data flow is as follows:

1. The data provider submits record-level data to the HWDB. Most data providers are provincial/territorial regulatory colleges, but some are national health professional associations.
2. Upon request, CIHI returns quality-corrected record-level data (e.g., missing data elements have been corrected) to the data provider.
3. Upon request, CIHI returns quality-corrected record-level data (submitted by a data provider) to the relevant ministry of health. This return of data is with the data provider's approval, in accordance with CIHI's data-sharing agreements with the data providers.
4. Ministries of health submit record-level data to the HWDB in some cases.
5. Upon request, CIHI returns quality-corrected record-level data (e.g., missing data elements have been corrected) to the ministry of health that submitted the data to CIHI.
6. CIHI releases aggregate data to the public.
7. CIHI discloses de-identified record-level and aggregate data to third-party organizations. These disclosures are in accordance with CIHI's data-sharing agreements with the data providers.

Figure 1 illustrates the HWDB data flow.

Figure 1 HWDB data flow

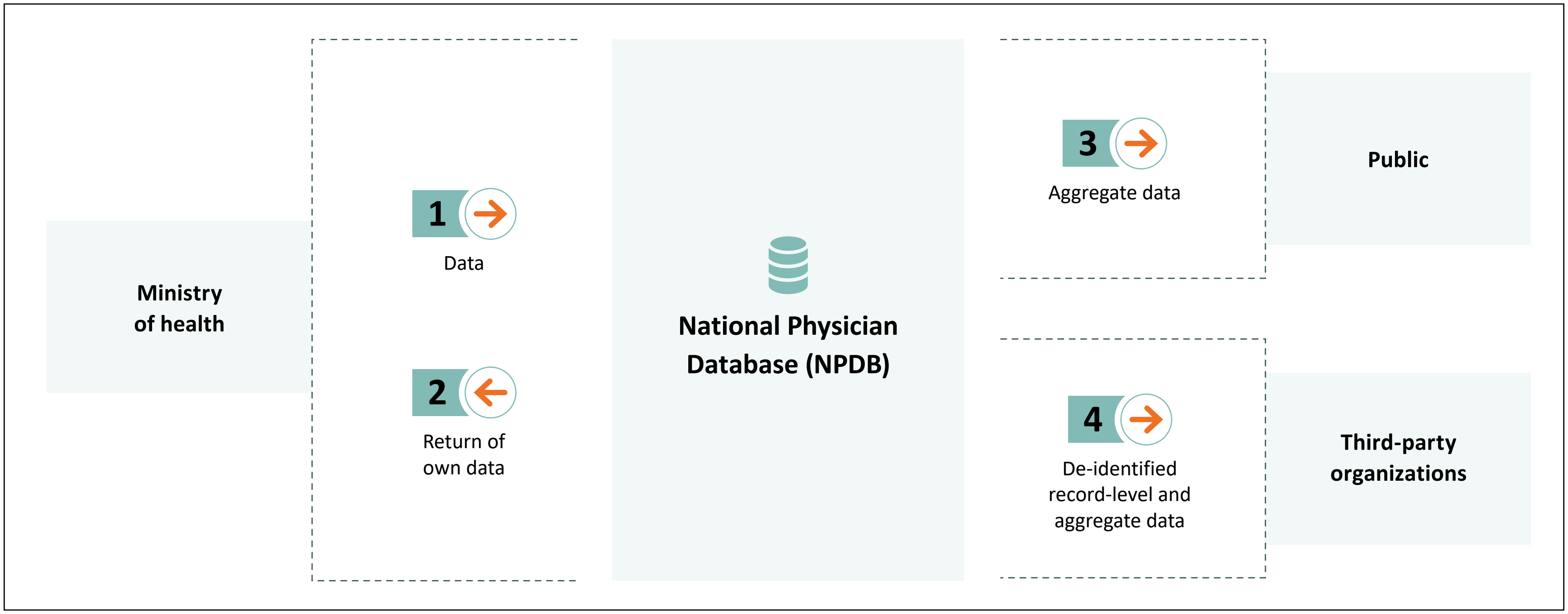

Data provider
1 Data
2 Return of own data to data provider
Ministry of health
3 Return of own data (data submitted by data provider)
4 Data
5 Return of own data (data submitted by ministry of health)
Health Workforce Database (HWDB)
6 Aggregate data
Public
7 De-identified record-level and aggregate data
Third-party organizations

The NPDB data flow is as follows:

1. Ministries of health submit record-level data to the NPDB.
2. Upon request, CIHI returns quality-corrected record-level data (e.g., missing data elements have been corrected) to the ministry of health.
3. CIHI releases aggregate data to the public.
4. CIHI discloses de-identified record-level and aggregate data to third-party organizations, in accordance with CIHI's data-sharing agreements with the ministries of health.

Figure 2 illustrates the NPDB data flow.

Figure 2 NPDB data flow


Ministry of health
1
Data
2
Return of own data
National Physician Database (NPDB)
3
Aggregate data
Public
4
De-identified record-level and aggregate data
Third-party organizations

3 Privacy analysis

Health care providers and health workforce personal information

Recent decisions by privacy commissioners and courts have concluded that information about a health care provider in “a business or professional context” is not personal information. For example, CIHI collects the health care provider’s work postal code, which is not personal information because it addresses the provider in a business or professional context.

However, commissioners and courts recognize that information addressing a health care provider’s “personal sphere” is personal information. For example, CIHI collects the postal code of the health care provider’s residence, and this is personal information because it addresses the provider’s personal sphere. Because some of the information that CIHI collects about health care providers is personal information, this PIA is required.

3.1 Privacy and Security Risk Management Program

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 its *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 that impact the privacy principles described in sections 3.3 to 3.12.

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 assessment score indicates a more serious threat and a greater imperative for treatment. Once an initial risk treatment has been 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 assessment 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.

CIHI's assessment of the health workforce databases did not identify any privacy or security risks.

3.2 Authorities governing health workforce data

CIHI is a secondary data collector of health information, specifically for the planning and management of Canada's health systems, 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.

Data stored in CIHI's health workforce databases is governed by CIHI's *Health Workforce Privacy Policy* and by data-sharing agreements with the data providers. The data-sharing agreements set out the purpose, use, retention and disposal requirements of personal information provided to CIHI, as well as any subsequent disclosures that are permitted.

3.3 Principle 1: Accountability for health workforce personal information

CIHI's president and chief executive officer is accountable for ensuring compliance with CIHI's *Health Workforce Privacy Policy*. 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 health workforce databases 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 health workforce databases.
Director, Health Workforce Information	Responsible for the overall operations of and strategic business decisions for the health workforce databases.
Manager, Health Workforce Information, Data Management and Operations	Responsible for implementing the operations of and strategic business decisions for the health workforce databases.
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 health workforce personal information

CIHI's 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. This includes developing information about health care providers and the services they provide in Canada. As discussed in Section 2.1, subsection Purpose of collection, CIHI collects record-level data about the health workforce as part of CIHI's mandate. CIHI uses the data to develop information about Canada's health workforce, which a range of stakeholders use for purposes such as

- Identifying changes in health workforce practice patterns over time;
- Measuring the impact of workforce policy changes; and
- Supporting health workforce planning.

In order to generate this information, CIHI collects record-level data about the following types of information for the purposes indicated.

Provider identifiers

Examples include provincial/territorial registration numbers (for the HWDB) and unique physician identifiers (for the NPDB). CIHI uses this information to uniquely identify a professional in its health workforce databases to enable longitudinal analyses of health professionals' supply, distribution and mobility trends, and also to identify a particular health care provider's record when communicating with the data provider (e.g., to correct the record).

Place of work

Examples include the type of facility (e.g., community mental health and addiction centre, general hospital) where the health care provider works. The HWDB (only) also collects the health facility identifier. CIHI uses this information to examine differences in the distribution of health care providers in health facilities and the impact on patient care.

Demographics

Examples include gender, Indigenous identifier, racialized group and a list of the languages in which the health care provider is able to provide services. CIHI uses this information to develop information about demographic trends among health care providers in Canada.

Geography

Examples include provider residence postal code and employment postal code. CIHI uses this information to understand the geographic distribution of the health workforce, including relocation, and the relationship between where a provider lives and works.

Education

Examples include graduation province/territory and year. CIHI uses this information to produce information about the supply of health care providers.

Employment

Examples include full-time/part-time/casual status and employment position. The HWDB (only) also collects place of work, area of practice, annual earned hours and whether the position is publicly or privately funded. CIHI uses this information in order to produce information about health care providers' activities and to understand the capacity of the available workforce.

3.5 Principle 3: Consent for the collection, use or disclosure of health workforce personal information

CIHI is a secondary collector of data and does not have direct contact with health care providers. 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 collection of health workforce personal information

CIHI is committed to the principle of data minimization. Under sections 1 and 2 of CIHI's *Health Workforce Privacy Policy*, 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 workforce in Canada.

CIHI consults with data providers nationally to identify the information which CIHI's health workforce databases need to collect to fulfill the intended purposes (discussed in Section 2.1). CIHI updates this information with data providers annually. Health care providers' names and contact information are not collected because they are not required for the purposes in question.

3.7 Principle 5: Limiting use, disclosure and retention of health workforce personal information

Limiting use

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, where staff are required to conduct and store the outputs from their analytical work.

The process ensures that all requests for access to CIHI's health workforce databases are traceable and authorized, in compliance with Section 10 of CIHI's *Health Workforce Privacy Policy*. 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 CIHI's health workforce databases.

Data linkage

CIHI can perform only very limited data linkage using health workforce data. Specifically, CIHI can perform linkages only within a single health workforce database (i.e., not across multiple databases). Within a single database, CIHI can link a health care provider's record for a given year to that provider's record for another year. The following rules apply to any linkages that CIHI performs using health workforce data.

Sections 14 to 31 of CIHI's *Health Workforce Privacy Policy* govern linkage of records of health workforce personal information. Pursuant to this policy, CIHI permits the linkage of health workforce personal information under certain circumstances. Data linkage within a single data holding for CIHI's own purposes is generally permitted. Data linkage for all third-party requests is subject to an internal review and approval process. The linked data remains subject to the use and disclosure provisions in the *Health Workforce Privacy Policy*.

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

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

Section 24 All of the following criteria are met:

1. The purpose of the data linkage is consistent with CIHI's mandate;
2. The public benefits of the linkage significantly offset any risks to the privacy of individuals;
3. The results of the data linkage will not be used for any purpose that would be detrimental to the individuals that the health workforce personal information concerns;
4. 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
5. 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
6. The data linkage has demonstrable savings over other alternatives or is the only practical alternative.

Destruction of linked data

Section 28 of CIHI's *Health Workforce Privacy Policy* sets out the requirement that CIHI will destroy health workforce personal information 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 *Health Workforce Privacy Policy* 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.

Data linkage rules not applicable to contextual linkage

As indicated in Section 3.4, the record-level data that CIHI collects about health care providers indicates the facility the health care provider works at. Accordingly, CIHI can link this information to the information CIHI collects about care provided at the facility where the health care provider works. However, the record-level data that CIHI collects about health care providers does **not** identify which patients the health care provider encountered. This is merely a contextual linkage. It does not qualify as a data linkage under CIHI's *Health Workforce Privacy Policy*, which is linkage of 2 records of information that are specific to a given health care provider. Since this activity is not considered data linkage, it is not subject to the data linkage procedures discussed above.

Return of own data

In accordance with Section 34 of CIHI's *Health Workforce Privacy Policy*, CIHI may return health workforce databases records to the submitting data provider. The return of own data is considered a use and not a disclosure.

Where the data provider is a regulatory authority or national health professional association (refer to Section 2.2), Section 34 of CIHI's *Health Workforce Privacy Policy* establishes that CIHI may also return records to the relevant ministry of health for data quality purposes and for purposes consistent with its mandate (e.g., for health services and population health management, including planning, evaluation and resource allocation). CIHI returns records to the ministry of health only upon request and with the data provider's approval in accordance with CIHI's data-sharing agreement with the data provider.

Limiting disclosure

Third-party data requests

Customized record-level and/or aggregated data from CIHI's health workforce databases may be requested by a variety of third parties.

CIHI administers its 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 *Health Workforce Privacy Policy*, CIHI discloses health workforce information in a manner consistent with its mandate and core functions, and 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 health workforce personal information (in limited circumstances, for example, with individual consent) may be disclosed to the recipient on a case-by-case basis. CIHI discloses information to third parties only as permitted by its data-sharing agreement with the data provider. Also, CIHI discloses record-level data to a third party only 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.

CIHI uses a secure access environment (SAE) as the preferred means of providing record-level data access to third-party data requestors (the SAE is separate from CIHI's secure analytical environment that CIHI staff access, as described in Section 3.7). 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.ca on the Make a data request web page and in the *SAE Privacy Impact Assessment*.

CIHI has adopted a complete life cycle approach to record-level data that it has extracted into files and sent to researchers and other approved users. As part of that life cycle, Privacy and Legal Services (PLS) has developed and is responsible for an 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 annually 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, CIHI's health workforce databases may collect Indigenous identifiers. CIHI does not currently release Indigenous-identifiable health workforce data. If this changes in the future, the disclosures would be 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, refer to *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 *Health Workforce Privacy Policy*.

CIHI's *Health Workforce Privacy Policy* establishes that CIHI may make publicly available aggregate health workforce data with units of observation of less than 5 when

- The information is already publicly available through other sources; and
- Making the information available will not reveal any additional personal information not already publicly available.

CIHI applies this principle to its health workforce publications. Many regulatory authorities already make information about individual health care providers publicly available, and CIHI's publications are unlikely to reveal additional information. Accordingly, in 2017, CIHI stopped suppressing units of observation less than 5 in aggregate health workforce reports. CIHI consulted with data providers when making this change. In accordance with data provider instructions, CIHI continues to suppress units of observation less than 5 in publications addressing licensed practical nurses in the Yukon and registered nurses in the Northwest Territories or Nunavut.

CIHI continues to suppress units of observation less than 5 in its NPDB publications.

Aggregated statistics and analyses are made available in publications on cihi.ca.

Limiting retention

The health workforce databases form 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 health workforce personal information

CIHI has a comprehensive Data and Information 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 health workforce databases are subject to an information 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 health workforce databases data. As part of the day-to-day information quality processes supporting CIHI's health workforce databases, when data providers submit records, CIHI checks the records against the relevant specifications to identify errors and inconsistencies.[ii] CIHI then provides data providers with error and validation reports, and with an opportunity to correct the records.

[ii] Specification manuals for the HWDB and NPDB are available on cihi.ca.

3.9 Principle 7: Safeguards for health workforce personal information

CIHI's Privacy and Security Framework

CIHI's *Privacy and Security Framework* provides a comprehensive approach to enterprise privacy and security management. Based on best practices from across the public and private 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 health workforce databases 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. The logs record access to record-level health workforce data that is provided to CIHI staff. CIHI's internal *Health Workforce Policy and Procedures* 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's employees are made aware of the importance of maintaining the confidentiality of health workforce personal information 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 attempt to log in, 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 health workforce personal information

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

3.11 Principle 9: Individual access to, and amendment of, health workforce personal information

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

3.12 Principle 10: Complaints about CIHI’s handling of health workforce personal information

As set out in sections 64 and 65 of CIHI’s *Health Workforce Privacy Policy*, questions, concerns or complaints about CIHI’s handling of health workforce personal information are investigated by the chief privacy officer and general counsel.

4 Review and update process

This PIA will be updated or renewed in compliance with CIHI’s *Privacy Impact Assessment Policy*.

✉ 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 511
Montréal, Que.
H3A 2R7
514-842-2226

cihi.ca

63631-1124