



# Nursing Database, Health Human Resources Database and Health Workforce Database

## Privacy Impact Assessment

August 2019



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.

All rights reserved.

The contents of this publication may be reproduced unaltered, in whole or in part and by any means, solely for non-commercial purposes, provided that the Canadian Institute for Health Information is properly and fully acknowledged as the copyright owner. Any reproduction or use of this publication or its contents for any commercial purpose requires the prior written authorization of the Canadian Institute for Health Information. Reproduction or use that suggests endorsement by, or affiliation with, the Canadian Institute for Health Information is prohibited.

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](http://cihi.ca)  
[copyright@cihi.ca](mailto:copyright@cihi.ca)

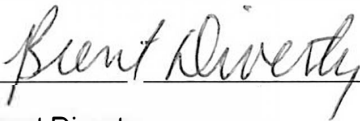
© 2019 Canadian Institute for Health Information

Cette publication est aussi disponible en français sous le titre *Base de données sur les infirmières et infirmiers, Base de données sur les ressources humaines de la santé et Base de données sur la main-d'œuvre de la santé : évaluation des incidences sur la vie privée, août 2019.*

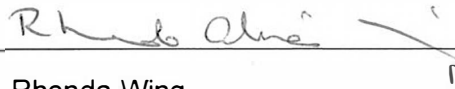
The Canadian Institute for Health Information (CIHI) is pleased to publish the following privacy impact assessment in accordance with its *Privacy Impact Assessment Policy*:

- Nursing Database
- Health Human Resources Database
- Health Workforce Database

Approved by:



Brent Diverty  
Vice President, Programs



Rhonda Wing  
Chief Privacy Officer & General Counsel

Ottawa – August 2019

# Table of contents

Quick facts about the Nursing Database, Health Human Resources Database and Health Workforce Database . . . . .	5
1 Introduction . . . . .	7
2 Background . . . . .	8
2.1 Introduction to the HWDB, NDB and HHRDB . . . . .	8
2.2 Data collection . . . . .	10
2.3 Access management, data submission and flow for the NDB and HHRDB . . . . .	13
3 Privacy analysis . . . . .	16
3.1 Privacy and Security Risk Management Program . . . . .	16
3.2 Authorities governing NDB and HHRDB data . . . . .	17
3.3 Principle 1: Accountability for health workforce personal information . . . . .	18
3.4 Principle 2: Identifying purposes for health workforce personal information . . . . .	18
3.5 Principle 3: Consent for the collection, use or disclosure of health workforce personal information . . . . .	19
3.6 Principle 4: Limiting collection of health workforce personal information . . . . .	19
3.7 Principle 5: Limiting use, disclosure and retention of health workforce personal information . . . . .	20
3.8 Principle 6: Accuracy of health workforce personal information . . . . .	23
3.9 Principle 7: Safeguards for health workforce personal information . . . . .	24
3.10 Principle 8: Openness about the management of health workforce personal information . . . . .	25
3.11 Principle 9: Individual access to, and amendment of, health workforce personal information . . . . .	25
3.12 Principle 10: Questions, concerns or complaints about CIHI's handling of health workforce personal information . . . . .	25
4 Conclusion . . . . .	26
Appendix: Text alternative for figure . . . . .	26

# Quick facts about the Nursing Database, Health Human Resources Database and Health Workforce Database

1. The Health Workforce Information team at the Canadian Institute for Health Information (CIHI) is responsible for 3 distinct data holdings that include record-level or aggregate-level data for the following regulated health care providers.

Record-level health workforce information:

## **Nursing Database (NDB)**

- Registered nurses (RNs), including nurse practitioners (NPs)
- Licensed practical nurses (LPNs)
- Registered psychiatric nurses (RPNs)

## **Health Human Resources Database (HHRDB)**

- Occupational therapists (OTs)
- Pharmacists
- Physiotherapists (PTs)
- Medical radiation technologists (MRTs) (2007 to 2015)
- Medical laboratory technologists (MLTs) (2007 to 2015)

Aggregate-level health workforce information:

## **Health Workforce Database (HWDB)**

- Audiologists
- Chiropractors
- Dental assistants
- Dental hygienists
- Dentists
- Dietitians
- Environmental public health professionals
- Genetic counsellors
- Health information management professionals
- Medical physicists
- Midwives
- Opticians
- Optometrists
- Paramedics
- Pharmacy technicians
- Physician assistants
- Psychologists
- Respiratory therapists
- Social workers
- Speech–language pathologists
- Medical radiation technologists (MRTs)
- Medical laboratory technologists (MLTs)

2. The Health Personnel Database, a national database containing aggregate data, was transferred from Health Canada's Health Information Division to CIHI in 1995 and later renamed the Health Workforce Database (HWDB). The NDB began when CIHI assumed responsibility for data collection and management of record-level registered nurses data from Statistics Canada, starting with the 1996 data year. Developments in subsequent years, such as the creation of the HHRDB, further expanded CIHI's collection of record-level health workforce information.
3. CIHI collects the majority of its record-level data from regulatory/licensing authorities in the provinces and territories. A national association may submit data where no regulatory/licensing authority for a health care provider group exists in a jurisdiction. The data is collected on an annual basis.
4. The record-level data collected is defined by national minimum data sets maintained by CIHI for each type of health care provider. Through agreement with CIHI, regulatory/licensing authorities and national associations submit a set of standardized data to CIHI.
5. The record-level data submitted to CIHI is a subset of demographic, geographic, education and employment information collected by provincial/territorial licensing authorities, or national associations, during annual registration processes.
6. CIHI does not collect health care providers' names, work or home addresses (number, street name and city) or contact information (e.g., telephone number).
7. CIHI does collect postal code of residence with the record-level regulated nursing data.
8. Aggregate-level data is collected on an annual basis for inclusion in the HWDB, from a combination of professional associations, regulatory bodies and provincial and territorial government ministries.
9. CIHI provides national, standardized, supply-based data and allows for timely, objective and evidence-based analyses and cross-country comparisons to support key stakeholders in decision-making and policy formulation relevant to health workforce planning and management.
10. The data may also be used in conjunction with other data sources to support policy-making, approved analysis and research projects.

# 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 health workforce data in the Nursing Database (NDB), Health Human Resources Database (HHRDB) and Health Workforce Database (HWDB).

The HWDB collects aggregate data only. The NDB and HHRDB collect record-level data, including health workforce personal information, and therefore are the focus of this assessment. This PIA replaces the individual PIAs completed for the NDB and HHRDB in 2012, and the PIA addendum completed for the Health Personnel Database (now HWDB) in 2011. This PIA includes 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 NDB and HHRDB, 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, August 2017](#).

## 2 Background

### 2.1 Introduction to the HWDB, NDB and HHRDB

#### HWDB

The Health Personnel Database, a national database, was transferred to CIHI in 1995 from Health Canada's Health Information Division. Originating in the 1970s, the database held data on 31 health provider groups. The data holding was renamed the Health Workforce Database and today it holds data on 22 health provider groups.

The HWDB is the only national database containing such a broad variety of Canadian health care provider data. It enables time-series comparisons of health human resources at both national and provincial/territorial levels. For example, CIHI reports on the registration status and sex of providers for some groups.

The HWDB does not collect, use or disclose personal information. Record-level data is not collected in the HWDB, nor are any direct personal identifiers. The aggregate data collected may contain small cell sizes. However, in keeping with Section 32 of the [Health Workforce Privacy Policy, 2011](#), CIHI makes statistical information publicly available only in a manner designed to minimize any risk of identifiability and residual disclosure of personal information about individuals. As such, the HWDB will not be subject to further privacy analysis in this PIA. In compliance with CIHI's [Privacy Impact Assessment Policy, August 2017](#), further privacy assessment of the HWDB will be conducted should the situation change in the future.

For additional information on the health workforce information contained in the HWDB, please visit the [Health Workforce metadata](#) web page.

#### NDB

The NDB collects record-level data on 3 regulated professionals: registered nurses, including nurse practitioners, licensed practical nurses<sup>i</sup> and registered psychiatric nurses.<sup>ii</sup> Regulated nurses are integral to the functioning of Canada's health care systems and represent the largest group within the health care workforce.

---

i. The term licensed practical nurse (LPN) is used throughout this document. In Ontario, registered practical nurse (RPN), registered nursing assistant (RNA) and licensed nursing assistant (LNA) are accepted corresponding terms.  
ii. RPNs are educated and regulated as a separate profession in Manitoba, Saskatchewan, Alberta, British Columbia and Yukon only.



Since 1980, data has been collected on the supply and distribution of registered nurses in Canada. Historically, Statistics Canada was responsible for the collection and dissemination of RN data, and produced the *Revised Registered Nurses Data Series* (from 1980 to 1988) and the *Registered Nurses Management Data* (from 1989 to 1998). CIHI assumed responsibility for data collection and management in the 1996 data year and for dissemination of reports in the 1999 data year.

In 2002, CIHI began collecting record-level LPN and RPN data. Previously, only minimal aggregate information was available.

For additional information on the RN (including NP), LPN and RPN data contained in the NDB, please visit the [Health Workforce Metadata](#) web page.

## **OT, PT, pharmacist, MLT and MRT data in the HHRDB**

Between 2004 and 2009, CIHI undertook the Health Human Resources Databases Development Project to develop separate, national, supply-based databases on 5 groups of regulated health care providers. Collectively, these databases are referred to as the Health Human Resources Database (HHRDB). The results of the project were the creation of the following:

- Occupational Therapist Database (OTDB) and the Pharmacist Database (PDB) — first year of record-level data collection in 2006;
- Physiotherapist Database (PTDB) — first year of record-level data collection in 2007; and
- Medical Radiation Technologist Database (MRTDB) and Medical Laboratory Technologist Database (MLTDB) — first year of record-level data collection in 2008. Following completion of collection of the 2015 data, CIHI ceased collection of record-level MLT and MRT data (for more information, see the section [Changes to the NDB and HHRDB since 2012 PIAs](#)).

For additional information on OT, PT, pharmacist, MLT and MRT data contained in the HHRDB, please see the [Health Workforce Metadata](#) web page.

## 2.2 Data collection

NDB and HHRDB record-level data is collected from the provincial/territorial regulatory/licensing authority or national association, or from a provincial/territorial government that has already collected the necessary information from the provincial/territorial source. CIHI receives a subset of the information for secondary use, specifically to support the planning and management of the health system, including statistical analysis and reporting.

The NDB and HHRDB contain demographic, geographic, education and employment information on health care providers holding an active practising licence in a Canadian province/territory.

The following are examples of the data elements included in record-level collection in the NDB and HHRDB:

### **Demographic data**

- Registrant's provincial unique identification/registration number
- Sex
- Year of birth

### **Geographic data**

- Registrant's country or province/territory of residence at the time of registration or renewal
- Registrant's postal code of residence (regulated nurses only)
- Country, province/territory or university/institute registrant graduated in/from
- Employer's country or province/territory or postal code of registrant's employment location

### **Education data**

- University of graduation (entry to practice)
- Year of graduation (entry to practice)
- Level of education (entry to practice)

### **Employment**

- Category/status
  - Employed, unemployed
  - Permanent, temporary, self-employed
  - Full time, part time

Following is a description of selected data elements from the NDB and HHRDB that could be considered sensitive, as well as the purpose for their collection:

### **Jurisdictional Identification Number/Registration Number**

This number, assigned by each data provider,<sup>iii</sup> uniquely identifies a health care provider within the information system maintained by that data provider. CIHI collects only the Jurisdictional Identification Number/Registration Number; it does not collect names associated with it. This number is collected for the following purposes:

- To uniquely identify a professional within the information system maintained by each data provider, for purposes of communicating with the data provider and making required changes specific to that health care provider's information; and
- To enable longitudinal, retrospective and concurrent analyses of supply, distribution and mobility trends.

### **Sex**

This data element is required to determine trends in employment, recruitment and career patterns for HHR planning (e.g., proportion of the workforce that is female).<sup>iv</sup>

### **Year of Birth**

This data element is required to determine trends and to establish patterns for health workforce planning (e.g., to calculate the average age and age grouping of the workforce). Only the year of birth is collected. Day and month of birth are not collected to further protect the privacy of the registrants and to reduce the possibility of re-identification. Collecting year of birth provides maximum flexibility in responding to information needs associated with the age-related characteristics of the workforce (e.g., age-related retirement projections).<sup>iv</sup>

### **Postal Code of Residence**

For regulated nurses, CIHI collects the 6-character postal code of residence. It is required to support the following types of analysis:

- Methodology applied to provide a more accurate representation of workforce supply, by reducing the level of double counting of regulated nurses that register in more than one jurisdiction but are employed in only 1 (i.e., secondary registrants or interprovincial duplicates);

---

iii. Data providers may choose to submit pseudonymized numbers to CIHI instead of the registration number. Pseudonymized means that a registration number has been removed and a manufactured number assigned in its place. The manufactured number is assigned in a consistent manner that allows data users to determine that several records (e.g., records appearing in different data years) relate to the same individual.

iv. The College of Registered Nurses of Manitoba and the College of Licensed Practical Nurses of Manitoba do not supply CIHI with record-level sex and year of birth data, and the College of Occupational Therapists of Manitoba, the College of Physiotherapists of Manitoba and the College of Pharmacists of Manitoba supply incomplete information. In these circumstances, CIHI has worked collaboratively with these data providers and Manitoba Health to obtain sufficient information to address some of CIHI's analytical requirements.

- Sub-provincial/-territorial analysis of mobility/geography and distribution of the regulated nursing workforce (e.g., nurses living where they work or commuting from a rural to an urban centre); and
- Analysis with other common variables, such as education (i.e., barriers to continuing education) and employment.

The 6-digit postal code of residence by itself is not normally a person-identifiable data element; the postal code is attached to a geographic area. However, when the postal code is collected in combination with other data elements, such as profession, age and sex, it increases the possibility of re-identification of an individual (residual disclosure).

[Section 3.7](#) and [Section 3.9](#) describe CIHI's disclosure avoidance measures and security safeguards, respectively.

For a complete, detailed description of all data elements, values and rationale for collection, as well as record-level data sources, coverage and availability in the NDB and HHRDB, please see the [Health Workforce Metadata](#) web page.

## Changes to the NDB and HHRDB since 2012 PIAs

Since the last PIAs for the NDB and HHRDB were conducted in 2012, the following changes to data collection have taken place:

- Since 2013, CDs/USB keys with record-level data are no longer used to submit data to CIHI or to return data to data providers. CIHI now uses a secure web-based electronic Data Submission Services (eDSS) to receive data and the Data Dissemination Tool to return data to data providers.
- In 2015,
  - Automated reporting functionality for Compare Reports previously found in the HHRDB internal system ceased to be used, with responsibility for report generation transferred to Health Workforce Information staff. All associated work is now completed within CIHI's SAS environment, with return of data to data providers occurring via the DDT. The data processing functionality of the HHRDB internal system, used to generate error reports for providers of OT, PT and pharmacist data, remains operational with no external connection or functionality. The HHRDB internal system will be fully decommissioned in 2019–2020; the remaining error report generation functionality will be addressed within CIHI's SAS environment.

- In 2016,
  - Following the collection of 2015 data, CIHI ceased collection of record-level MLT and MRT data. A number of factors influenced this decision, including limited comparability of the data and variability in data quality across jurisdictions, limited uptake and use of the data by stakeholders, poor timeliness of data submissions, and increasing resource pressures facing data providers. The use, disclosure, retention and destruction of MLT and MRT data currently held by CIHI continue to be governed by CIHI's [Health Workforce Privacy Policy, 2011](#) and the agreements under which the data was originally collected. The data is available through CIHI's third-party data request process. CIHI will review the retention of the data at the next review cycle of this PIA to determine whether the data will continue to be retained or securely destroyed.
  - All LPN data submissions are submitted to CIHI via eDSS. Prior to 2016, CIHI received paper submission of LPN data from the Northwest Territories (paper submissions had all personal information redacted, prior to transfer to CIHI).

As of 2017, all activities formerly completed within a dedicated NDB system (e.g., data loading, processing and reporting) were migrated to CIHI's SAS environment. CIHI's Information Management Leadership Committee approved the decommissioning of the original NDB system, and it was decommissioned in August 2018. A privacy and security risk associated with this change was identified (see [Section 3.1](#) for more information).

## 2.3 Access management, data submission and flow for the NDB and HHRDB

Access to CIHI's secure applications is subject to CIHI's role-based access management process, which is managed by CIHI's Client Support Applications (CSA) department. CSA 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, NDB and HHRDB data providers submit record-level data to CIHI through CIHI's secure web-based eDSS.

At the time of processing, all submitted record-level NDB and HHRDB data automatically undergoes validation and a data quality check for errors and inconsistencies against specifications outlined in the manual for each health care provider group.<sup>v</sup> Data processing is internal to CIHI, with no external connection. Processing is completed through a combination of methods, including use of

---

v. Specification manuals for NDB and HHRDB record-level data collected by CIHI (OT, pharmacist, PT and regulated nurses) are available under Submission Support Resources at [cchi.ca](http://cchi.ca). At the time of this assessment, the following manuals were in use: *Occupational Therapist Database Manual, Version 3.0*; *Pharmacist Database Manual, Version 3.0*; *Physiotherapist Database Manual, Version 2.0*; and the *Regulated Nurses Database Data Element List*.

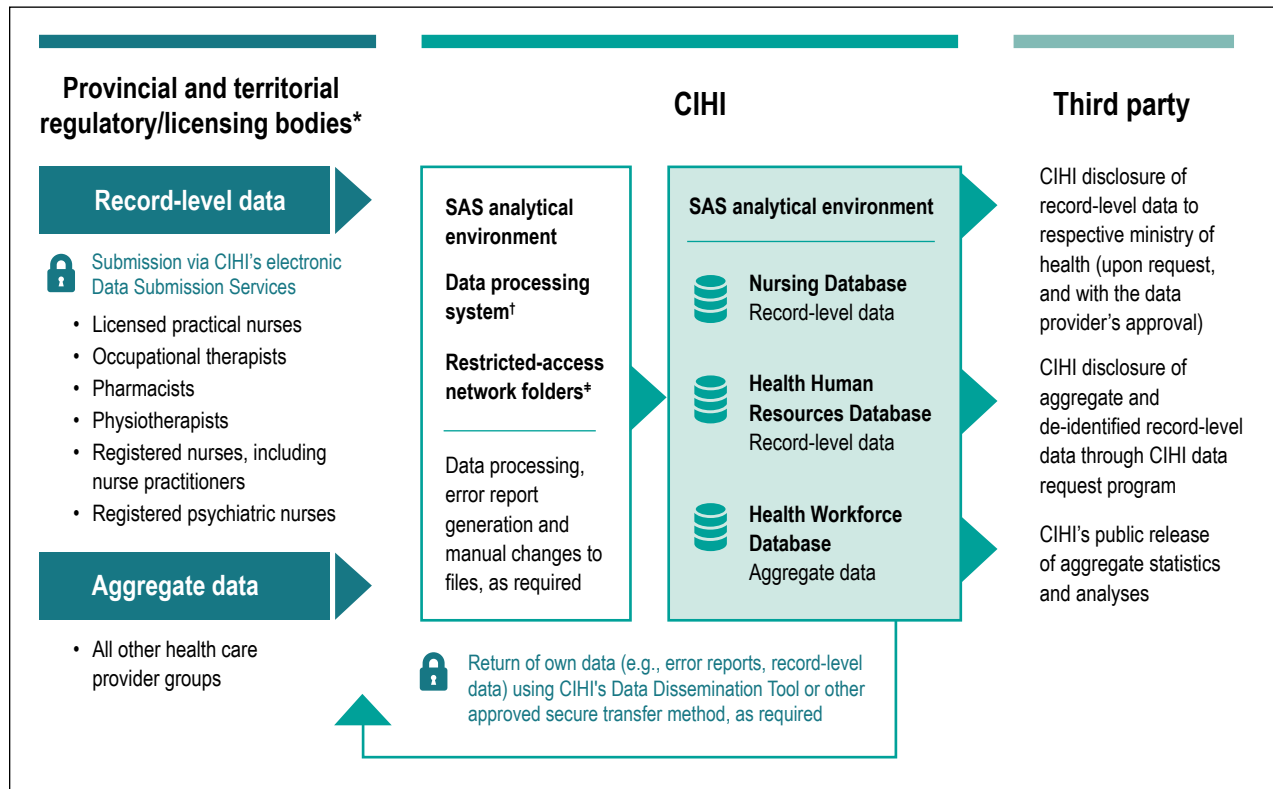
- CIHI's SAS analytical environment;
- An internal data processing system created during the Health Human Resources Development Project, used to generate error reports for some record-level data that has been collected. In 2019–2020, the system will be fully decommissioned, with activities transferred to the SAS environment; and
- Manual processing of files within restricted-access folders on CIHI's file server.

Error and validation reports generated at the time of processing are made available to the respective data providers via the DDT, in compliance with CIHI's *Secure Information Transfer Standard*. These reports identify records (using the registrant's provincial unique identification/registration number) with errors; specify the number of records a data provider has successfully submitted; indicate the reason records were rejected or the relevant warning message; and permit the data provider to correct errors in the records and resubmit them to the NDB and HHRDB.

Once the iterative error correction process is completed, final summary reports of file processing results are returned to data providers via the DDT. A complete copy of the NDB and HHRDB record-level data set is then uploaded to CIHI's SAS analytical environment where it is made available to approved CIHI staff for CIHI purposes. CIHI returns NDB and HHRDB data to the data provider that originally supplied the data. CIHI also discloses health workforce personal information to the respective ministry of health (upon request, and with the data provider's approval), aggregate and record-level data to other third-party requestors, and aggregate data to the public. The figure presents a high-level illustration of the data flows for the NDB, HHRDB and HWDB.

Staff access to the SAS analytical environment is provided through CIHI's centralized SAS Data Access process. The process ensures that all requests for access, including access to NDB and HHRDB record-level data, are traceable and authorized. The SAS Data Access system 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 NDB and HHRDB record-level data.

**Figure** Nursing Database, Health Human Resources Database and Health Workforce Database data flow



**Notes**

\* In some circumstances (e.g., a self-regulating licensing authority is not present in a jurisdiction), a national health professional association or government entity may be the CIHI data source.

† An internal system with no external connectivity, used to generate error reports for some record-level data that has been collected. The system will be fully decommissioned in 2019–2020.

‡ Restricted access folders on CIHI's file server.

## 3 Privacy analysis

### 3.1 Privacy and Security Risk Management Program

Privacy and security risk management (PSRM) 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. In 2015, CIHI approved its [Privacy and Security Risk Management Framework](#), and implemented the associated [Policy on Privacy and Security Risk Management](#). CIHI's chief privacy officer 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, for example. 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 Senior Management Committee on behalf of the corporation.



The following privacy and security risk was identified during this PIA:

**Privacy and security risk identified:** If products are not securely managed throughout the life cycle, including the decommissioning phase, security vulnerabilities can be introduced.

**Background:** On December 6, 2016, CIHI's Information Management Leadership Committee approved the decommissioning of the NDB system, which includes the NDB application and the NDB database. This PIA identified

- That decommissioning of the NDB was not complete and there was no firm date of completion scheduled (as described in [Section 2.2](#), full decommissioning of the NDB was subsequently completed August 2018); and
- That CIHI needed to develop an internal decommissioning standard.

**PSRM process:** The privacy and security risk identified above has been added to CIHI's Privacy and Security Risk Register, and will be assessed in accordance with PSRM methodology.

## 3.2 Authorities governing NDB and HHRDB data

### General

CIHI adheres to its [Health Workforce Privacy Policy, 2011](#) and to any applicable privacy legislation and/or legal agreements.

### Privacy legislation

CIHI is a secondary data collector of health workforce 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.

### Agreements

At CIHI, NDB and HHRDB data is governed by CIHI's [Health Workforce Privacy Policy, 2011](#), legislation in the jurisdictions and data-sharing agreements with each data provider (regulatory authority, government, professional association or society). The data-sharing agreements set out the purpose, use, disclosure, retention and disposal requirements of NDB and HHRDB data provided to CIHI, as well as any subsequent disclosures that may be 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, 2011](#). CIHI has a chief privacy officer and general counsel, a corporate Privacy, Confidentiality and Security Committee, a Governance and Privacy Committee of its Board of Directors, and an external chief privacy advisor.

### Organization and governance

The following table identifies key internal senior positions with responsibilities for NDB and HHRDB data in terms of privacy and security risk management:

**Table** Key positions and responsibilities

Position/group	Role/responsibilities
<b>Vice president, Programs</b>	Responsible for the overall strategic direction of the Health Workforce Information Program
<b>Director, Pharmaceuticals and Health Workforce Information Services</b>	Responsible for the overall operations and strategic business decisions of the NDB and HHRDB
<b>Manager, Health Workforce Information</b>	Responsible for day-to-day decisions regarding NDB and HHRDB operations
<b>Chief information security officer</b>	Responsible for the strategic direction and overall implementation of CIHI's Information Security Program
<b>Chief privacy officer</b>	Responsible for the strategic direction and overall implementation of CIHI's Privacy Program
<b>Manager, Data Acquisition Products</b>	Responsible for ensuring the availability of technical resources and solutions for ongoing operations and enhancements of data processing system

## 3.4 Principle 2: Identifying purposes for health workforce personal information

The NDB and HHRDB provide pan-Canadian, standardized, supply-based data and allow for timely, objective and evidence-based analyses and jurisdictional comparisons to support key stakeholders on decision-making and policy formulation relevant to health workforce planning and management.

The NDB and HHRDB collect health workforce personal information, including record-level demographic, education/training, geographic and employment data for health care provider groups identified previously in the [Quick facts section](#) and in [Section 2.1](#).

## 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 individuals in the health workforce. 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, 2011](#), 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 systems.

The focus of data collection for the NDB and HHRDB — demographic, geographic, education and employment information — represents a subset of the priority information needs for HHR planning and management that were identified and validated through an initial national consultation process by CIHI in 2005,<sup>vi</sup> and most recently in 2013.<sup>vii</sup>

A review and update of the variables included in NDB and HHRDB record-level collection are completed annually with data providers to ensure that the purposes of the NDB and HHRDB continue to be met.

Individual health care providers' names, home or work addresses (number, street name and city) and contact information (e.g., telephone number) are not collected in the NDB and HHRDB because they are not required for the purposes of the database.

CIHI makes data specifications and other associated documentation, such as file layouts, available to data providers. All submissions of record-level NDB and HHRDB data to CIHI must conform to the respective submission and edit specifications associated with each health care provider group.<sup>viii</sup>

---

vi. For more information, see Guidance Document for the Development of Data Sets to Support Health Human Resources Management in Canada (visit [cihi.ca](http://cihi.ca)).

vii. For more information, see *Health Human Resources Minimum Data Set Guide* (visit [cihi.ca](http://cihi.ca)).

viii. For more information on data elements included in NDB and HHRDB record-level collection, see the *Regulated Nurses Database Data Element List*, *Occupational Therapist Data Manual*, *Physiotherapist Data Manual* and the *Pharmacist Data Manual* (visit the [Health Workforce metadata](#) web page).

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

### Limiting use

CIHI limits the use of data in the NDB and HHRDB to the authorized purposes, as described in [Section 3.4](#). These include comparative analyses within and among jurisdictions; trend analyses to assess/monitor the impact of differences in policy, practices and service delivery; and 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.

### Data linkage

Sections 14 to 31 of CIHI's [Health Workforce Privacy Policy, 2011](#) 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 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. The linked data remains subject to the use and disclosure provisions in the [Health Workforce Privacy Policy, 2011](#).

Criteria for approval of data linkages are set out in sections 23 and 24 of CIHI's [Health Workforce Privacy Policy, 2011](#), 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:

- 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 health workforce personal 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.

## **Destruction of linked data**

Section 28 of CIHI's [Health Workforce Privacy Policy, 2011](#) 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, 2011](#) 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**

In addition to returning data to the submitting data provider, Section 34 of CIHI's [Health Workforce Privacy Policy, 2011](#) establishes that CIHI may return records to the relevant ministry of health where appropriate, for data quality purposes and for purposes consistent with their mandate. An example would be for health services management, including planning, evaluation and health human resources allocation. The return of own data is considered a use and not a disclosure.

## Limiting disclosure

### Third-party data requests

Customized record-level and/or aggregate data from the NDB and HHRDB may be requested by a variety of third parties.

CIHI administers a third-party data request program that 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, 2011](#), 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 aggregate 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, 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 has adopted a complete life cycle approach for record-level third-party data requests. As part of that life cycle, the Privacy and Legal Services branch 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, the Privacy and Legal Services branch 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.

## 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, 2011](#). CIHI may make publicly available aggregate health workforce data with units of observation of less than 5, where

- 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.

Starting in 2017, units of observation less than 5 are no longer suppressed in aggregate reporting of health care provider groups found in the NDB and HHRDB, with the exception of reports that include aggregate Yukon LPN data and/or aggregate RN data for the Northwest Territories and Nunavut in the NDB. Data providers for these jurisdictions continue to require CIHI to apply its standard cell suppression methodology for these 2 professions (i.e., units of observation no less than 5).

Aggregate statistics and analyses are made available in publications and on [CIHI's website](#).

## Limiting retention

The NDB and HHRDB 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 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, NDB and HHRDB data is subject to a 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 NDB and HHRDB data.

## 3.9 Principle 7: Safeguards for health workforce personal information

### 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 NDB and HHRDB 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.

CIHI's internal Health Workforce Privacy (2011) policy and procedures set 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 a 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 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, 2011](#) are available to the public on its corporate website at [cihi.ca](http://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, 2011](#).

### 3.12 Principle 10: Questions, concerns or 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, 2011](#), questions, concerns or complaints about CIHI's handling of health workforce personal information are investigated by the chief privacy officer, who may direct an inquiry or complaint to the privacy commissioner of the jurisdiction of the person making the inquiry or complaint.

## 4 Conclusion

CIHI's assessment of the NDB and HHRDB identified 1 privacy/security risk (see [Section 3.1](#)).

Any recommendations resulting from a PIA, including those arising from PSRM assessments initiated because of a PIA, are tracked in the Corporate Action Plan Master Log of Recommendations, and monitoring and follow-up action is taken accordingly to ensure implementation.

This PIA will be updated or renewed in compliance with CIHI's [Privacy Impact Assessment Policy, August 2017](#).

## Appendix: Text alternative for figure

Data collection by CIHI: Once authenticated through CIHI's access management system processes for granting and revoking access, NDB and HHRDB data providers submit record-level data to CIHI through CIHI's secure web-based electronic Data Submission Services. HWDB data is aggregate level and may be submitted to CIHI via other means.

Internal data processing following collection by CIHI: All data submitted to CIHI undergoes data processing and a data quality check for errors and inconsistencies, within 1 of 3 restricted-access internal environments, before being integrated into the respective database within CIHI's SAS analytical environment. Error and validation reports generated at the time of processing are made available to the respective data providers via the Data Dissemination Tool in compliance with CIHI's *Secure Information Transfer Standard*.

CIHI return, disclosure and use of data: CIHI staff access data within the SAS analytical environment on a need-to-know basis, to return data to the original data provider, to fulfill third-party data requests, and to release aggregate statistics and analyses to the public.



**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

20831-1019

