CIHI Portal Privacy Impact Assessment

October 2020

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.

Canadian Institute for Health Information
495 Richmond Road, Suite 600
Ottawa, Ontario K2A 4H6
Phone: 613-241-7860
Fax: 613-241-8120
cihi.ca
copyright@cihi.ca

How to cite this document:
Canadian Institute for Health Information. *CIHI Portal Privacy Impact Assessment, October 2020*. Ottawa, ON: CIHI; 2021.

Cette publication est aussi disponible en français sous le titre *Évaluation des incidences sur la vie privée du Portail de l'ICIS, octobre 2020*.

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

- *CIHI Portal, October 2020*

Approved by

Brent Diverty
Vice President, Data Strategies and Statistics

Rhonda Wing
Chief Privacy Officer and General Counsel

Ottawa, October 2020

Table of contents

Quick facts about CIHI Portal

1. CIHI Portal is a secure means of accessing selected data already held at the Canadian Institute for Health Information (CIHI) in the clinical administrative databases (CAD),[i] the National Rehabilitation Reporting System (NRS) and the Canadian MIS Database (CMDB). It also contains publicly available files from Statistics Canada.
2. The data from existing data holdings (i.e., CAD, NRS, CMDB) is reported on separately in CIHI Portal. All privacy-sensitive patient data — such as health care numbers, chart numbers, registration numbers, full dates of birth, full postal codes and provider numbers — has been removed or truncated.
3. The tool allows clients to create reports on clinical administration, resourcing, service provision, cost-efficiencies and population demographics.
4. CIHI Portal serves as a focal point for collaborating and establishing communities of practice, and offers clients the ability to
   - Share and view pre-built reports, query the data based on their own requirements, and map and build customized reports for evaluation purposes to support decision-making and to facilitate knowledge transfer; and
   - Support regular performance measurement and the determination of best practices by allowing clients to compare their organizations with customized peer groups at local, regional, provincial and national levels.
5. Clients may be hospitals, regional health authorities, ministries of health or other health care–related public bodies.
6. To use CIHI Portal, clients must sign CIHI's Electronic Reporting Services Agreement. The Services Agreement limits clients' rights to use and disclose de-identified data and facility-identifiable information obtained through CIHI Portal. Specifically, clients and their designated users are permitted to use such data solely for non-commercial purposes limited to their internal management, data quality, planning, research, analysis or evidence-based decision-support activities.
7. CIHI Portal does not allow direct access to individual records. Queries to create reports may return rows with individual record counts, but designated users cannot see or request the extraction of individual records.
8. One of the unique features of CIHI Portal is the patient dimension functionality that allows clients to identify trends in patient readmissions across time and geography. This functionality is a result of data linkages that occur within the DAD and within NACRS only.

i. The CAD are the Discharge Abstract Database (DAD) and the National Ambulatory Care Reporting System (NACRS).

Definitions

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

Services Agreement means CIHI's Secure Electronic Reporting Services Agreement.

Client means the organization specified in the Services Agreement that agrees to be bound by the terms of the Services Agreement for access to CIHI Portal.

Designated user means a client employee or permitted contractor who has been authorized by the client to access and use CIHI Portal.

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

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

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 CIHI Portal. This PIA, which replaces the May 2014 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* and how the principles apply to CIHI Portal, as well as a look at the application of CIHI's *Privacy and Security Risk Management Framework*.

The primary driver for this PIA is compliance with CIHI's Privacy Impact Assessment Policy.

2 Background

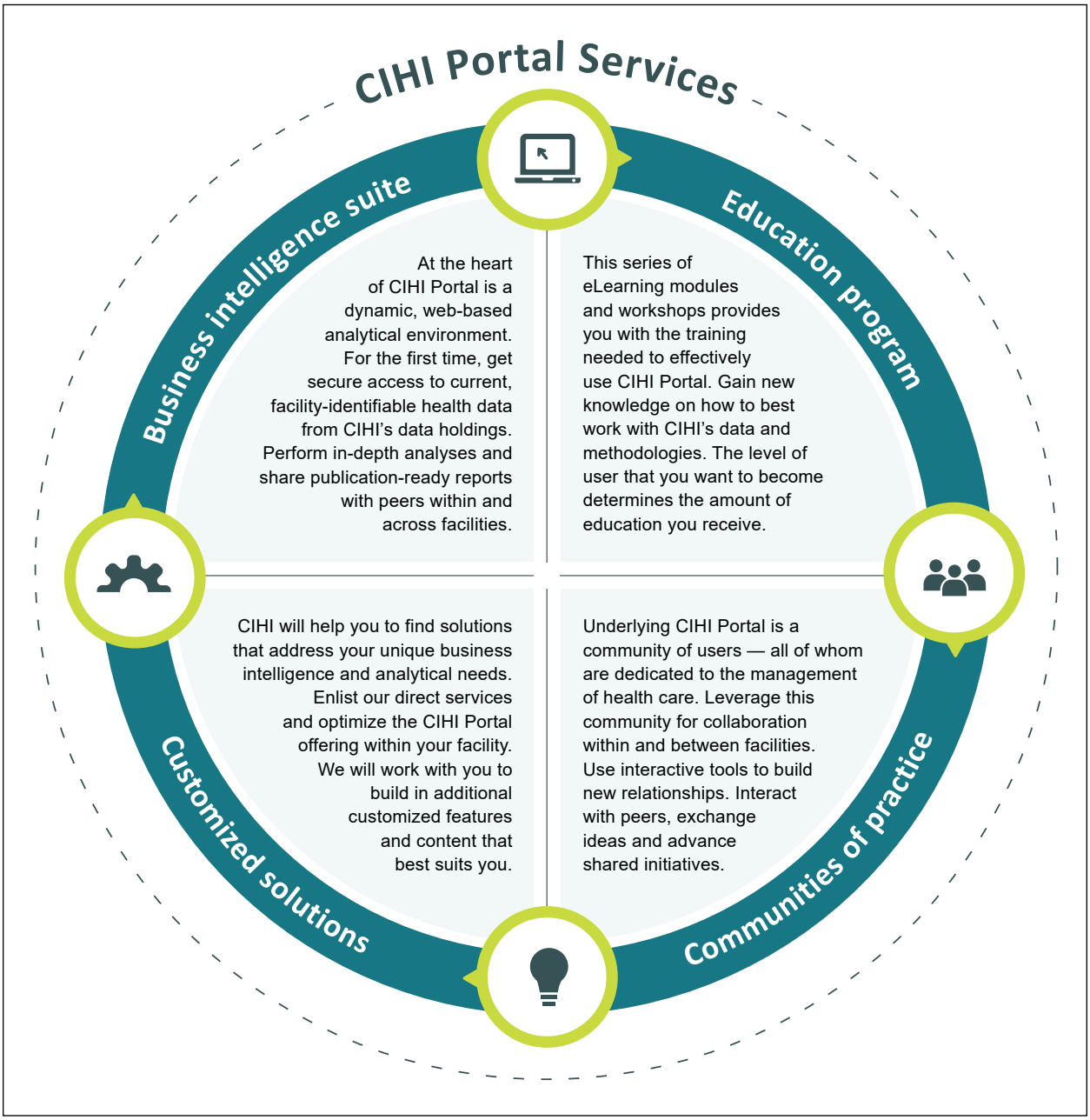
2.1 Introduction to CIHI Portal

CIHI Portal is an analytical web-based tool for health care data, designed by CIHI to meet the needs of its clients, who are for the most part also its data providers.

The tool's intended purpose is to assist health care service organizations such as hospitals, regional health authorities and ministries of health by providing them with online access to pan-Canadian health care data in a secure environment that safeguards privacy and confidentiality for monitoring, planning for and making decisions about the delivery of health care services. The CIHI Portal team provides a comprehensive training program, support for building communities of practice and customized reporting solutions, and ongoing client support.

CIHI Portal offers clients the ability to share and view pre-built reports, query the data based on their own requirements, and map and build customized reports for purposes of evaluation to support decision-making and to facilitate knowledge transfer. CIHI Portal supports regular performance measurement and the determination of best practices by allowing clients to compare their organizations with customized peer groups at local, regional, provincial and national levels. Clients can carry out internal research and planning on clinical administration, resourcing, service provision, cost-efficiencies and population demographics. CIHI Portal serves as a focal point for collaborating and establishing communities of practice. Through CIHI Portal, Clients are able to share reports, methodologies and findings with peers within and across organizations. Together, they can create internal and external networks of collaboration. This unique bundle of features allows users from various levels of health care management across the country to answer questions that are specific to their needs.

Figure 1 CIHI Portal's services



CIHI Portal serves 2 types of clients:

1. **Submitters:** Data providers, such as individual health care facilities, regional health authorities, selected communities of practice and participating provincial and territorial ministries/departments of health
2. **Non-submitters:** Provincial/territorial: With the support/approval of the ministry of health in the requesting organization's province/territory

   Federal: For federal government departments/agencies or for pan-Canadian organizations not subject to provincial/territorial control, the following criteria are to be considered:

   - The requesting organization has responsibility for planning and management of health care systems or has a decision-making role regarding health care system policy (see sections 37(a) and (b) of the *Privacy Policy, 2010*); and
   - The requesting organization has expertise in managing record-level data, including appropriate privacy and security policies and processes.

Requests for access to CIHI Portal are submitted to CIHI's vice president of Communications and Client Experience for approval. CIHI's Executive Committee is then informed of all non-submitter approvals.

2.2 Data sources

CIHI Portal contains data from 2 sources: subsets of existing CIHI data holdings and publicly available files from Statistics Canada. The existing CIHI holdings are the clinical administrative databases (CAD), the National Rehabilitation Reporting System (NRS) and the Canadian MIS Database (CMDB) (see below for more information about these data holdings).

The data from these existing data holdings is reported separately in CIHI Portal. All privacy-sensitive patient data — such as health care numbers, chart numbers, registration numbers, full dates of birth, full postal codes and provider numbers — has been removed from or truncated in the data mart. The masking of privacy-sensitive patient data involving abortion and medical assistance in dying is addressed by CIHI's Sensitive Data Working Group, a sub-committee of the Privacy, Confidentiality and Security Committee.

Currently, CIHI Portal maintains 5 to 10 of the most recent years of the selected data, depending on the holding.

CIHI data

Clinical administrative databases

The CAD are 2 separate pan-Canadian databases: the Discharge Abstract Database–Hospital Morbidity Database (DAD-HMDB) and the National Ambulatory Care Reporting System (NACRS). These administrative databases contain information about patients, providers and health facilities. For example, they contain personal, geographic and demographic attributes about patients, and clinical, diagnostic, intervention and other care delivery aspects and administrative information about individual patients resulting from hospital inpatient acute separations, emergency department separations or outpatient (ambulatory care) separations (e.g., clinic, day surgery). Examples of information contained in the CAD about health care providers include their service type (e.g., cardiology) and role in the care of the patient (e.g., most responsible physician, consultant). Examples of health facility–identifiable information (i.e., information that directly identifies a health facility by name) include facilities where patients received care, including information about facilities where patients were transferred from and/or transferred to. In addition, the CAD include value-added derived variables, such as Case Mix Groups.

The CAD also collect information in special project fields, which are used by data providers to capture supplemental information in the form of alpha and/or numeric values not routinely captured.

For more information, read the CAD PIA.

National Rehabilitation Reporting System

The NRS collects information about the extent of improvement in patients' physical and cognitive functioning during inpatient rehabilitation, along with a range of supporting information, such as when a patient's rehabilitation services begin and end, estimates of the resources consumed in providing rehabilitation services and patients' socio-demographic characteristics that are relevant to rehabilitation. It contains data on inpatients who receive rehabilitation services for a range of conditions, including orthopedic trauma or surgery, stroke and spinal cord dysfunction.

For more information, read the NRS PIA.

Canadian MIS Database

The CMDB collects data and reports on the day-to-day operations of health service organizations through financial and statistical information on hospitals and regional health authorities across Canada. The data is collected according to a standardized framework. The CMDB does not include patient-identifiable information. It does contain information on the salaries of employees, summarized to the national functional centre level, at health care organizations that submit data; no identifying information, such as name or employee number, is included.

For more information, read the CMDB PIA.

Master data (supporting data)

Master data includes CIHI's Organization Index (OI), as well as aggregated, non-confidential population and geography dimension (GeoDIM) data sourced from Statistics Canada.

Organization Index

CIHI developed and maintains the OI

- To reconcile variability in organization 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.

CIHI Portal uses information from the OI as the basis for aggregating results to ensure accuracy of reporting at multiple levels (hospital, regional, provincial/territorial and national). For example, when there are multiple regional health authorities under a province, the OI ensures that data can be

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

Population

The population estimates are CIHI-derived data sets created from Statistics Canada's population files, based on census and latest boundary files. The population estimates are used by CIHI to calculate population-based indicators, and can be used to calculate age- and sex-standardized rates and other statistics.

Geography dimension

The GeoDIM is a CIHI-derived data set created from Statistics Canada's Postal Code Conversion File (PCCF) and Health regions: boundaries and correspondence with census geography. The GeoDIM is used by CIHI's eReporting products to assign geographic information based on patient (or facility) postal code.

Statistics Canada: Postal Code Conversion File

Income (quintile and decile)

National and area income information is sourced from Statistics Canada's PCCF based on census data.

The data elements available in CIHI Portal identify the quintile and decile membership of the patient at the level of the dissemination area. Specifically, CIHI has introduced 4 income data elements to CIHI Portal:

- **National Income Quintiles:** The national income per person equivalent (IPPE) split into 5 equal categories, where the IPPE is a household size–adjusted measure of income based on the most recent census summary data.
- **National Income Deciles:** The national IPPE split into 10 equal categories, where the IPPE is a household size–adjusted measure of income based on the most recent census summary data.
- **Area Income Quintiles:** The area-based (neighbourhood income quintile) IPPE split into 5 equal categories, where the IPPE is a household size–adjusted measure of income based on the most recent census summary data.
- **Area Income Deciles:** The area-based (neighbourhood income decile) IPPE split into 10 equal categories, where the IPPE is a household size–adjusted measure of income based on the most recent census summary data.

Introducing national and area income quintiles and deciles allows ad hoc analyses related to socio-economic status on patient populations to be performed.

2.3 Access management and flow for CIHI Portal

CIHI Portal serves 2 types of clients: data providers that submit data to CIHI (**submitters**) and **non-submitters**. Non-submitting organizations that want to use CIHI Portal must meet criteria specified by CIHI. As part of the access management process, both types of clients are required to sign CIHI's Services Agreement and the CIHI Portal Schedule that is specific to each type of client (see Section 3.2 for more details).

Access to CIHI's secure applications is subject to CIHI's role-based access management process. CIHI manages access to its secure applications using established access management system processes for granting and revoking access.

There are 3 types of access requests (new, existing and revoke) and 2 types of designated users (analysts and information consumers):

Types of requests

New client access

Organizations that have not entered into an agreement with CIHI to use CIHI Portal must complete and sign the Services Agreement and the CIHI Portal Schedule. The process of becoming a new client includes identifying an organizational contact (OC) (i.e., the individual designated by the client to operationalize the terms and conditions of the Services Agreement), who is responsible for identifying designated users and their access role (see below). Once these documents are signed and returned, CIHI will grant the appropriate access and send notifications to the new designated users.

Existing organization access requests

To add a designated user from an organization that is already a client, a formal request from the established OC is required. CIHI will amend the CIHI Portal Schedule and send it to the OC to confirm the access request. Once the revised schedule is signed, CIHI will grant the appropriate access, notify the OC and send a notification to the new designated user.

Revoking access

To revoke access to CIHI Portal, a formal request from the OC is required. CIHI will contact the OC to confirm the request to revoke access and ensure the CIHI Portal Schedule is revised and signed. Once signed, CIHI will revoke access and send a notification to the OC.

Note that signing a revised CIHI Portal Schedule is required for analysts only, not for information consumers.

Designated user access role

Analyst

Analysts have maximum access and the most flexibility to work with the data available through CIHI Portal (e.g., creating reports, calculating new metrics from existing data).

Information consumer

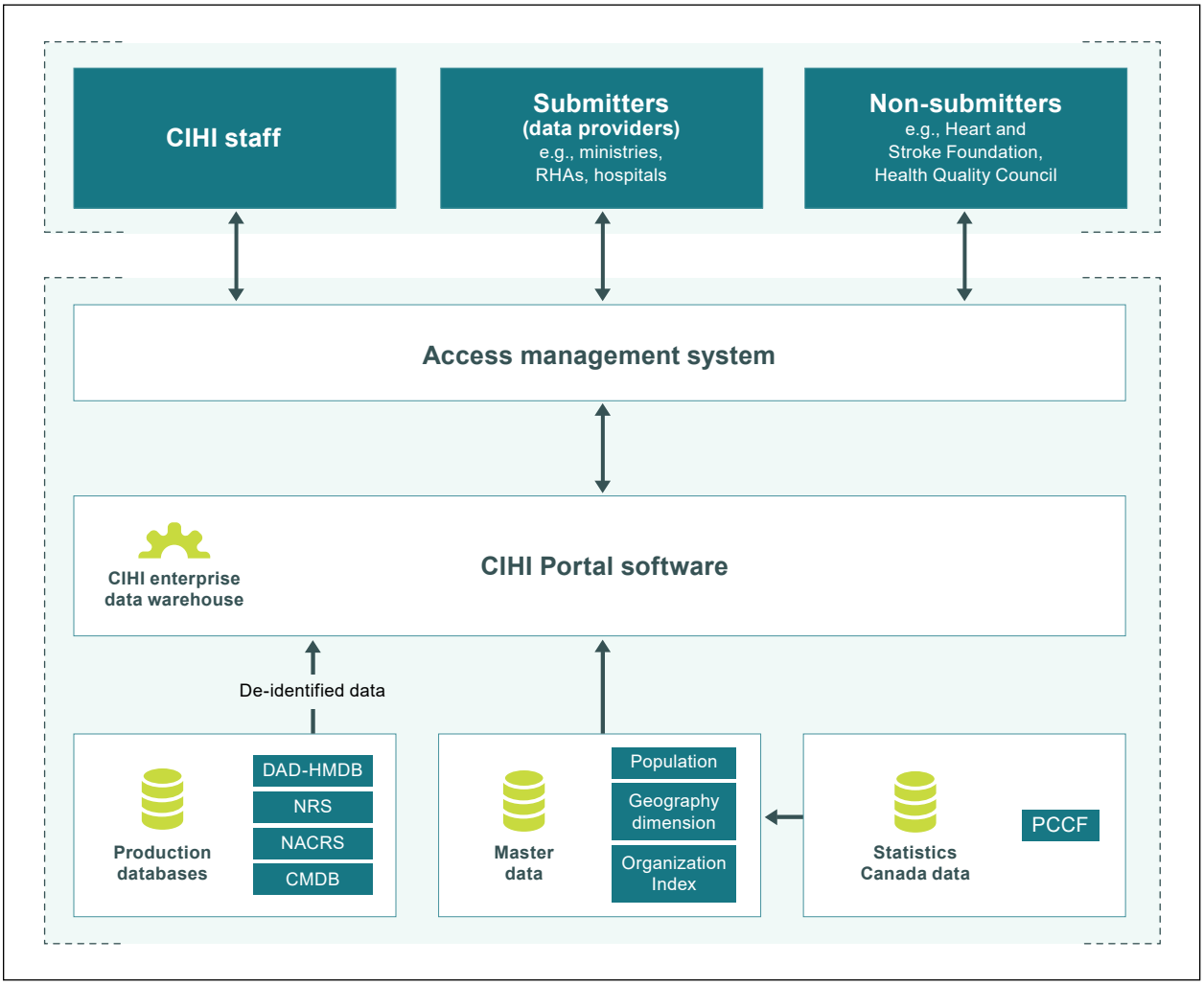
Information consumers can view, save and manipulate any existing reports. Designated users with this access role cannot create any new reports, and data access is limited to the content of the existing reports. The outputs from these queries may be shared within CIHI Portal or exported in aggregate form to other aggregate file formats (such as MS Excel). The underlying de-identified record-level data is not exportable.

CIHI staff access

Staff access to CIHI Portal is provided through CIHI's centralized SAS Data Access process. The process ensures that all requests for access, including access to CIHI Portal data, are traceable and authorized. The SAS Data Access system is subject to an annual audit to ensure that staff are accessing data on a need-to-know basis. Section 3.9 includes additional information about how the various procedural and technical measures are deployed to prevent unauthorized access and otherwise secure CIHI Portal data.

The following figure provides an overview of CIHI Portal's data flow.

Figure 2 CIHI Portal data flow



Notes
RHAs: Regional health authorities.
DAD-HMDB: Discharge Abstract Database–Hospital Morbidity Database.
NACRS: National Ambulatory Care Reporting System.
NRS: National Rehabilitation Reporting System.
CMDB: Canadian MIS Database.
PCCF: Postal Code Conversion File.

3 Privacy analysis

3.1 Privacy and Security Risk Management Program

Privacy and security risk management is a formal, repeatable process for identifying, assessing, treating and monitoring risks in order to minimize the probability of such risks materializing and/or their impact should they occur. 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. 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 score 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.

3.2 Authorities governing CIHI Portal 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 health systems, including statistical analysis and reporting. Data providers are responsible for meeting the statutory requirements in their respective jurisdictions, where applicable, at the time the data is collected.

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

CIHI Portal 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.

CIHI's Secure Electronic Reporting Services Agreement

Clients (submitters and non-submitters) are required to sign CIHI's Services Agreement. The Services Agreement limits clients' rights to use and disclose de-identified data and facility-identifiable information obtained through CIHI Portal. Specifically, clients and their designated users are permitted to use such data solely for non-commercial purposes limited to the client's internal management, data quality, planning, research, analysis or evidence-based decision-support activities. CIHI Portal data cannot be disclosed to any third party, except in the case of the client's own data. Publication or disclosure outside of the client organization is permitted only where all reasonable measures are employed to prevent the identification of individuals and data does not contain cell sizes with fewer than 5 observations. Health facility–identifiable information cannot be released unless the client has notified CIHI prior to the disclosure, to permit CIHI to notify the applicable ministry.

Clients assume responsibility for ensuring that designated users of CIHI Portal in their organizations are aware of and comply with the terms and conditions of the Services Agreement, such as

- Keeping de-identified data obtained through CIHI Portal, including any reports, in confidence, using the same degree of care that they use to protect their own confidential information, but no less than reasonable care, to prevent any theft, loss of, unauthorized access to or use, disclosure, copying, modification or disposal of the data, except as expressly provided for in the Services Agreement or as required by law; and
- Where possible, accessing CIHI Portal from the client's network only or the client facility's network; otherwise, the client shall ensure that access over the internet is done within a secure environment.

Clients agree to immediately notify CIHI of any unauthorized use of any designated user's means of access or any other breach of confidentiality or security of which they become aware.

In addition, the Services Agreement sets out the following specific requirements and responsibilities with respect to access management:

- Clients are to ensure at all times that CIHI has accurate and current registration data for all designated users.
- Clients and their designated users are responsible for maintaining the confidentiality of the means of access (e.g., usernames and passwords are kept strictly confidential). The means of access may not be shared with or disclosed to any person or entity for any reason, is not transferable and cannot be assigned to an un-named individual or occupational position.

- Clients are fully responsible for all activities that occur under their designated users' means of access.
- Clients and their designated users must not permit any third party or unauthorized user to access CIHI Portal.

CIHI has put in place a mandatory training program for designated users of CIHI Portal that addresses each of these items.

As a reminder for the designated users, they must accept the Terms and Conditions of Use, a summary of access and use–related provisions, each time they log in to CIHI Portal prior to accessing any 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.

Clients are accountable for ensuring compliance with the Services Agreement within their respective organizations. They are also subject to the requirements of data protection laws in their respective jurisdictions and the independent oversight of privacy commissioners or their equivalents.

Organization and governance

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

Table 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 CIHI Portal
Director, Digital Innovation	Responsible for strategic recommendations and decisions about the direction of CIHI's digital products (including Portal) and information management initiatives
Director, Strategy, Architecture and Standards	Responsible for strategic recommendations and decisions on key information technology to help ensure alignment and/or integration of key initiatives with overall CIHI corporate priorities and plans
Chief information security officer	Responsible for the strategic direction and overall implementation of CIHI's Information Security Program
Chief privacy officer	Responsible for the strategic direction and overall implementation of CIHI's Privacy Program
Manager, Digital Content and Channel Management	Responsible for managing day-to-day operations for CIHI's digital products (including CIHI Portal)
Manager, Information Integration and Intelligence Products	Responsible for ensuring that technical requirements are met for the ongoing development, deployment and maintenance of CIHI's digital products and system administration

3.4 Principle 2: Identifying purposes for personal health information

CIHI Portal is a service provided by CIHI to meet the needs of its clients for online access to de-identified pan-Canadian CAD, NRS and CMDB data. The Services Agreement limits clients' rights to use and disclose de-identified health information and facility-identifiable information obtained through CIHI Portal. Specifically, clients and their designated users are permitted to use such data solely for non-commercial purposes limited to internal management, data quality, planning, research, analysis or evidence-based decision-support activities. The intended purposes and scope of CIHI Portal are clearly identified in this PIA and on the CIHI Portal page of CIHI's website.

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 health care systems.

CIHI Portal is a secure means of accessing selected data already held at CIHI in the CAD, NRS and CMDB.

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

Limiting use

Clients

CIHI limits the use of CIHI Portal data by clients to authorized purposes, as described in Section 2.1. 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

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. Permissions are granted following completion of CIHI Portal's eLearning courses — one for each existing CIHI data holding that supplies CIHI Portal. CIHI staff who use CIHI Portal remain bound by the confidentiality agreement that all CIHI staff are required to sign at the commencement of employment, and they are subsequently required to renew their commitment to privacy yearly.

CIHI Portal data used for internal CIHI analysis purposes does not contain names or direct identifiers, such as unencrypted health care numbers, full dates of birth and full postal codes. These identifiers are removed from records of existing CIHI data holdings before being moved to CIHI Portal (see Section 2.2).

Data linkage

Data linkages are performed at CIHI. While this potentially causes greater risk of identification of an individual, CIHI undertakes mitigating steps to reduce the risks (e.g., de-identification by removing patient identifiers and assigning meaningless transaction numbers.)

Data linkage that CIHI Portal performs is an automated process designed to support the patient dimension feature (readmission, previous admissions, revisits, previous visits) that allows designated users to analyze multiple admissions/visits (i.e., subsequent or previous admissions of patients in a cohort for the same or other facilities). These linkages occur in the background without client intervention, meaning that designated users cannot access the 4 variables (encrypted health card number, health card number province, date of birth and gender) used by CIHI Portal to perform linkages. Data linkages can only be performed *within* the DAD and NACRS data holdings, not *across* them.

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.

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

Limiting disclosure

As described in Section 3.2, before being provided with access to CIHI Portal, clients must sign a Services Agreement that imposes confidentiality and security restrictions and obligations. CIHI Portal data cannot be disclosed to any third party, except in the case of the client's own data.

Clients are also subject to the requirements of data protection laws in their respective jurisdictions.

Limiting retention

CIHI Portal 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, CIHI Portal 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 CIHI Portal 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 CIHI Portal 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).

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 CIHI Portal 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 alternatives for figures

Figure 1: CIHI Portal's services

Business intelligence suite

At the heart of CIHI Portal is a dynamic, web-based analytical environment. For the first time, get secure access to current, facility-identifiable health data from CIHI's data holdings. Perform in-depth analyses and share publication-ready reports with peers within and across facilities.

Education program

This series of eLearning modules and in-class workshops provides you with the training needed to effectively use CIHI Portal. Gain new knowledge on how to best work with CIHI's data and methodologies. The level of user that you want to become determines the amount of education you receive.

Customized solutions

CIHI will help you to find solutions that address your unique business intelligence and analytical needs. Enlist our direct services and optimize the CIHI Portal offering within your facility. We will work with you to build in additional customized features and content that best suits you.

Communities of practice

Underlying CIHI Portal is a community of users — all of whom are dedicated to the management of health care. Leverage this community for collaboration within and between facilities. Use interactive tools to build new relationships. Interact with peers, exchange ideas and advance shared initiatives.

Figure 2: CIHI Portal data flow

CIHI Portal contains data from subsets of existing CIHI production databases (Discharge Abstract Database–Hospital Morbidity Database, National Ambulatory Care Reporting System, National Rehabilitation Reporting System, Canadian MIS Database), master data (Organization Index, population and geography dimension) and Statistics Canada's Postal Code Conversion File.

De-identified data from CIHI's databases, the master data and data from the Postal Code Conversion file flows into CIHI Portal, which is part of the CIHI data enterprise warehouse.

Authorized CIHI Portal users — CIHI staff, submitters (also known as data providers, such as ministries, regional health authorities and hospitals) and non-submitters (such as the Heart and Stroke Foundation and Health Quality Council) — are authenticated using CIHI's access management system. Users have the ability to access CIHI Portal to share and view pre-built reports, query the data based on their own requirements, and map and build customized reports for purposes of evaluation to support decision-making and to facilitate knowledge transfer.

help@cihi.ca

CIHI Ottawa
495 Richmond Road
Suite 600
Ottawa, Ont.
K2A 4H6
613-241-7860

CIHI Toronto
4110 Yonge Street
Suite 300
Toronto, Ont.
M2P 2B7
416-481-2002

CIHI Victoria
880 Douglas Street
Suite 600
Victoria, B.C.
V8W 2B7
250-220-4100

CIHI Montréal
1010 Sherbrooke Street West
Suite 602
Montréal, Que.
H3A 2R7
514-842-2226

cihi.ca

23607-0121