



# Ontario Mental Health Reporting System

## Privacy Impact Assessment

June 2022



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)

© 2022 Canadian Institute for Health Information

RAI-MDS 2.0 © interRAI Corporation, Washington, D.C., 1995, 1997, 1999. Modified with permission for Canadian use under licence to the Canadian Institute for Health Information. Canadianized items and their descriptions © Canadian Institute for Health Information, 2022.

How to cite this document:

Canadian Institute for Health Information. *Ontario Mental Health Reporting System Privacy Impact Assessment, June 2022*. Ottawa, ON: CIHI; 2022.

Cette publication est aussi disponible en français sous le titre *Système d'information ontarien sur la santé mentale : évaluation des incidences sur la vie privée, juin 2022*.

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

- *Ontario Mental Health Reporting System Privacy Impact Assessment*

Approved by

Brent Diverty

Vice President, Data Strategies and Statistics

Rhonda Wing

Executive Director, Chief Privacy Officer and General Counsel

Ottawa, June 2022

# Table of contents

Quick facts about the Ontario Mental Health Reporting System .....	5
1 Introduction .....	5
2 Background .....	6
What is OMHRS? .....	6
History of OMHRS .....	6
2.1 Data providers .....	7
2.2 Data collection .....	7
2.3 Data flows .....	8
2.4 Access management and data submission .....	9
3 Privacy analysis .....	9
3.1 Privacy and Security Risk Management Program .....	9
3.2 Authorities governing OMHRS data .....	10
3.3 Principle 1: Accountability for personal health information .....	11
3.4 Principle 2: Identifying purposes for personal health information .....	12
3.5 Principle 3: Consent for the collection, use or disclosure of personal health information .....	13
3.6 Principle 4: Limiting collection of personal health information .....	13
3.7 Principle 5: Limiting use, disclosure and retention of personal health information .....	14
3.8 Principle 6: Accuracy of personal health information .....	20
3.9 Principle 7: Safeguards for personal health information .....	20
3.10 Principle 8: Openness about the management of personal health information .....	22
3.11 Principle 9: Individual access to, and amendment of, personal health information .....	22
3.12 Principle 10: Complaints about CIHI's handling of personal health information .....	22
4 Conclusion .....	22
Appendix .....	23
Text alternative for figure .....	23

# Quick facts about the Ontario Mental Health Reporting System

1. The Ontario Mental Health Reporting System (OMHRS) is a Canadian Institute for Health Information (CIHI) database that captures data about hospital inpatient mental health care. CIHI analyzes this data and uses it to produce accurate, timely and comparable statistical information about access to care, quality of care and the resources consumed in providing that care.
2. Facilities, ministries of health, and regional health authorities use this information to make better-informed decisions about hospital inpatient mental health care.
3. OMHRS primarily collects information about adult hospital inpatient mental health care provided in Ontario. OMHRS also currently receives data from a small number of facilities in Newfoundland and Labrador and Manitoba.
4. Each OMHRS record reflects the OMHRS minimum data set and includes personal identifiers, demographic information, health characteristics, administrative information, health facility identifiers and free text fields.

## 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 Ontario Mental Health Reporting System (OMHRS). This PIA, which replaces the November 2016 version, includes both a review of the 10 privacy principles set out in the Canadian Standards Association's *Model Code for the Protection of Personal Information* and how the principles apply to the OMHRS, as well as a look at the application of CIHI's [Privacy and Security Risk Management Framework](#).

The primary driver for this PIA is compliance with CIHI's [Privacy Impact Assessment Policy](#).

## 2 Background

### What is OMHRS?

OMHRS is a CIHI database that contains data about hospital inpatient mental health care. This data is used to produce accurate, timely and comparable statistical information on hospital inpatient mental health care including access to care, quality of care and the resources consumed in providing that care. Facilities, ministries of health, and regional health authorities use this information to make better-informed decisions about hospital inpatient mental health care.

OMHRS primarily contains information about *adult* hospital inpatient mental health care provided in Ontario. OMHRS also contains some information about *youth* hospital inpatient mental health care provided in Ontario, and some information about adult hospital inpatient mental health care provided in provinces and territories outside Ontario. OMHRS does not collect data regarding mental health care provided by outpatient or community-based services such as residential care facilities (e.g., group homes) or private practitioners.

### History of OMHRS

Prior to 1994, Statistics Canada’s Mental Health Statistics program was responsible for collecting data regarding hospital inpatient mental health care, via the Hospital Mental Health Survey (HMHS). While Statistics Canada still maintains historical data for 1930 to 1994, CIHI assumed responsibility for collecting and analyzing data regarding hospital inpatient mental health care as of 1994–1995.

Initially, CIHI collected information about mental health care provided by hospitals via CIHI’s Discharge Abstract Database (DAD), which is designed to capture information about hospital care generally.

In the early 2000s, CIHI and the Ontario Ministry of Health — the primary provincial stakeholder and sponsor of OMHRS — identified the need for a specialized hospital mental health database to capture standardized, patient-specific, clinical, demographic, administrative and resource utilization information; CIHI developed OMHRS in response. As of March 31, 2021, OMHRS contained more than 1.6 million records, representing over 900,000 episodes of care from over 90 facilities (*episode of care* means the period of time between the patient being admitted to the facility and the patient being discharged from the facility).

## 2.1 Data providers

The Ontario Ministry of Health mandated Ontario facilities with designated adult mental health beds to begin submitting data to OMHRS in 2005. Some facilities in other provinces and territories began submitting data to OMHRS on a voluntary basis in 2008, and OMHRS currently receives data from a small number of facilities in Newfoundland and Labrador and Manitoba.

## 2.2 Data collection

### **Resident Assessment Instrument–Mental Health**

Hospitals collect patient information during the course of delivery of inpatient mental health care services. To collect this information in a standardized fashion, OMHRS-submitting facilities use a tool called the Resident Assessment Instrument–Mental Health (RAI-MH). The RAI-MH was developed collaboratively by CIHI, interRAI (a network of researchers and practitioners committed to improving care for persons who are disabled or medically complex), the Ontario Ministry of Health, the Ontario Hospital Association (OHA) and selected pilot hospitals. These collaborators determined which data elements to include in the initial data set and are involved in updating the data set from time to time in order to improve the quality or relevance of the data collected, to align the data set with updated interRAI instrument standards, or to meet other needs of the Ontario Ministry of Health, the OHA or CIHI.

Some of the data collected by facilities using the RAI-MH is included in the OMHRS record submitted to CIHI about the individual. Specifically, each OMHRS record reflects the OMHRS minimum data set and includes personal identifiers, demographic information, health characteristics, administrative information, health facility identifiers and free text fields. Further information about the data included in the OMHRS minimum data set can be found on [CIHI's website](#).

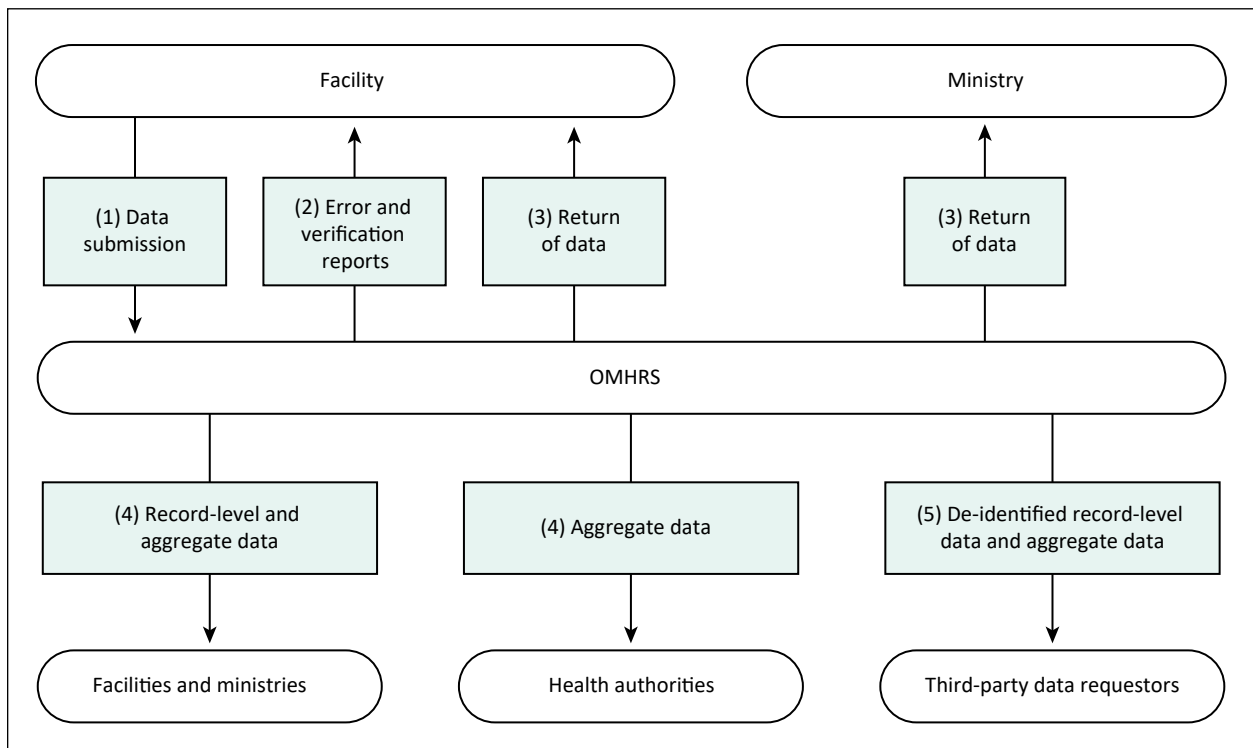
## 2.3 Data flows

OMHRS data flows are as follows:

1. The facility submits records to CIHI.
2. OMHRS makes available submission reports to help the facility correct errors in the records (e.g., missing data elements).
3. A copy of the records as accepted by OMHRS, as well as reports that contain personal health information, are available to the facility and the ministry. The Ontario Ministry of Health does not receive data submitted by facilities in Manitoba and Newfoundland and Labrador, while the respective ministry in Manitoba and Newfoundland and Labrador receives data submitted by facilities in that province — along with Ontario data aggregated to the province level, for comparison purposes.
4. CIHI provides record-level and aggregate data to facilities that submit data, and to the ministry. CIHI provides aggregate data to health authorities.
5. CIHI provides de-identified record-level and aggregate data to third-party data requestors, upon request (see [Section 3.7](#)).

The figure below illustrates OMHRS data flows.

**Figure** OMHRS data flows





## 2.4 Access management and data submission

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

Software extracts data directly from the facility's records. Then, once the organization has been authenticated through CIHI's AMS, it can submit that record-level data to OMHRS via CIHI's secure web-based electronic Data Submission Services (eDSS).

# 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 Executive Committee on behalf of the corporation.

As indicated in [Section 3.4](#), CIHI is currently undertaking a PSRM process regarding free text fields.

There were no other privacy and security risks identified as a result of this PIA.

## 3.2 Authorities governing OMHRS data

### General

CIHI adheres to its [Privacy Policy, 2010](#) and to any applicable privacy legislation and/or legal agreements.

### Privacy legislation

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

The following provinces and territories have enacted health information–specific privacy legislation: Newfoundland and Labrador, Prince Edward Island, Nova Scotia, New Brunswick, Ontario, Manitoba, Saskatchewan, Alberta, Yukon and the Northwest Territories. Health information–specific privacy legislation authorizes facilities to disclose personal health information without patient consent for the purposes of health system use, provided that certain requirements are met. For example, CIHI is recognized as a prescribed entity under the *Personal Health Information Protection Act* of Ontario, so health information custodians in Ontario may disclose personal health information to CIHI without patient consent pursuant to Section 29 as permitted by Section 45(1) of the act.

In provinces and territories that do not currently have health information–specific privacy legislation in place, facilities are governed by public-sector legislation. This legislation authorizes facilities to disclose personal information for statistical purposes without an individual's consent.

## Agreements

At CIHI, OMHRS data is governed by CIHI's [Privacy Policy, 2010](#), by legislation in the jurisdictions and by data-sharing agreements with the provinces and territories. The data-sharing agreements set out the purpose, use, disclosure, retention and disposal requirements of personal health information provided to CIHI, as well as any subsequent disclosures that may be permitted. The agreements also describe the legislative authority under which personal health information is disclosed to CIHI.

### 3.3 Principle 1: Accountability for personal health information

CIHI's president and chief executive officer is accountable for ensuring compliance with CIHI's [Privacy Policy, 2010](#). CIHI has a chief privacy officer and general counsel, a corporate Privacy, Confidentiality and Security Committee, 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 OMHRS data in terms of privacy and security risk management:

**Table** Key positions and responsibilities

Position/group	Roles/responsibilities
<b>Vice President, Data Strategies and Statistics</b>	Responsible for the overall strategic direction of the OMHRS
<b>Director, Specialized Care</b>	Responsible for the overall operations and strategic business decisions of OMHRS
<b>Manager, Specialized Care Data Management</b>	Responsible for overall operations and maintenance of OMHRS
<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

## 3.4 Principle 2: Identifying purposes for personal health 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 producing information about hospital inpatient mental health care to support the planning and management of publicly funded services in Canada. In order to fulfil these goals, CIHI collects the following types of OMHRS data for the purposes indicated.

### Personal identifiers

Examples include health care number and OMHRS-specific patient identifier. CIHI uses this information to develop a complete picture of the care provided to an individual by linking together records describing the different types of care provided to the individual, at different times, by different facilities. In order to perform these linkages, CIHI needs to know which records pertain to the individual. Accordingly, all records must include identifying information.

### Demographic information

Examples include birthdate, postal code, sex, marital status, language, education, vocational status and Indigenous-identifiable data. CIHI uses age (calculated using date of birth), geographic information (derived from postal code), sex, language, vocational status and Indigenous-identifiable data for demographic analysis of health care services and outcomes.

### Health characteristics

Examples include reason for admission, family relationships, experience of abuse, addictions, mental health diagnoses, medication history, treatments recently provided, risk of harming self or others, and physical health issues. CIHI uses this information to evaluate the types of conditions that require hospital inpatient mental health services, the quality of care provided to the individual and the costs associated with treatment.

### Administrative information

Examples include dates for admission and discharge from the facility. CIHI uses this information to evaluate wait times for care and resources consumed in providing care.

## Health facility information

Examples include the names/codes of facilities providing care, along with information that the Ontario Ministry of Health requires for analytical purposes (e.g., type, size and location of facilities). CIHI uses this information to prepare information that is specific to a given facility or group of facilities.

## Free (open) text fields

Fields are designed to permit the collection of unstructured data. For example, special project fields may permit the capture of information necessary to support a project that CIHI, the provinces and territories or health care facilities decide to undertake. Free text fields are not intended to contain personal health information. CIHI regularly evaluates the risk of a facility entering personal health information (e.g., health care number, name) into a free text field and takes steps to address this risk (e.g., checking these fields for personal health information, restricting internal and external access to such fields). Risks associated with free text fields are currently being evaluated using CIHI's Privacy and Security Risk Management Program, discussed in [Section 3.1](#).

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

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

## 3.6 Principle 4: Limiting collection of personal health information

CIHI is committed to the principle of data minimization. Per sections 1 and 2 of CIHI's [Privacy Policy, 2010](#), CIHI collects from data providers only the information that is reasonably required for health system uses, including statistical analysis and reporting, in support of the management, evaluation and monitoring of health care systems. Accordingly, OMHRS collects only the information it requires for these purposes.

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

### Limiting use

CIHI limits the use of OMHRS data to 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

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 the Statistical Analysis System (SAS) environment is provided through CIHI's centralized SAS Data Access process, which is managed through CIHI's Service Desk. This environment is a separate, secure space for analytical data files, including general use data files, where staff are required to conduct and store the outputs from their analytical work.

The general use data files are pre-processed files designed specifically to support internal analytical users' needs. This pre-processing includes the removal of the original health care number (replaced with an encrypted health care number), and full date of birth and full postal code, which are replaced by a set of standard derived variables.

The process ensures that all requests for access, including access to OMHRS data, are traceable and authorized, in compliance with Section 10 of CIHI's [Privacy Policy, 2010](#). 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 OMHRS data.

### Data linkage

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

Sections 14 to 31 of CIHI's [Privacy Policy, 2010](#) govern linkage of records of personal health information. Pursuant to this policy, CIHI permits the linkage of personal health 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. When carrying out data linkages, CIHI will generally do so using consistently encrypted health care numbers. The linked data remains subject to the use and disclosure provisions in the [Privacy Policy, 2010](#).

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

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

Section 24 All of the following criteria are met:

- a. The purpose of the data linkage is consistent with CIHI's mandate;
- b. The public benefits of the linkage significantly offset any risks to the privacy of individuals;
- c. The results of the data linkage will not be used for any purpose that would be detrimental to the individuals that the personal health information concerns;
- d. The data linkage is for a time-limited specific project and the linked data will be subsequently destroyed in a manner consistent with sections 28 and 29; or
- e. The data linkage is for purposes of an approved CIHI ongoing program of work where the linked data will be retained for as long as necessary to meet the identified purposes and, when no longer required, will be destroyed in a manner consistent with sections 28 and 29; and
- f. The data linkage has demonstrable savings over other alternatives or is the only practical alternative.

## Client linkage standard

In 2015, CIHI implemented a corporate-wide client linkage standard to be used for the linkage of records created in 2010–2011 or later, where the records include the following data elements: Encrypted Health Care Number and Province/Territory That Issued the Health Care Number. For the linkage of records that do not satisfy these criteria, the linkage mechanism is determined on a case-by-case basis.

## **Destruction of linked data**

Section 28 of CIHI's [Privacy Policy, 2010](#) sets out the requirement that CIHI will destroy personal health 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 [Privacy Policy, 2010](#) further requires that for time-limited specific projects, the secure destruction of linked data will occur within 1 year after publication of the resulting analysis, or 3 years after the linkage, whichever is sooner, in a manner consistent with CIHI's *Secure Destruction Standard*. For linked data resulting from an ongoing program of work, secure destruction will occur when the linked data is no longer required to meet the identified purposes, in a manner consistent with CIHI's *Secure Destruction Standard*. These requirements apply to data linkages both for CIHI's own purposes and for third-party data requests.

## **OMHRS supports HMHDB**

CIHI merges records from OMHRS with records from CIHI's [Discharge Abstract Database \(DAD\)](#) to create an additional CIHI database called the [Hospital Mental Health Database \(HMHDB\)](#), which provides information about inpatient mental health care across the country.<sup>i</sup>

This activity does not qualify as data linkage as defined by CIHI's [Privacy Policy, 2010](#) because it does not result in the creation of new composite records. Data linkages in general are discussed in [Section 3.7](#).

## **Return of own data**

A submitting organization can access secure web-based submission reports, which indicate how many records the organization has successfully submitted to OMHRS. These reports also indicate which records were not submitted successfully and the reason (e.g., the records were missing information). The reports permit the organization to identify errors in the records so that it may correct and resubmit them. In order to identify the records that contain errors, the report refers to the client identifier that the organization assigns to each patient; the report contains no health card numbers.

---

i. HMHDB also collects data directly from a single facility in Canada.



In addition to returning data to submitting facilities, Section 34 of CIHI's [Privacy Policy, 2010](#) establishes that CIHI may return records to the relevant ministry 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) or as directed in the data-sharing agreement or other legal instrument. Accordingly, CIHI makes record-level OMHRS data for Ontario facilities submitting to OMHRS available to the facilities and the Ontario Ministry of Health. These reports do not reflect data submitted by facilities in Manitoba and Newfoundland and Labrador. CIHI also makes record-level OMHRS data for Manitoba and Newfoundland and Labrador facilities submitting to OMHRS available to the respective ministry of health. These reports reflect Ontario data aggregated to the province level, for comparison purposes.

## Limiting disclosure

### Disclosing reports

CIHI provides comparative reports to all data providers on a quarterly basis. These reports provide aggregated facility-identifiable data to enable data providers to analyze their data over time and compare themselves with other similar service providers. The reports also include, for each facility, record-level data based on that facility's own submissions.

As a safeguard, before receiving access to the reports, the organization must sign a service agreement that, among other things,

- Restricts use of the data to non-commercial purposes limited to the client's internal management, data quality, planning, research, analysis, or evidence-based decision-support activities;
- Prohibits disclosure of the data to any third party, except in the case of the client's own data;
- Permits publication only once all reasonable measures have been employed to prevent the identification of individuals, and once the data does not contain cell sizes with fewer than 5 observations; and
- Prohibits the release of health facility-/organization-identifiable information unless the client has notified CIHI prior to the disclosure, in order to permit CIHI to notify the applicable ministry.

## Agreement with interRAI

CIHI signed a licence agreement with interRAI — a network of researchers and practitioners committed to improving care for persons who are disabled or medically complex. This licence grants CIHI an exclusive right to use interRAI’s assessment instruments in Canada for the purposes of national statistical reporting. The licence agreement also commits CIHI to supply interRAI with an annual copy, in de-identified form, of the data collected using the interRAI assessment instruments — including data submitted to OMHRS. Accordingly, CIHI provides interRAI with de-identified data from OMHRS under a data-sharing agreement that establishes the purposes for which interRAI may use the data (e.g., to develop assessment forms), along with interRAI’s responsibilities to protect the data.

## Third-party data requests

Customized record-level and/or aggregated data from OMHRS may be requested by a variety of third parties.

CIHI administers the 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 [Privacy Policy, 2010](#), CIHI discloses health information in a manner consistent with its mandate and core functions, and CIHI data disclosures are made at the highest degree of anonymity possible while still meeting the research and/or analytical purposes of the requester. This means that, whenever possible, data is aggregated. When aggregated data is not sufficiently detailed for the intended purpose, record-level de-identified data or personal health 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.

As the preferred means of record-level data access, CIHI uses a secure access environment (SAE). CIHI’s SAE is an encrypted, secure environment hosted in CIHI’s data centre. Consistent with CIHI’s existing policies and procedures, approved researchers — who are subject to stringent agreement terms — access data extracts that have been prepared and vetted by CIHI staff for an approved research project. Record-level data cannot be copied or removed from the SAE; only aggregate results can be extracted from the SAE. Further information about CIHI’s SAE is available on [CIHI’s website](#) ([Make a Request](#); [SAE Privacy Impact Assessment](#)).

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

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

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

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

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

## Limiting retention

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

## 3.8 Principle 6: Accuracy of personal health 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, OMHRS 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 OMHRS data.

## 3.9 Principle 7: Safeguards for personal health 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 OMHRS data are highlighted below.

### System security

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

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

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

CIHI's employees are made aware of the importance of maintaining the confidentiality of personal health 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 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 personal health information

CIHI makes information available about its privacy policies, data practices and programs relating to the management of personal health information. Specifically, CIHI's [Privacy and Security Framework](#) and [Privacy Policy, 2010](#) are available to the public on its corporate website ([cihi.ca](http://cihi.ca)).

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

Personal health 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 personal health information will be processed in accordance with sections 60 to 63 of CIHI's [Privacy Policy, 2010](#).

### 3.12 Principle 10: Complaints about CIHI's handling of personal health information

As set out in sections 64 and 65 of CIHI's [Privacy Policy, 2010](#), questions, concerns or complaints about CIHI's handling of information are investigated by the chief privacy officer, 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 OMHRS did not identify any privacy or security risks.

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

# Appendix

## Text alternative for figure

### Figure: OMHRS data flows

OMHRS data flows are as follows:

1. The facility submits records to CIHI.
2. OMHRS makes available submission reports to help the facility correct errors in the records (e.g., missing data elements).
3. A copy of the records as accepted by OMHRS, as well as reports that contain personal health information, are available to the facility and the ministry. The Ontario Ministry of Health does not receive data submitted by facilities in Manitoba and Newfoundland and Labrador, while the respective ministry in Manitoba and Newfoundland and Labrador receives data submitted by facilities in that province — along with Ontario data aggregated to the province level, for comparison purposes.
4. CIHI provides record-level and aggregate data to facilities that submit data, and to the ministry. CIHI provides aggregate data to health authorities.
5. CIHI provides de-identified record-level and aggregate data to third-party data requestors, upon request (see [Section 3.7](#)).

**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

18615-0622

