CIHI Portal—Privacy Impact Assessment

CIHI
ICIS
Canadian Institute
for Health Information
Institut canadien
d’information sur la santé

Our Vision

Better data. Better decisions.
Healthier Canadians.

Our Mandate

To lead the development and maintenance of comprehensive and integrated health information that enables sound policy and effective health system management that improve health and health care.

Our Values

Respect, Integrity, Collaboration, Excellence, Innovation

CIHI is pleased to publish the following Privacy Impact Assessment pursuant to its Privacy Impact Assessment Policy:

CIHI Portal
Privacy Impact Assessment

Approved by:

Stephen O'Reilly
Executive Director,
Atlantic Canada & Integrated eReporting

Anne-Mari Phillips
Chief Privacy Officer & General Counsel

Ottawa – May 2014

Table of Contents

10 Quick Facts About CIHI Portal

1. CIHI Portal is an analytical web-based tool for health care data. CIHI designed it to provide clients with secure online access to de-identified pan-Canadian health care data already held at CIHI.
2. CIHI Portal does not allow direct access to individual records. Queries to create reports may return rows with individual record counts, but users cannot see or request the extraction of individual records.
3. The tool allows clients to create reports on clinical administration, resourcing, service provision, cost-efficiencies and population demographics for planning and research purposes.
4. It serves as a focal point for collaborating and establishing communities of practice, and offers clients the ability to
   a. 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
   b. 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. CIHI Portal clients may be hospitals, regional health authorities, ministries of health or other health care–related public bodies.
6. In order to use CIHI Portal, clients must sign a service agreement with CIHI. The service agreement limits CIHI Portal clients' rights to use and disclose de-identified data and facility-identifiable information obtained through CIHI Portal. Specifically, clients and their users are permitted to use such data solely for internal, non-commercial, local/regional evidence-based decision-making, planning and analytical purposes.
7. 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.
8. CIHI Portal does not collect or use any new personal health information for its own purposes.
9. It contains data from 2 sources: subsets of existing CIHI data holdings and publicly available files from Statistics Canada. Existing CIHI holdings include the clinical administrative databases, the National Rehabilitation Reporting System and the Canadian MIS Database.
10. The data from existing data holdings is unlinked and is reported on separately within CIHI Portal. All privacy-sensitive 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.

1 Introduction

The Canadian Institute for Health Information (CIHI) collects and analyzes information on health and health care in Canada. Its mandate is to lead the development and maintenance of comprehensive and integrated health information that enables sound policy and effective health system management that improve health and health care. Flowing from its mandate, and in accordance with all applicable legislation, CIHI's core functions include

- Identifying health information needs and priorities;
- Coordinating and promoting the development and maintenance of national health information standards;
- Developing and managing health databases and registries;
- Conducting analyses in the areas of population health and health services;
- Developing national health indicators; and
- Conducting education sessions.

CIHI Portal is an analytical web-based tool for health care data. CIHI designed it to provide health care organizations such as hospitals, regional health authorities and ministries of health with online access to pan-Canadian health care data in a secure environment that safeguards privacy and confidentiality. The intended purpose of CIHI Portal is to help these organizations access key information required for monitoring, planning for and making decisions about the delivery of health care services.

This privacy impact assessment (PIA) updates the foundational PIA completed in 2008 and the related 2008–2009 and 2010–2011 addendums. The purpose of this PIA is to re-examine the potential privacy, confidentiality and security risks, if any, associated with CIHI Portal in its entirety, including any enhancements for 2013–2014. It 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 they apply to CIHI Portal.

2 CIHI Portal Background and Context

2.1 Background

CIHI Portal was initially developed in 2003 as a pilot project to demonstrate the value and feasibility of implementing an analytical tool that provided access to pan-Canadian data to assist health system stakeholders with high-level decision-making and performance management. Following a successful pilot project, CIHI Portal moved to an expanded and enhanced beta test in the fall of 2005, which addressed potential privacy, confidentiality and security issues that arose from access to CIHI Portal. This was accomplished by adopting practices in the area of privacy risk management, including controls on users, service agreements with clients, data disclosure and disclosure avoidance rules, and security practices. Since then, several enhancements to CIHI Portal that were approved by CIHI's e-Reporting and Analytical Portal Project Steering Committee have been implemented. All enhancements underwent a privacy review prior to implementation to identify any privacy risks and measures to mitigate those risks. All recommendations made in these reviews were addressed by CIHI.

2.2 Description of CIHI Portal and User Community

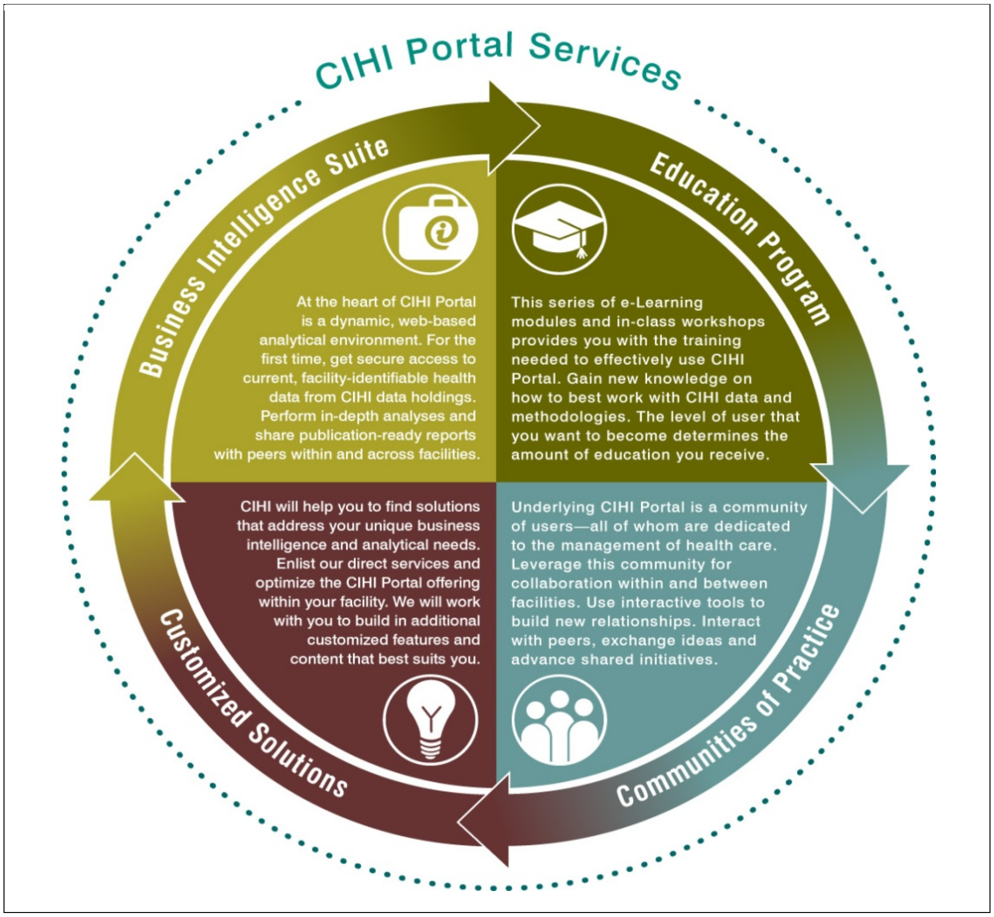
2.2.1 Description of CIHI Portal

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 intended purpose of CIHI Portal 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 product and service combine access to CIHI's enterprise data warehouse via a web-based business intelligence reporting tool with a comprehensive training program, support for building communities of practice and customized reporting solutions, and ongoing client support.

CIHI Portal offers its 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 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 the questions that are specific to their needs.

One of the unique features of CIHI Portal is the patient dimension functionality that was added in 2008 and updated in 2013. This functionality is specific to inpatient, day surgery and emergency department data sourced from the clinical administrative databases (CAD), existing CIHI data holdings (see Section 2.3: Description of Data Accessible Through CIHI Portal). Using this functionality, clients are able to identify trends in patient readmissions across time and geography. This is accomplished by creating a meaningless but unique number for each patient based on encrypted provincial/territorial health card number, date of birth and gender. By using report templates and filters, clients are able to select cohorts of patients of interest (e.g., all patients who had a hip replacement at a particular facility in 2009) and view a summary report on the subsequent or previous admissions of these patients for the same or other facilities.

Figure 1: CIHI Portal Services



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 data holdings. Perform in-depth analyses and share publication-ready reports with peers within and across facilities.

This series of e-Learning 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 data and methodologies. The level of user that you want to become determines the amount of education you receive.

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.

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.

2.2.2 CIHI Portal User Community

Access to CIHI Portal has traditionally been limited to a specific community of users who are, for the most part, also its data providers, such as individual health care facilities, regional health authorities, selected communities of practice and participating provincial and territorial ministries/departments of health. All users have entered into, and remain bound by, a CIHI Portal service agreement and so have access to CIHI Portal and appear on the list of CIHI Portal users posted on CIHI's website. In 2012, CIHI's Executive Committee approved expanding access to CIHI Portal to selected third-party organizations provided they could demonstrate that they meet all of the following criteria:

- The requester is a legally constituted organization that has a health care–related public mandate that supports the management of the health care system.
- The requesting organization has expertise in managing record-level data, including appropriate privacy and security policies and processes.
- The requesting organization is an accountable data custodian with a good track record.
- The requesting organization requires the data to be accessed through CIHI Portal to fulfill its mandate, or the ministry of health in the requesting organization's province supports its access to CIHI Portal.

Requests for access to CIHI Portal are submitted to the executive director, Atlantic Canada and Integrated eReporting, for approval. CIHI's Executive Committee is then informed of all third-party approvals.

2.3 Description of Data Accessible Through CIHI Portal

CIHI Portal contains data from 2 sources: subsets of existing CIHI data holdings and publicly available files from Statistics Canada. Existing CIHI holdings include the CAD, the National Rehabilitation Reporting System (NRS) and the Canadian MIS Database (CMDB). The data from existing data holdings is unlinked and is reported on separately with CIHI Portal. All privacy-sensitive 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.

2.3.1 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 databases contain demographic, diagnostic, intervention and administrative information about individual patients resulting from hospital inpatient acute separations, emergency department separations or outpatient (ambulatory care) separations (e.g., clinic and day surgery separations). The CAD are related in that they are both repositories of clinical, demographic and administrative data that is originally collected by hospitals and other health care facilities. CIHI Portal contains a selected subset of data from the CAD, which does not include names of recipients (patients), health card numbers, full dates of birth or full postal codes of recipients, or provider numbers (identifiers). (For more information about the CAD, read the privacy impact assessment.)

Discharge Abstract Database–Hospital Morbidity Database

The DAD-HMDB contains information on all acute care hospital inpatient and day surgery separations, including limited data about long-term care, rehabilitation and mental health events from some facilities.

National Ambulatory Care Reporting System

NACRS contains clinical, administrative and demographic information primarily from Ontario hospital-based and community-based ambulatory care: day surgery, outpatient clinics and emergency departments.

National Rehabilitation Reporting System

The NRS contains data on inpatients who receive rehabilitation services for a range of conditions, including orthopedic trauma or surgery, stroke and spinal cord dysfunction. Data is collected from participating adult inpatient rehabilitation facilities and programs across Canada, including specialized facilities or hospital rehabilitation units, programs and designated rehabilitation beds. (For more information about the NRS, read its privacy impact assessment.)

Canadian MIS Database

The CMDB collects and reports on day-to-day operations of health service organizations and contains financial and statistical information on hospitals and regional health authorities across Canada. The data is collected according to a standardized framework for collecting and reporting financial and statistical data on the day-to-day operations of health service organizations. The CMDB does not include patient-identifiable information. The CMDB does contain information on the salaries of employees, summarized to the national functional centre level, at health care organizations that submit data to the database; no identifying information, such as name or employee number, is included. (For more information about the CMDB, read its privacy impact assessment.)

2.3.2 Other Data

CIHI Portal also contains aggregated, non-confidential population statistics from Statistics Canada's census of population, as well as geographic and income data. The data elements made 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 additional data elements to CIHI Portal:

1. **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.
2. **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.

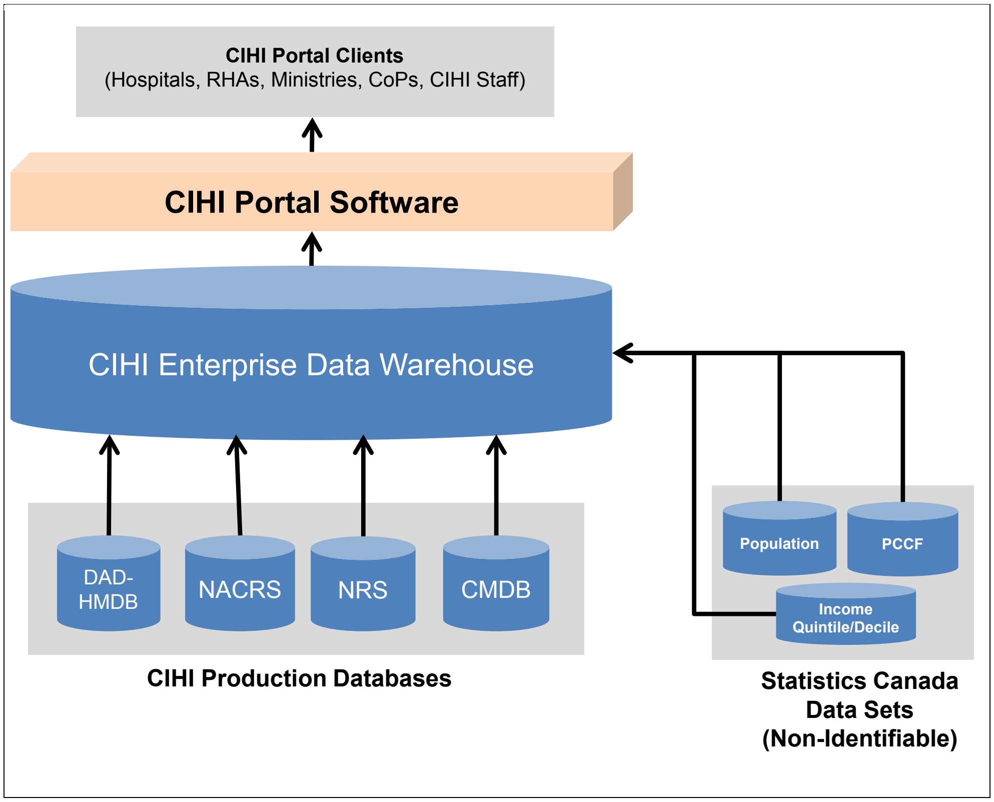
3. **Area Income Quintiles:** The area-based (neighbourhood income quintile) IPPE split into 5 equal categories, where the IPPE is a household size–adjusted measure of income based on the most recent census summary data.
4. **Area Income Deciles:** The area-based (neighbourhood income decile) IPPE split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

The rationale for introducing national and area income quintiles and deciles is to allow CIHI Portal users to perform ad hoc analyses related to socio-economic status on their patient populations.

2.3.3 Overview of Data Flow

Users access CIHI Portal through a secure web interface. Depending on their role, users are able to create ad hoc custom queries and/or access reports created by CIHI and other CIHI Portal users, both within and outside of their organizations. The outputs from these queries may be shared within CIHI Portal or exported to other file formats (such as MS Excel). The underlying record-level data is not exportable.

Figure 2: Data Flow in CIHI Portal


CIHI Portal Clients
(Hospitals, RHAs, Ministries, CoPs, CIHI Staff)
CIHI Portal Software
CIHI Enterprise Data Warehouse
DAD-HMDB
NACRS
NRS
CMDB
CIHI Production Databases
Population
PCCF
Income Quintile/Decile
Statistics Canada Data Sets (Non-Identifiable)

Notes

RHAs: Regional health authorities.

CoPs: Communities of practice.

PCCF: Postal Code Conversion File.

3 Privacy Analysis

3.1 Authorities Governing CIHI and CIHI Portal

General

CIHI adheres to its *Privacy Policy on the Collection, Use, Disclosure and Retention of Personal Health Information and De-Identified Data, 2010* (Privacy Policy, 2010) and to any applicable privacy legislation and/or agreements.

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.

All provinces and territories have public-sector privacy legislation in place. This legislation includes provisions that authorize public bodies covered by the acts to disclose person-identifiable data, without the consent of the individual, for statistical purposes. Newfoundland and Labrador, Nova Scotia, New Brunswick, Ontario, Manitoba, Saskatchewan and Alberta also have health information–specific privacy legislation with express lawful authority to use and disclose personal health information, without individual consent, for purposes of managing the health system, including statistical analysis and reporting.

For example, CIHI is recognized as a prescribed entity under Ontario's *Personal Health Information Protection Act*. 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.

Agreements

As indicated above in Section 2.3, CIHI Portal contains data sourced from subsets of existing CIHI data holdings. This data flows directly into CIHI via existing applications/systems from data providers (e.g., hospitals and other health care facilities). For the most part, these existing data flows are governed by CIHI's Privacy Policy, 2010, existing 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 Portal Service Agreement

In order to be able to use CIHI Portal, CIHI Portal clients (which could be hospitals, regional health authorities, ministries of health or other health care–related public bodies) must sign a service agreement with CIHI. The service agreement is signed at a senior level in the organization to ensure that clients are aware of both their organizational responsibilities and the responsibilities of their users.

The service agreement limits CIHI Portal clients' rights to use and disclose de-identified data and facility-identifiable information obtained through CIHI Portal. Specifically, clients and their users are permitted to use such data solely for internal, non-commercial, local/regional evidence-based decision-making, planning and analytical purposes. CIHI Portal data cannot be disclosed to any third party, except as expressly permitted in the service agreement or as required by law. Specifically, publication or disclosure outside of the client organization is permitted only where all reasonable measures are employed to prevent the identification of individuals and there are no cell sizes with fewer than 5 observations. Organization-identifiable information cannot be released unless the written consent of each organization identified in the information has been obtained prior to release.

Clients assume responsibility for ensuring that users of CIHI Portal in their organizations are aware of the terms and conditions of the service agreement. Within each client organization, individual users must be made aware of their strict obligation to

- Keep their usernames and passwords strictly confidential;
- Keep de-identified data obtained through CIHI Portal, including any reports, strictly confidential and not disclose such data to persons or organizations outside the client's organization, except as expressly provided for in the service agreement or as required by law;
- Use de-identified record-level data from CIHI Portal solely for non-commercial, internal purposes related to the client's planning, research/analysis or decision-support activities, unless explicitly permitted by an agreement between CIHI and the client;
- Not attempt to identify individuals when accessing and using de-identified data accessible through CIHI Portal and/or attempt to link this data with personal health information originating from any other source; and
- Access CIHI Portal from the client's corporate network only.

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

In addition, the service agreement sets out the following specific requirements and responsibilities with respect to usernames and passwords:

- Each user must create a user profile (name, title and email address), username and password on CIHI's website, as instructed by CIHI, to gain access to those areas of CIHI Portal that he or she is permitted to use.
- Clients and their users are responsible for maintaining the confidentiality of the means of access.
- Clients are fully responsible for all activities that occur under their means of access.
- Usernames and passwords may not be shared and are non-transferable, nor can they be assigned to an un-named individual or occupational position (such as director of health records).
- Clients and their users must not permit any third party or unauthorized user to access CIHI Portal.

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

As a reminder for the users, they must accept the Terms and Conditions of Use each time they log in to CIHI Portal prior to accessing any data.

3.2 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 team; a Privacy and Data Protection Committee of its Board of Directors; and an external chief privacy advisor.

CIHI Portal clients are accountable for applying the service 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.

3.2.1 Organization and Governance

Organization

CIHI Portal Services was established as a program area in the Acute and Ambulatory Care Information Services Branch in April 2007. In April 2013, the program area was moved to a newly created branch, Integrated eReporting, that reports to the executive director for Atlantic Canada and Integrated eReporting.

Governance

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

Position/Group	Role/Responsibilities
Executive Director, Atlantic Canada and Integrated eReporting	The executive director for Atlantic Canada and Integrated eReporting is responsible for the overall operations and strategic direction of CIHI Portal.
Integrated eReporting Operations Committee	Chaired by CIHI's executive director for Atlantic Canada and Integrated eReporting, this committee makes strategic recommendations and decisions about the direction of CIHI Portal and CIHI's integrated eReporting products.
Vice President and Chief Technology Officer	The chief technology officer is responsible for the strategic direction and overall operations/implementation of CIHI's technological and security solutions.
Information Management Steering Committee	Chaired by CIHI's chief technology officer, this committee makes strategic recommendations and decisions related to technology.
Chief Privacy Officer and General Counsel	The chief privacy officer is responsible for the strategic direction and the overall implementation of CIHI's Privacy program.

(cont'd on next page)

Position/Group	Role/Responsibilities
Chief Information Security Officer	The chief information security officer is responsible and accountable for leading CIHI's Information Security program, including defining goals, objectives and metrics consistent with the corporate Strategic Plan and CIHI's Privacy program, to ensure the organization's security principles, policies, procedures and practices support the protection of the organization's information.
Manager, Portal Services	The manager for Portal Services is responsible for ongoing management, development and deployment of CIHI Portal. The manager makes operational decisions about CIHI Portal, supports the Integrated eReporting Operations Committee and consults internally and externally with CIHI Portal clients as appropriate.
Manager, Information Access and Delivery, and Manager, Health Information Applications	These managers are responsible for ensuring that technical requirements for the ongoing development and maintenance of CIHI Portal are met. The Health Information Applications team is responsible for acting as system administrator for CIHI Portal.

3.3 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 health care data. The service agreement limits CIHI Portal clients' rights to use and disclose de-identified health information and facility-identifiable information obtained through CIHI Portal. Specifically, clients and their users are permitted to use such data solely for internal, non-commercial, local/regional evidence-based decision-making, planning and analytical purposes. The intended purposes and scope of CIHI Portal are clearly identified in this PIA and on CIHI's website.

3.4 Principle 3: Consent for the Collection, Use or Disclosure of Personal Health Information

CIHI obtains data for purposes of the planning and management of the health system, including statistical analysis and reporting, under specific legislative authority and/or by legal agreements governing the flow of data. The de-identified, record-level data found in CIHI Portal is sourced from subsets of existing CIHI data holdings and is collected in its original form through the administration of the health care system in the various jurisdictions and provided to CIHI as a secondary user.

3.5 Principle 4: Limiting Collection of Personal Health Information

CIHI is committed to the principle of data minimization. Per sections 1 and 2 of CIHI's Privacy Policy, 2010, CIHI collects from data providers only personal health information and de-identified data that is reasonably required for health system uses, including statistical analysis and reporting, in support of the management, evaluation or monitoring of the allocation of resources to, or planning for, the health care system in Canada, including support for the improvement of the overall health of Canadians. CIHI limits its collection of personal health information and de-identified data to that which is reasonably required for health system uses, including statistical analysis and reporting.

CIHI Portal does not collect or use any new personal health information for its own purposes. It is a secure means of access to selected data already held at CIHI in the CAD, NRS and CMDB.

Special Project Fields

CIHI Portal contains Special Project fields found in the DAD and NACRS abstracts. These fields are used by data providers to capture supplemental information not routinely captured in the DAD and NACRS abstracts for all jurisdictions. This supplemental information is captured in the form of alpha and/or numeric values in either reserved or unreserved project fields.

Reserved fields are designated for the use of CIHI and/or specific jurisdictions; they typically involve larger-scale projects (e.g., Canadian Paediatric Surgical Wait Times, Canadian Stroke Network), where data is jointly defined by project participants. Data related to these reserved projects is stored within the appropriate database (DAD or NACRS) and routinely returned to data providers as part of CIHI's data quality processing, including error/warning notification.

Unreserved fields are undesignated and available for use by CIHI, a data provider or data providers participating jointly in a project. Data captured in unreserved fields is defined by those submitting the data, and only they know what information is being captured.

Privacy Risk: Personal Health Information Included in Special Project Fields

Mitigation Measures Currently in Place

- The CAD's abstracting manual informs data providers to not use Special Project fields to record personal identifiable or confidential information (e.g., health care [card] numbers, chart numbers, provider numbers).
- The CAD conducts semi-annual audits of Special Project fields to ensure that health care numbers are not collected.
- CIHI Portal clients have signed a service agreement (see Section 3.1), which imposes a variety of confidentiality and security restrictions and obligations on them, including a prohibition against attempting to identify individuals.
- Values entered into unreserved project fields are meaningful to only the data provider.

3.6 Principle 5: Limiting Use, Disclosure and Retention of Personal Health Information

3.6.1 Limiting Use

CIHI limits the use of CIHI Portal to authorized purposes, and only authorized users have access. The CIHI Portal service agreement allows clients to use de-identified record-level data for only their own non-commercial, internal analysis, planning, research and decision-making purposes.

As described in Section 3.1, CIHI Portal clients are required to sign a service agreement, which imposes confidentiality and security restrictions and obligations. Failure to respect the terms and conditions of the service agreement would jeopardize their continued access to CIHI Portal. CIHI Portal clients are also subject to the requirements of data protection laws in their respective jurisdictions.

CIHI staff are permitted to access and use CIHI Portal data on a need-to-know basis only, including for data processing and quality management purposes, the production of 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 they signed at the commencement of employment; staff are subsequently required to renew their commitment to privacy annually.

3.6.2 Limiting Disclosure

Query results obtained through CIHI Portal may contain de-identified data in the form of small cell sizes (defined as 5 or fewer occurrences) that are not suppressed in the reports produced by users. Information obtained through CIHI Portal will not be published by clients but will be used to inform internal decision-making in a specific health care environment. Specifically, publication or disclosure outside of the client organization is permitted only where all reasonable attempts to prevent the identification of individuals are employed and there are no cell sizes with fewer than 5 observations. If information obtained through CIHI Portal is going to be published or further disclosed, the Portal Service Agreement clearly instructs clients to present the information in such a way as to prevent the re-identification of individuals.

Privacy Risk: Re-Identification and Residual Disclosure

Combining data, such as on a patient's age and geographic representation (e.g., forward sortation area of a patient's residence), plus the name and location of a facility in a rural area could lead to the re-identification of individuals and residual disclosure of information.

Mitigation Measures Currently in Place

The disclosure of reports produced by authorized users is limited to CIHI Portal clients who have signed a service agreement (see Section 3.1), which imposes a variety of confidentiality and security restrictions and obligations on them.

The terms of the service agreement provide for

- A prohibition against attempts to identify individuals;
- A prohibition against data linkage using information gained through CIHI Portal;
- A prohibition against further publication by CIHI Portal clients, including requirements to present the information in such a way as to prevent the re-identification of individuals and to suppress cell sizes with fewer than 5 observations; and
- Consequences for institutions in the case of demonstrated breaches, such as denial of further access to CIHI Portal.

Access to CIHI Portal is governed on the need-to-know principle and determined by the role of the user. Further, within client organizations, users are broken down into 3 roles: report reader, information consumer and analyst. Report readers are permitted to view reports only—they cannot create or manipulate reports. Information consumers can manipulate existing reports. Analysts have maximum access and the most flexibility to work with the data available through CIHI Portal (e.g., creating reports or calculating new metrics from existing data).

In addition, specific protective measures implemented in CIHI Portal to control disclosures include the following:

- Only a selected subset of variables from the existing CIHI data holdings (CAD, NRS, CMDB) is included in CIHI Portal.
- De-identification measures are applied to the data (e.g., dates of birth, health card numbers, chart numbers and full postal codes of patients are not included in CIHI Portal).
- CIHI Portal does not allow direct access to individual records. Queries to create reports may return rows with individual record counts, but users cannot see or request the extraction of individual records.
- The organizational contact identified in the service agreement is responsible for naming authorized users in each user role and for communicating changes in user access to CIHI.
- Mandatory education (eLearning and instructor-led training) for users reinforces the appropriate use and disclosure of data from CIHI Portal.
- Technical safeguards (e.g., usernames and passwords, encryption, auditing, system monitoring) regulate the query environment and limit disclosure by minimizing risks of unauthorized access, including providing access to only named users (for further information, see Principle 7: Safeguards for Personal Health Information).

Termination of pregnancy data sourced from the DAD, NACRS and the CMDB is also contained in CIHI Portal. In the DAD and NACRS projects, key information such as diagnosis and intervention codes that could potentially identify a termination of pregnancy is masked to an unknown or not applicable value. This is intended to mitigate the risk that data would reveal information related to the provision of abortion services in British Columbia at the facility level and thereby contravene Section 22.1 of B.C.'s *Freedom of Information and Protection of Privacy Act*.

Privacy Risk: Contravention of B.C.'s *Freedom of Information and Protection of Privacy Act*

Mitigation Measures Currently in Place

CIHI Portal has implemented specific protective measures to control disclosures, including special protections to mask sensitive abortion data (any procedure that terminates a pregnancy for any reason, including therapeutic abortions). For example, therapeutic abortion data is masked in CMDB eReports by rolling 7 sub-accounts into the more general account Gynecology Specialty Clinic. An annual review of termination of pregnancy data is conducted by the CIHI Portal team and the Management of Termination of Pregnancy Working Group to ensure adequate masking processes are implemented.

3.6.3 Limiting Retention

Data accessible through CIHI Portal forms part of CIHI's information holdings and is retained by CIHI for as long as required to meet the intended purpose. Currently, CIHI Portal maintains 5 to 10 of the most recent years of the selected data, depending on the holding.

3.7 Principle 6: Accuracy of Personal Health Information

CIHI has a comprehensive data quality program. Any known data quality issues are addressed by the data provider or documented in data limitations documentation, which is made available to all users. Information Technology Services and Portal Services verify that the data available within CIHI Portal corresponds to the data in existing CIHI data holdings (CAD, NRS, CMDB) in terms of accuracy (volumes, completeness).

3.8 Principle 7: Safeguards for Personal Health Information

CIHI's Privacy and Security Framework

CIHI has developed the Privacy and Security Framework to provide a comprehensive approach to 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 provide an integrated view of the organization's information management practices. Key aspects of CIHI's system security with respect to CIHI Portal are described below.

System Security

CIHI has established physical, technical and administrative security practices to ensure the confidentiality and security of all of its data holdings. Moreover, CIHI's employees are aware of the importance of maintaining the confidentiality of personal health information through a mandatory privacy and security training program, and through ongoing communications about CIHI's privacy and security policies and procedures.

CIHI is committed to safeguarding its IT ecosystem, to securing its data holdings and to 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 and 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, 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.

Through the use of system audit trails and logs for CIHI Portal, monitoring and auditing activities include

- Capturing what was queried, when and by whom;
- Logging all system accesses and queries run by username, time and date; and
- Disconnecting sessions after a pre-set time.

In addition to the general safeguards already in place, CIHI Portal has implemented the following technical and administrative safeguards:

- CIHI Portal security architectures/security filters are designed using the need-to-know principle and determined by the role of the user.
- Users cannot change or remove a security filter—it is enforced automatically when users execute queries. These privileges and permissions are tested after each data or functionality release to ensure they are still performing as expected.
- Users of CIHI Portal cannot turn off security features. Only the internal CIHI Portal administrator has the ability to modify security filters, privileges and permissions.
- Encryption software incorporated in CIHI Portal uses a networking protocol called secure sockets layer (SSL). SSLs are cryptographic protocols that provide secure transmission and communication on the internet for such things as web browsing, email, internet faxing, instant messaging and other data transfers.
- Usernames and passwords permit authentication and ensure that only authorized users can access CIHI Portal.

In addition,

- The system will lock out users after a pre-determined number of failed login attempts;
- Users may be required to attain re-authorization via mandatory training and evaluation if they have not used CIHI Portal in 12 months; and
- User-created passwords must meet a minimum standard deemed to be secure.

Technical Safeguards

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 risk register, and appropriate action is taken.

3.9 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 on its corporate website. As well, this PIA is accessible on CIHI's website (www.cihi.ca).

3.10 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 health decisions affecting the individual. 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.

3.11 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, complaints about CIHI's handling of personal health information are investigated by the chief privacy officer. The chief privacy officer may direct an inquiry or complaint to the privacy commissioner of the jurisdiction of the person making the inquiry or complaint.

4 Conclusion

This PIA summarizes CIHI's assessment of the privacy implications of CIHI Portal. It identified 3 potential risks; however, this assessment concludes that the mitigation measures currently in place are such that CIHI is prepared to accept and manage any remaining risks.

Appendix A: Examples of CIHI Portal Data

Type of Information	Examples of Data and Variables
Recipients: Socio-Demographic/ Demographic/ Geographic	• Forward sortation area (first 3 digits of postal code) • Residence code • Province/territory of residence • Census subdivision • Age in years • Gender • Statistics Canada income deciles by census division of residence • Living arrangement/setting (e.g., living with family or living in an institution) • Residence type (e.g., living in a private dwelling or homeless)
Facilities: Identification/ Geographic	• Facility or institution number • Type of facility • Province/health region/census subdivision/postal code
Entry/Admission/ Status	• Entry code (e.g., day surgery, clinic) • Admit by ambulance flag • Admission category (e.g., newborn, stillbirth) • Readmission flag
Patient Service	• General medicine • Cardiology • Obstetrics/gynecology • Psychiatry
Provider Information	**Provider Service:** The level of training or specialty of a physician or non-physician health care professional responsible for the care and treatment of the patient *Examples* • Physician services – General practitioner – Cardiologist – Obstetrician – Psychiatrist • Non-physician services – Dentist – Physiotherapist **Provider Type:** The role played by a health care provider during a patient’s stay (e.g., most responsible provider, admitting, consulting, intervention)
Clinical Information/Health Characteristics/ Assessments	• ICD-10-CA diagnoses (e.g., appendicitis) • CCI interventions (e.g., appendectomy) • Motor and cognitive functional abilities (e.g., eating, grooming, bathing, communication, problem-solving, memory, financial management) • Newborn and neonatal weight
Special Care Unit (SCU)	• SCU type – Pediatric intensive care unit – Neurological intensive care unit

(cont’d on next page)

Type of Information	Examples of Data and Variables
Transfer/Follow-Up/Discharge Status	• Service transfer—Patient service • Service interruption • Follow-up assessment • Transfer to/from facility • Discharge disposition (e.g., alive, dead, transfer)
Date and Time Periods	• Ambulance arrival date and time • Emergency department decision to admit date and time • Admission or discharge date and time (week, quarter, month or year) • SCU admission or discharge date and time (week, quarter, month or year)
Derived Variables	• Age/gestational age • Length of stay (e.g., total length of stay in days, length of stay in hours in SCU) • Emergency or surgical wait times • Plx level (complexity) • MCC (major clinical category) • CMG (Case Mix Group) • RIW (Resource Intensity Weight) • MAC (major ambulatory cluster) • CACS (Comprehensive Ambulatory Classification System) • Distinct cases (e.g., SCU) • COUNT (e.g., number of pediatric intensive care unit visits) • SUM (e.g., total cases, procedure minutes) • AVG (e.g., hospital distance in kilometres) • MED (e.g., median length of stay in days)
Special Projects—Supplemental Information not Routinely Captured	• Reserved projects for use by CIHI and/or specific jurisdictions (e.g., wait times, stroke) • Unreserved projects (undefined data not specified for use by CIHI and/or provinces/territories; values are meaningful to only the data provider)

Production of this document is made possible by financial contributions from Health Canada and provincial and territorial governments. The views expressed herein do not necessarily represent the views of Health Canada or any provincial or territorial government.

For permission or information, please contact CIHI:

Canadian Institute for Health Information
495 Richmond Road, Suite 600
Ottawa, Ontario K2A 4H6

Phone: 613-241-7860
Fax: 613-241-8120
www.cihi.ca
copyright@cihi.ca

Cette publication est aussi disponible en français sous le titre *Portail de l’ICIS — Évaluation des incidences sur la vie privée*.

Talk to Us

CIHI Ottawa
495 Richmond Road, Suite 600
Ottawa, Ontario K2A 4H6
Phone: 613-241-7860

CIHI Toronto
4110 Yonge Street, Suite 300
Toronto, Ontario M2P 2B7
Phone: 416-481-2002

CIHI Victoria
880 Douglas Street, Suite 600
Victoria, British Columbia V8W 2B7
Phone: 250-220-4100

CIHI Montréal
1010 Sherbrooke Street West, Suite 300
Montréal, Quebec H3A 2R7
Phone: 514-842-2226

CIHI St. John's
140 Water Street, Suite 701
St. John's, Newfoundland and Labrador A1C 6H6
Phone: 709-576-7006

7921-0614

20 YEARS • ANS 1994 • 2014

www.cihi.ca
At the heart of data

CIHI ICIS
Canadian Institute
for Health Information
Institut canadien
d'information sur la santé