



Your Health System: Insight

Privacy Impact Assessment

December 2021



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

copyright@cihi.ca

© 2022 Canadian Institute for Health Information

How to cite this document:

Canadian Institute for Health Information. *Your Health System: Insight Privacy Impact Assessment, December 2021*. Ottawa, ON: CIHI; 2022.

Cette publication est aussi disponible en français sous le titre *Votre système de santé : En profondeur — évaluation des incidences sur la vie privée, décembre 2021*.

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

- *Your Health System: Insight Privacy Impact Assessment, December 2021*

Approved by

Neala Barton

Vice President, Communications and Client Experience

Rhonda Wing

Executive Director, Chief Privacy Officer and General Counsel

Ottawa, December 2021

Table of Contents

Quick facts about the Your Health System: Insight web tool	6
Definitions	7
1 Introduction	8
2 Background	8
2.1 Introduction to Your Health System: Insight	8
2.2 Data	10
CIHI data	10
Statistics Canada data	12
2.3 Access management and data flow for Your Health System: Insight	12
Access	13
Data flows	14
3 Privacy analysis	16
3.1 Privacy and Security Risk Management Program	16
3.2 Authorities governing Your Health System: Insight data	17
General	17
Privacy legislation	17
Agreements	17
3.3 Principle 1: Accountability for personal health information	18
Organization and governance	18
3.4 Principle 2: Identifying purposes for personal health information	19
3.5 Principle 3: Consent for the collection, use or disclosure of personal health information	19
3.6 Principle 4: Limiting collection of personal health information	19
3.7 Principle 5: Limiting use, disclosure and retention of personal health information	20
Limiting use	20
Limiting disclosure	22
Limiting retention	22
3.8 Principle 6: Accuracy of personal health information	23
Cautionary notes: Use and interpretation	23
3.9 Principle 7: Safeguards for personal health information	23
CIHI's Privacy and Security Framework	23
System security	24

3.10 Principle 8: Openness about the management of personal health information	25
3.11 Principle 9: Individual access to, and amendment of, personal health information . .	25
3.12 Principle 10: Complaints about CIHI’s handling of personal health information	25
4 Conclusion	26
Appendices	27
Appendix A: Indicators	27
Appendix B: Text alternative for figure	28

Quick facts about the Your Health System: Insight web tool

1. Your Health System: Insight builds on CIHI's years of experience in reporting indicators and measures that support Canada's health systems in monitoring performance and management.
2. Your Health System: Insight is an analytical web-based tool in a secured private environment. The tool is not publicly available.
3. Clients must sign the Electronic Reporting Services Agreement with CIHI in order to access Your Health System: Insight. The agreement limits clients' rights to use and disclose information obtained through Your Health System: Insight.
4. It is a tool to be used by clients, such as individual health care facilities, regional health authorities or participating provincial and territorial ministries or departments of health, to get quick, easy access to their results on key performance indicators as well as the underlying data.
5. Your Health System: Insight offers its clients access to closed- and open-year data, access to constantly evolving web tool features and data, and the ability to view performance drivers and pan-Canadian comparisons in different ways. Combined, this helps clients better understand what's driving their performance, compare their results with those of others across Canada, and improve in their part of Canada's health systems.
6. Your Health System: Insight contains clinical and administrative data from CIHI's Clinical Administrative Databases (the Discharge Abstract Database–Hospital Morbidity Database and the National Ambulatory Care Reporting System). The data was collected in its original form through the administration of various jurisdictions' health care systems and provided to CIHI as a secondary user. The cost estimates in Your Health System: Insight are derived from the Cost of a Standard Hospital Stay indicator and Resource Intensity Weights.
7. The aggregate data contained in Your Health System: Insight includes indicators and measures from the acute care setting that are reported at the facility level (by name) and regional, provincial, territorial and national levels, and that are available to all designated users.
8. A key feature of Your Health System: Insight is the automated return of record-level information, which is the contributing data used to build a particular indicator. This feature allows designated users of clients that are data providers to reconcile their indicator results with their own locally held data, and to use the data to identify underlying factors that may be driving their results.
9. Data in Your Health System: Insight is refreshed monthly to support clients in monitoring their performance and progress in a timely manner.
10. Your Health System: Insight was designed in consultation with users, so it has an intuitive design. Navigation is quick and simple; there are no deeply layered menus.

Definitions

For the purposes of this privacy impact assessment, the following terms have the following meanings.

Aggregate data means record-level data that has been compiled to a level of aggregation that ensures the identity of individuals cannot be determined by reasonably foreseeable methods.

Client means the organization specified in CIHI's Electronic Reporting Services Agreement that is binding itself to comply with the terms of the agreement.

Contextual measures refers to additional information that helps to explain or interpret the indicator results (e.g., number of acute care stays, average length of stay, percentage of alternate level of care).

Data provider means an organization, health care provider or other individual that discloses health information to CIHI; this may include ministries of health, regional health authorities and similar bodies, and hospitals and other health care facilities.

Designated user means a client's employee or permitted contractor who has been authorized by the client to access and use Your Health System: Insight.

Health facility–identifiable information means information that directly identifies a health facility by name.

Record-level data means data in which each record is related to a single individual.

Your Health System: Insight data means any aggregate data and record-level data included in the Your Health System: Insight web tool.

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 Your Health System: Insight. This PIA, which replaces the October 2015 version, includes a review of the 10 privacy principles set out in the Canadian Standards Association's *Model Code for the Protection of Personal Information*, as the principles apply to Your Health System: Insight, and 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

Your Health System: Insight builds on CIHI's years of experience in reporting indicators and measures that support Canada's health systems in monitoring performance and management. It serves as an analytical centre to provide authorized users with a deeper look at various standardized indicators and summary measures on health system performance.

2.1 Introduction to Your Health System: Insight

Your Health System: Insight was the first product delivered under the Integrated eReporting approach, which provides a seamless, targeted and integrated reporting experience for CIHI stakeholders to support the management of Canada's health systems. The solution is implemented in a restricted environment and offers authorized users




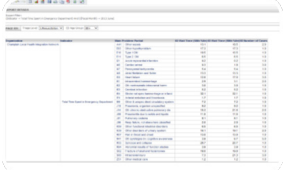
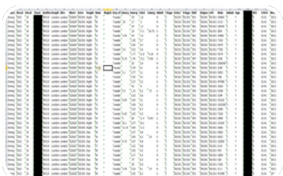
- A summary of health system performance and management measures at a glance through visualizations and a summary dashboard;
- Trending and pan-Canadian comparisons with customizable peer groups at the facility, regional, provincial or territorial, and national levels;

- A breakdown of indicator results by relevant clinical and administrative data elements (e.g., admission category, triage level, sex, age); and
- Functionalities to save, print and export results.

Designated users of clients that are data providers will have the added benefit of being able to explore and unpack their indicators, reconcile their indicator results with their own locally held data by allowing them to access and drill down to the underlying patient record-level data and factors that may be driving their results, and save, print and export those results (see Table 1).

Your Health System: Insight includes health system indicators, operations and utilization measures and contextual measures for each participating facility. These indicators focus on measures in the areas of access, safety, appropriateness and effectiveness from the acute care setting (see Appendix A for a list of indicators and measures available). As part of the integration initiative, CIHI plans to increase the number of indicators and measures to include those reported in other CIHI eReporting products.

Table 1 Features of Your Health System: Insight

	<p>Summary results</p> <ul style="list-style-type: none"> • Customize your user preference • View a summary of performance and trends • Identify potential improvement opportunities
	<p>Trends and comparisons</p> <ul style="list-style-type: none"> • View results over time • Select comparators • Get a presentation-ready report (export to interactive PDF)
	<p>Visual exploration</p> <ul style="list-style-type: none"> • Use data visualizations to explore your results • Uncover potential performance drivers • Customize to suit your needs
	<p>Custom breakdowns</p> <ul style="list-style-type: none"> • Use prompts to create custom reports • Drill into your results, right down to the chart number • Contrast results with those of your comparators
	<p>Chart export</p> <ul style="list-style-type: none"> • Export your results, right down to the chart number • Integrate your results into your own system

Your Health System: Insight clients are categorized in 1 of 2 community groups:

- **Data providers**, which are organizations that disclose health information to CIHI (e.g., health care facilities, regional health authorities); and
- **Non-data providers**, which are
 - Pan-Canadian organizations not subject to provincial or territorial jurisdictional control;
 - Provincial or territorial organizations (e.g., health quality councils); and
 - Federal government departments and agencies.

2.2 Data

Your Health System: Insight utilizes existing record-level data from CIHI's Clinical Administrative Databases (CAD) and Organization Index (OI) and contains geographic data from Statistics Canada.

CIHI data

Clinical Administrative Databases

The CAD is composed of 2 pan-Canadian databases: the Discharge Abstract Database–Hospital Morbidity Database (DAD-HMDB) and the National Ambulatory Care Reporting System (NACRS).

Discharge Abstract Database–Hospital Morbidity Database

The DAD-HMDB contains data on all acute care hospital inpatient separations, data on day surgery separations from certain provinces and territories, and limited data from long-term care, rehabilitation and mental health facilities. Examples of such information are patient demographic, diagnostic, intervention and health facility–identifiable information, and other care delivery aspects and administrative information.

National Ambulatory Care Reporting System

NACRS contains clinical, administrative and demographic information for hospital-based and community-based ambulatory care, including day surgery from certain provinces and territories, outpatient clinics and emergency departments.

(Refer to [Clinical Administrative Databases — Privacy Impact Assessment, August 2019](#).)

While the CAD contains full postal codes, full dates of birth, encrypted health card numbers of recipients (patients) and health care provider numbers (identifiers), Your Health System: Insight does not. Neither the CAD nor Your Health System: Insight contains the names of patients or health care providers.

Other data elements contained in the CAD and utilized by Your Health System: Insight include those related to termination of pregnancy (TOP) data and medical assistance in dying (MAID) data. The technology available in Your Health System: Insight allows the masking of TOP and MAID data to occur in the analytical source of truth (ASOT) files while maintaining the analytical functionality, value and usability of the business intelligence tool upon which Your Health System: Insight was built. All geographic and facility-level information for TOP and MAID records is aggregated to the regional or provincial or territorial level but clinical data remains the same. For Ontario MAID records and British Columbia TOP records, CIHI masks the institution- or facility-identifiable data and the institution or facility and patient geography data, but not the clinical data. The result is that the MAID and TOP data is no longer associated with the institution or facility but rather is aggregated at the provincial or territorial level. The masking process was approved by the Sensitive Data Working Group via the internal document *Corporate Procedures for Handling Sensitive Data (Including Termination of Pregnancy and Medical Assistance in Dying Data)*.

The record-level data in Your Health System: Insight is used to build a particular indicator. The underlying data is not accessible to Your Health System: Insight users. Your Health System: Insight indicator results and contextual measures reported at the facility level (by name), provincial or territorial level and national level that are available to all users include, but are not limited to, rates (e.g., adjusted rate, crude rate) and numerator and denominator counts that may include small cell counts. As many as 15 or more different factors (e.g., age group, sex, triage levels, Case Mix Group, main patient services) can be explored.

Organization Index

CIHI's OI is a database developed and maintained by CIHI for the following purposes:

- To reconcile variability in organizational information such as organization names;
- To facilitate organizational linkage across data holdings;
- To track ongoing changes to organizations and their hierarchical relationships with each other; and
- To record changes to organizations over time.

Your Health System: Insight uses information from the OI as the basis for aggregating results to ensure the accuracy of reporting at multiple levels (hospital, regional, provincial or territorial, and national levels). For example, where there are multiple regional health authorities under a jurisdiction (e.g., province), the OI ensures that Your Health System: Insight data can be

- Rolled up to the level of the jurisdiction; or
- Rolled down to the level of
 - Any regional health authority under the jurisdiction; or
 - Any single corporation under the regional health authority; or
 - Any health care facility under a corporation it owns and operates.

Statistics Canada data

Geography Dimension and Postal Code Conversion File+

The Geography Dimension (GeoDIM) is a CIHI-derived data set created from Statistics Canada's Postal Code Conversion File and Postal Code Conversion File Plus (PCCF+) as well as from [Health Regions: Boundaries and Correspondence With Census Geography](#). The GeoDIM is used by CIHI eReporting products to assign geographic information based on patient (or facility) postal code.

GeoDIM will always assign the same geographic information to each postal code; however, the PCCF+ (a SAS program) uses population weights to allocate postal codes linked to multiple census geographies. Thus the PCCF+ will not always result in the same geographic information being assigned to a specific postal code, especially in rural areas where postal codes tend to cover large areas and cut across census geographies. In general, for assigning geographic information based on large geographic units (e.g., health region, province), either GeoDIM or the PCCF+ is suitable. However, for smaller geographic units (e.g., dissemination areas), the PCCF+ is considered the most comprehensive methodology.

Your Health System: Insight uses both GeoDIM and the PCCF+ in the following ways:

- GeoDIM is used to assign patient health region and province or territory to aggregate results at these 2 geographic levels; and
- The PCCF+ is used to assign patient income quintile to enable income analysis, and to assign Statistical Area Classification type to enable urban and rural/remote analysis.ⁱ
 - In the case of income quintile and urban and rural/remote assignment, these 2 variables are derived from smaller geographic units. Thus the PCCF+ was used rather than GeoDIM.

2.3 Access management and data flow for Your Health System: Insight

Your Health System: Insight is an interactive analytical tool that allows decision-support managers, analysts and clinicians to access the information they need to better understand, monitor and improve health care and Canada's health care systems.

Access to Your Health System: Insight is limited to data providers and approved non-data providers, as described in Section 2.1 above. For provincial or territorial organizations to access Your Health System: Insight, the support and/or approval of the ministry of health in the requesting organization's province or territory is required.

i. Income quintile results are used by the Health System Performance team to prepare results for Your Health System: In Brief and In Depth and Health Indicators e-Publication. Users cannot access this information through Your Health System: Insight.

For federal government departments or agencies or for pan-Canadian organizations not subject to provincial or territorial jurisdictional control to access Your Health System: Insight, the following criteria are considered:

- The requesting organization has responsibility for the planning and management of the health care system or has a decision-making role regarding health care system policy; and
- The requesting organization has expertise in managing record-level data, including appropriate privacy and security policies and processes.

In situations where either data providers or non–data providers want to access Quebec data, approval from the Ministère de la Santé et des Services sociaux du Québec must be obtained.

Both data providers and non–data providers are required to sign CIHI’s Electronic Reporting Services Agreement.

Access

All designated users can access indicator results, but only designated users of clients that are data providers can access patient record-level data supporting that data provider’s indicators.

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

For Your Health System: Insight, access is managed through 3 streams: general access, general access without Quebec data, and general and record-level access.

General access

This stream allows designated users to access aggregate indicator results containing health facility–identifiable information. It also allows them to view their indicator results in different ways, such as adjusted rate, crude rate, and numerator and denominator counts that may include small cell sizes.

General access without Quebec data

This stream has the same type of access role as general access but cannot access any Quebec data.

General and record-level access

This stream allows designated users to access aggregate indicator results containing health facility–identifiable information, to view their indicator results in different ways, and to obtain patient record-level data supporting their indicator.

All designated users may be granted permission for general access. Designated users of clients that are data providers may be granted permission for general access and/or access to record-level data. The decision on what level of access is to be granted is made by a client's organizational contact on the client's behalf.

Designated users log in to Your Health System: Insight through a secure web interface. Once logged in, users can

- Compare indicator results at, for example, the facility, regional, provincial or territorial, and national levels;
- Break down indicator results by relevant clinical and administrative data elements (e.g., admission category, triage level, sex, age);
- View their indicator results in different ways, such as adjusted rate or crude rate; and
- Save, print and export results.

Designated users of clients that are data providers can access their own patient record-level data and factors that may be driving their results.

Data flows

Selected records taken from existing CIHI databasesⁱⁱ (the DAD-HMDB and NACRS) are used by CIHI to create an ASOT file within CIHI's data warehouse to support the calculation of the indicator results. Once selected, records are linked to create episodes of care for each patient (see the figure below). Indicator methodologiesⁱⁱⁱ are then applied and hierarchical information from the OI is used (see Section 2.2) to calculate the indicator results at the facility, regional, provincial or territorial, and national levels.

Your Health System: Insight undertakes an independent double-verification and sign-off process ("block approval") to ensure the record-level CAD data-loading activities and indicator calculations occur consistently and correctly. Staff are required to follow the established data-loading activities, as approved by the director of Client Experience. If there is a change (e.g., new indicator, updated methodology), then the director of Client Experience must sign off on a new block approval. A similar verification and sign-off process is required to ensure

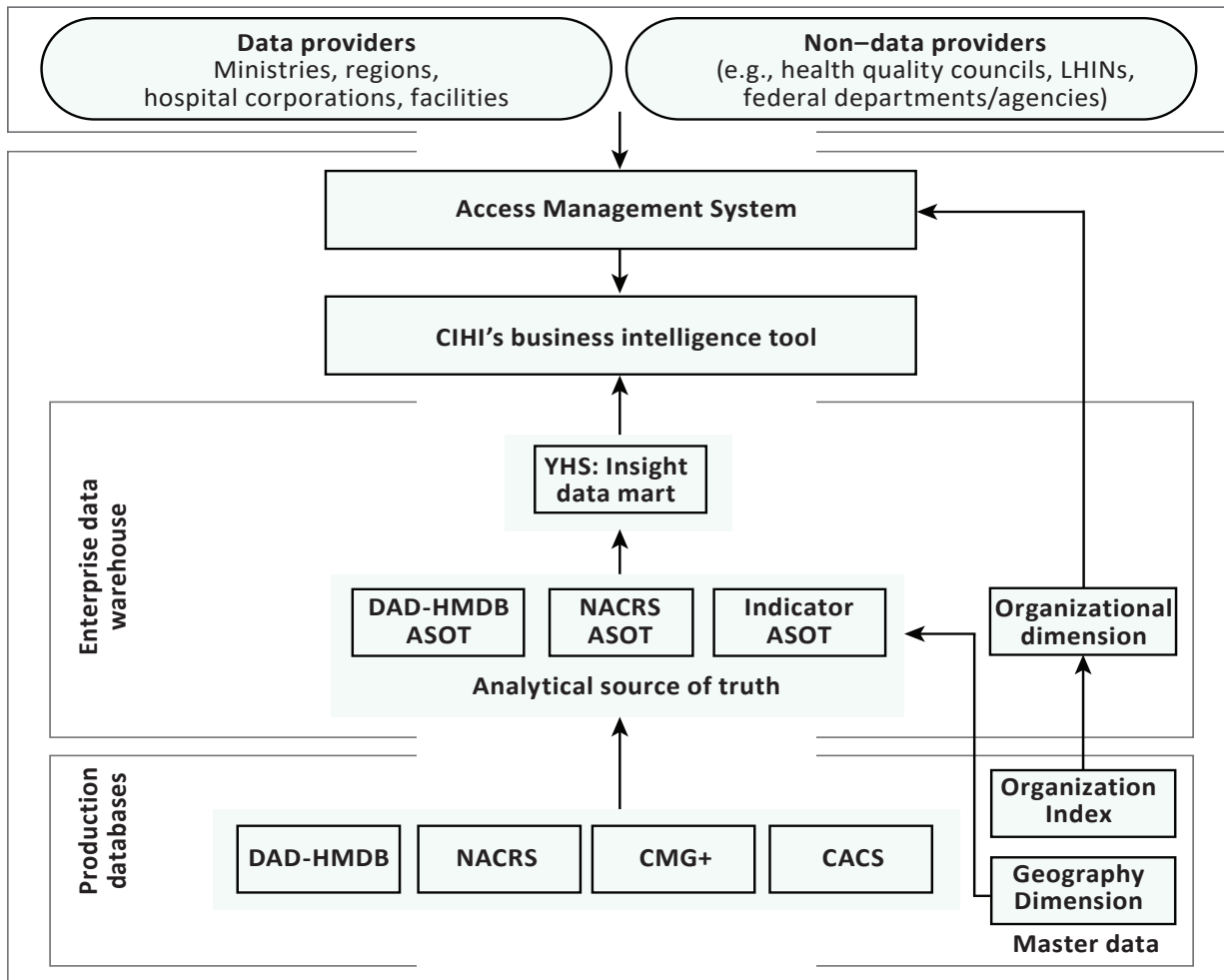
- Established protocols for handling sensitive data, including TOP and MAID information, were followed; and
- Data is linked to the correct organization.

ii. Other existing CIHI data sources used in calculating indicators include the following:

- Case Mix Group+: This is a CIHI inpatient grouping methodology designed to group patient data originating from the DAD.
- Comprehensive Ambulatory Classification System: This is a CIHI ambulatory grouping methodology designed to group ambulatory data (e.g., emergency department, day surgery and outpatient clinics originating from NACRS) and day surgery visit data from the DAD.

iii. The responsibility for developing indicators rests with the relevant CIHI program area.

Figure Overview of the data flow for Your Health System: Insight



Notes

- LHIN: Local health integration network.
- YHS: Your Health System.
- DAD-HMDB: Discharge Abstract Database–Hospital Morbidity Database.
- NACRS: National Ambulatory Care Reporting System.
- ASOT: Analytical source of truth.
- CMG+: Case Mix Group+.
- CACS: Comprehensive Ambulatory Classification System.

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 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.

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

3.2 Authorities governing Your Health System: Insight 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

As indicated above in Section 2.2, Your Health System: Insight contains data sourced from subsets of existing CIHI data holdings. This data flows directly into CIHI via existing applications and/or systems from, for example, data providers, hospitals and other health care facilities. These existing data flows are governed by CIHI’s [Privacy Policy, 2010](#), legislation in the jurisdictions and 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.

CIHI’s Electronic Reporting Services Agreement

To be able to use Your Health System: Insight, clients must sign CIHI’s Electronic Reporting Services Agreement. The agreement outlines obligations around access to Your Health System: Insight data, as well as security issues, use of the web tool and disclosure. It is signed at a senior level in the organization to ensure that clients are aware of their organizational responsibilities and the responsibilities of their designated users. Compliance with the terms and conditions of the agreement is mandatory. Failure to uphold the terms and conditions could result in termination of access to Your Health System: Insight data.

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 Your Health System: Insight data in terms of privacy and security risk management:

Table 2 Key positions and responsibilities

Position/group	Roles/responsibilities
Vice president, Communications and Client Experience	Responsible for the overall strategic direction of CIHI’s digital products, including Your Health System: Insight
Director, Client Experience	Responsible for strategic recommendations and decisions about the direction of CIHI’s digital products, including Your Health System: Insight
Chief information security officer	Responsible for the strategic direction and overall implementation of CIHI’s Information Security Program
Executive director, chief privacy officer and general counsel	Responsible for the strategic direction and overall implementation of CIHI’s Privacy Program
Manager, Product Management and Client Experience	Responsible for ongoing management, development and deployment of CIHI’s digital products
Manager, Information Integration and Intelligence Products	Responsible for ensuring technical requirements for the ongoing development, deployment and maintenance of CIHI’s digital products, as well as system administration

3.4 Principle 2: Identifying purposes for personal health information

Your Health System: Insight is a service provided by CIHI to meet the needs of its clients for online access to timely pan-Canadian health care data in a secure environment that safeguards privacy and confidentiality. The purpose of Your Health System: Insight is to support ongoing health system management as well as quality improvement initiatives at the hospital and regional levels.

CIHI's Electronic Reporting Services Agreement limits the rights of clients to access and use Your Health System: Insight data solely for non-commercial purposes limited to the client's internal management, data quality, planning, research, analysis or evidence-based decision-support activities.

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. Under sections 1 and 2 of CIHI's [Privacy Policy, 2010](#), CIHI collects from data providers only the information that is reasonably required for health system uses, including statistical analysis and reporting, in support of the management, evaluation or monitoring of the health care system. The purpose of Your Health System: Insight is described in Section 3.4.

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

Limiting use

Clients

CIHI limits the use of Your Health System: Insight data to authorized purposes, as described above in sections 2.1 and 3.4. These include comparative analyses within and among jurisdictions; trend analyses to assess and monitor the impact of differences in policy, practices and service delivery; and 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.

Data linkage

Data linkages are performed within Your Health System: Insight to create episodes of care during the development of indicators. Individual patients with multiple admissions are identified in order to follow them from one facility to another to support reporting and the analyses of health system indicators and measures such as readmissions. There are 5 indicators that are calculated based on where the hospital is located, and 5 indicators calculated based on where the patient lives. Linkage is an automated process performed by the system. Designated users are unable to access the record-level data involved in the linkages or perform linkages on their own.

The CAD received approval from CIHI's Privacy, Confidentiality and Security Committee to link data across its holdings (i.e., DAD and NACRS) for its own purposes, excluding Quebec data. This approval is applied to DAD and NACRS data that is linked in Your Health System: Insight using CIHI's client linkage standard (see below). The inclusion of Quebec data requires the approval of the Ministère de la Santé et des Services sociaux du Québec.

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 when linking records created in 2010–2011 or later, where the records include the encrypted health care number and the province or 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.

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 *Information Destruction Standard*. These requirements apply to data linkages both for CIHI's own purposes and for third-party data requests.

Return of own data

A key feature of Your Health System: Insight is the automated return of record-level information to allow data providers to reconcile their indicator results with their own locally held data, and to use the data to identify underlying factors that may be driving their results. The return of own data is considered a use and not a disclosure.

Limiting disclosure

Before being provided with access to Your Health System: Insight, users must sign CIHI's Electronic Reporting Services 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 where all reasonable measures are employed to prevent the identification of individuals, and 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.

Limiting retention

Your Health System: Insight 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.

Your Health System: Insight's data is sourced from the CAD and relies on its data quality activities to ensure the accuracy of the data. In addition, the following activities are in place to ensure the data quality of results generated by Your Health System: Insight.

The process for ensuring the accuracy of indicator calculations occurs over multiple phases. This ranges from the time that indicators are developed by the relevant CIHI program area through to the loading of indicators in the data warehouse, where quality assurance and user acceptance testing are performed when indicators are first introduced in Your Health System: Insight. Once tested, the calculations are automated to minimize human error.

Cautionary notes: Use and interpretation

Indicator results and measures reported in Your Health System: Insight include rates (e.g., adjusted rate, crude rate) and numerator and denominator counts that may include small cell cases. In compliance with Section 6.3(b) of the Electronic Reporting Services Agreement, clients who want to publish indicators or rates are obligated to

- Use caution when the number of cases in the denominator is low due to the instability of rates and avoid reporting the indicator or rate publicly; and
- Include the statement “interpret with caution” when the number of cases in the denominator is less than 50.

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 Your Health System: Insight 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 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

The October 2015 Your Health System: Insight PIA identified 5 privacy risks related to inappropriate access to record-level data. All 5 risks were resolved through CIHI's privacy and security risk assessment process.

This CIHI assessment of Your Health System: Insight did not identify any new privacy or security risks.

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

Appendices

Appendix A: Indicators

- 30-Day Acute Myocardial Infarction In-Hospital Mortality
- Emergency Department Wait Times (4 indicators)
- Hip Fracture Surgery Within 48 Hours
- Hospital Harm
- Hospital Standardized Mortality Ratio
- In-Hospital Mortality Following Major Surgery
- In-Hospital Sepsis
- Obstetric Trauma (2 indicators: Vaginal Delivery With Instrument and Vaginal Delivery Without Instrument)
- Readmissions (5 indicators calculated based on where the hospital is and 5 indicators calculated based on where the patient lives)
- 30-Day Stroke In-Hospital Mortality

Appendix B: Text alternative for figure

Data flow for Your Health System: Insight

This figure illustrates the flow of data in to and out of Your Health System: Insight.

Health indicator results in Your Health System: Insight are calculated based on a subset of records taken from CIHI's existing databases (e.g., the DAD-HMDB, NACRS). This subset is used by CIHI to create an ASOT file within CIHI's data warehouse to support the calculation of indicator results.

The data contained in the ASOT file is used to calculate indicator results by

- Linking selected records to create episodes of care for each patient;
- Applying indicator methodologies; and
- Leveraging hierarchical information from the Organization Index to calculate the indicator results at the facility, regional, provincial or territorial, and national levels.

The resulting processed ASOT data is loaded to the Your Health System: Insight data mart, the business intelligence tool upon which Your Health System: Insight is built.

Designated users of clients include data providers (ministries, regions, hospital corporations, facilities) and non-data providers (e.g., health quality councils, LHINs, federal departments/agencies). Through CIHI's Access Management System, all designated users of clients are authenticated by CIHI and receive general authorization to access aggregate Your Health System: Insight indicator results containing health facility-identifiable information and to view their client organization's indicator results. Clients may request designated users be granted additional permissions to view the organization's indicator results in different ways and to access the patient record-level data supporting each indicator.

Notes

LHIN: Local health integration network.

YHS: Your Health System.

DAD-HMDB: Discharge Abstract Database-Hospital Morbidity Database.

NACRS: National Ambulatory Care Reporting System.

ASOT: Analytical source of truth.

CMG+: Case Mix Group+.

CACS: Comprehensive Ambulatory Classification System.

**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

25857-0122

