Integrated interRAI Reporting System

Privacy Impact Assessment

August 2021

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

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

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. *Integrated interRAI Reporting System Privacy Impact Assessment, August 2021*. Ottawa, ON: CIHI; 2021.

Cette publication est aussi disponible en français sous le titre *Système d'information intégré interRAI : évaluation des incidences sur la vie privée, août 2021*.

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

- *Integrated interRAI Reporting System, August 2021*

Approved by

Brent Diverty
Vice President, Data Strategies and Statistics

Rhonda Wing
Chief Privacy Officer and General Counsel

Ottawa, August 2021

Table of contents

Quick facts about the Integrated interRAI Reporting System

1. The Integrated interRAI Reporting System (IRRS) is a pan-Canadian database at the Canadian Institute for Health Information (CIHI) that captures standardized clinical, demographic, administrative and resource utilization information on publicly funded home care and facility-based long-term care (LTC) services.
2. IRRS collects newer versions of the home care and LTC data sets that have historically been collected in CIHI's Home Care Reporting System (HCRS) and Continuing Care Reporting System (CCRS).
3. IRRS leverages a new data collection method with near-real-time messaging and new validation processes using a cloud-based application programming interface.
4. HCRS and CCRS, implemented in 2005 and 2003, respectively, were developed in consultation with stakeholders from across the country and contain only those data elements determined to be necessary to achieve the goals and purposes of those databases. IRRS is similarly limited to those data elements that were deemed important for reporting by stakeholders.
5. IRRS began collecting data in 2019; home care and facility-based LTC data is longitudinal and contains each client's historic information.
6. The data collected in IRRS is used to develop accurate, timely and comparable information that describes the population of clients receiving home care services and residents receiving LTC services, the services they receive and the clients'/residents' outcomes.
7. Health service administrators, policy-makers, governments, researchers and other stakeholders rely on this information to manage access to services, improve the quality of services provided and manage the resources required to deliver services.
8. Information derived from data submitted to IRRS is available via web-based eReports to organizations that submit data to IRRS, ministries of health, regional health authorities and other approved organizations. It will also be made available via public Quick Stats, Your Health System and other CIHI information products.

Note: This privacy impact assessment (PIA) does not cover the privacy, confidentiality and security risks associated with HCRS and CCRS. This information can be found on CIHI's website in the *HCRS PIA* and *CCRS PIA*.

Definitions

For the purposes of this PIA, the terms below have the following meanings:

Integrated interRAI Reporting System database (IRRS database) means any aggregate data and record-level data collected through and stored in CIHI's IRRS, which includes but is not limited to the following clinical assessment instruments and related administrative CIHI data:

- interRAI Home Care
- interRAI Long-Term Care Facilities

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

Client means a person receiving health care in a home care program or an LTC facility. In the LTC sector, these clients are commonly referred to as residents.

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 (LTC) homes, regional health authorities, medical practitioners and governments. This data includes information about health services provided to individuals, the health professionals who provide those services and the cost of the health services.

The purpose of this privacy impact assessment (PIA) is to examine the privacy, confidentiality and security risks associated with the Integrated interRAI Reporting System (IRRS). This PIA includes a review of the 10 privacy principles set out in the Canadian Standards Association's *Model Code for the Protection of Personal Information* and how the principles apply to IRRS, 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

CIHI has been collecting home care data since 2005 (see the *Home Care Reporting System [HCRS] PIA*) and LTC data since 2003 (see the *Continuing Care Reporting System [CCRS] PIA*). Both HCRS and CCRS capture information on the client's health, cognitive and functional status; demographic and administrative information; and information on resources used in providing care and services, through standardized interRAI assessments and administrative data agreed to by CIHI and its pan-Canadian stakeholders.

IRRS was developed to eventually replace HCRS and CCRS and to capture home care and LTC data using the updated versions of the interRAI instruments. These newer versions are designed to use common data standards across sectors, and IRRS leverages these common standards through an integrated system, as well as modernized means of data capture, including standard communication protocols such as the Health Level Seven (HL7) international standard. IRRS also utilizes the Fast Healthcare Interoperability Resources (FHIR) specification, which allows for the electronic exchange of health care information and uses cloud-based application programming interfaces (APIs) for data submission.

2.1 Introduction to IRRS

IRRS is a longitudinal database that collects individual (client) assessment information captured by data providers at multiple points throughout an individual's encounters with organizations that deliver home care and/or LTC services. The data standard is founded on 2 integrated interRAI instruments: the interRAI Home Care (HC) and the interRAI Long-Term Care Facilities (LTCF).

IRRS captures information on home care services funded by provincial and territorial governments, including services provided by private-sector agencies that the government retains to provide publicly funded services on its behalf. It captures information on both short-term home care services provided to clients (e.g., for time-limited acute conditions) and longer-term services provided to clients (e.g., services that enable clients to remain in a community setting).

Similarly, IRRS captures information about clients or residents living in publicly funded or subsidized LTC facilities (often also referred to as nursing homes or residential care). The organizations that submit LTC data to IRRS may be publicly or privately owned and operated.

The data collected in IRRS is used to develop accurate, timely and comparable information that describes the population of clients receiving home care services and of residents receiving LTC services, the services they receive and the clients'/residents' outcomes. Health service

administrators, policy-makers, governments, researchers and other stakeholders rely on this information to manage access to services, improve the quality of services provided and manage the resources required to deliver services.

IRRS incorporates into a single reporting system clinical, demographic, administrative and resource utilization information related to person-level care from publicly funded home care and LTC. The database

- Leverages a common and standardized language from the assessment system;
- Includes detailed items specific to individual care populations;
- Permits identification of multiple longitudinal records for a given individual; and
- Leverages CIHI's master data standards (CRDM, ICD-10-CA, Drug Product Database used in the National Prescription Drug Utilization Information System [NPDUIS] and Organization Index[i]).

The existing data holdings that support collection of home care and LTC information (HCRS and CCRS) will be maintained concurrently with IRRS for a period of time to support jurisdictions in transitioning to the new versions of the relevant instruments (interRAI HC and interRAI LTCF). Note that individual facilities will not concurrently submit data to IRRS and HCRS/CCRS.

At the time of writing this PIA, no interRAI HC data is being submitted to IRRS. There are plans for interRAI HC data to start being submitted later in 2021.

2.2 Data collection

IRRS currently supports 2 care sectors — home care and LTC (also known as continuing care) — and 2 interRAI instruments — the interRAI HC and interRAI LTCF. Below are descriptions of the instruments.

- **The interRAI HC assessment system** is designed to inform and guide comprehensive care and service planning in community-based settings. It focuses on a person's functioning and quality of life by assessing needs, strengths and preferences, and facilitates referrals when appropriate. When used over time, it provides the basis for an outcome-based assessment of the person's response to care or services. The interRAI HC is used to assess persons with chronic needs for care as well as those with post–acute care needs (e.g., after hospitalization, in a hospital-at-home situation).[1]
- **The interRAI LTCF assessment system** enables comprehensive, standardized evaluation of the needs, strengths and preferences of persons receiving continuing care services in hospital-based facilities and LTC homes.[2]

i. The Organization Index (OI) is a database that offers an integrated view of CIHI's organizational data, by tracing data that has been submitted to different CIHI data holdings back to a single organization. The OI also tracks ongoing changes to organizations and their hierarchical relationships with each other.

The interRAI HC, which contains approximately 306 data elements, and the interRAI LTCF, which contains approximately 314 data elements, are comprehensive assessment instruments that cover a number of domains. Approximately 242 data elements are common to both instruments; these are a core set of assessment items considered important in all care settings[3] and differ based on the care population being assessed or care setting where the assessment is performed.

For the 2 interRAI instruments that are currently supported in IRRS, the data is categorized into 3 distinct sections:

- **Client (demographic) data** (e.g., Case Record Number, Health Care Identification Number, Birthdate, Sex, Language)
- **Encounter (administrative) data** (e.g., Admission Date, Discharge Date, Current Payment Sources, Program Types)
- **Clinical assessment data** (e.g., Treatments, Diagnoses, Cognition, Physical Function)

The following is a list of identifiers collected by IRRS:

Personal (client) identifiers

- Health Care Identification Number
- Case Record Number
- Birthdate
- Postal Code of Usual Living Arrangement

Indigenous identifiers

- Indigenous Identity
- Current Payment Sources

Health facility/agency identifiers

- Facility/Agency Identifier
- Site Identifier

System features

Data is submitted to IRRS using software that data providers may build or secure through an external software vendor. This software may take advantage of any number of the following operations that have been built into IRRS:

Add/Create (client, encounter and assessment data): This feature is used to create and submit new client, encounter and assessment data not previously submitted.

Correct: This feature is used to correct erroneous data (e.g., an incorrect birthdate or diagnosis) that has been previously submitted and accepted.

Update: This feature is used to modify previously submitted and accepted data for the purposes of having more up-to-date administrative data available (e.g., Health Care Identification Number, Bed Type, Program Type, Current Payment Sources).

Validate: This feature allows data submitters to send data to IRRS to check it against CIHI's validation rules to identify issues that may require fixing. Unlike with the Create feature, data is not saved at CIHI but is only checked against the validation rules.

Delete: This feature is used to delete previously submitted and accepted data from IRRS.

Transfer: This feature enables a transfer of a client to another facility/agency so that the assessment cycle can be continued at the receiving facility/agency. However, this feature does not transfer client data from one facility/agency to another in IRRS.

Query: This feature permits data submitters to search for a subset of their own data within IRRS, most commonly for data reconciliation purposes. A limited number of search (input) parameters and returned outputs are permitted. The query functionality replicates the Verification Audit Report capabilities that are currently present in CCRS, HCRS and other CIHI databases. Below are examples of what users can query:

About the client

- CIHI Client ID
- Facility/Agency Identifier
- Case Record Number

About the encounter

- CIHI Encounter ID
- Day Stay Began/Case Opened
- Return Date
- Last Day of Stay

About the assessment

- CIHI Assessment ID
- Instrument Type/Identifier
- Reason for Assessment
- Assessment Reference Date

2.3 Access management, data submission and data flow for IRRS

IRRS is a longitudinal system that manages individual (client) assessment information captured by data providers at multiple points throughout an individual's encounters at health facilities or agencies delivering LTC or home care services.

Access management for the IRRS database

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

Access to IRRS requires a data provider's system to send data to CIHI to be registered with CIHI. The system can be registered by authorized data providers or their authorized software vendors. The registration process for access is outlined below:

System registration

Data providers or their authorized software vendors are required to sign CIHI's Health Information Standards and Specifications Agreement[ii] (including Schedule A — Product Terms and Conditions), which governs access to and use of the products[iii] as well as their rights, restrictions and obligations pertaining to the environment and the products (see also Section 3.2). Data providers or their authorized software vendors must also complete the Vendor Testing Form to identify the individuals who will be completing the system registrations.

To register a system with CIHI, a representative of the data provider or their authorized software vendor must create a CIHI profile. CIHI uses the profile information and information provided in the Vendor Testing Form to grant representatives access to register the system for the appropriate organizations. Once authenticated through CIHI's AMS, IRRS data flows directly from the data provider's system or the data provider's authorized software vendor application to CIHI's IRRS system.

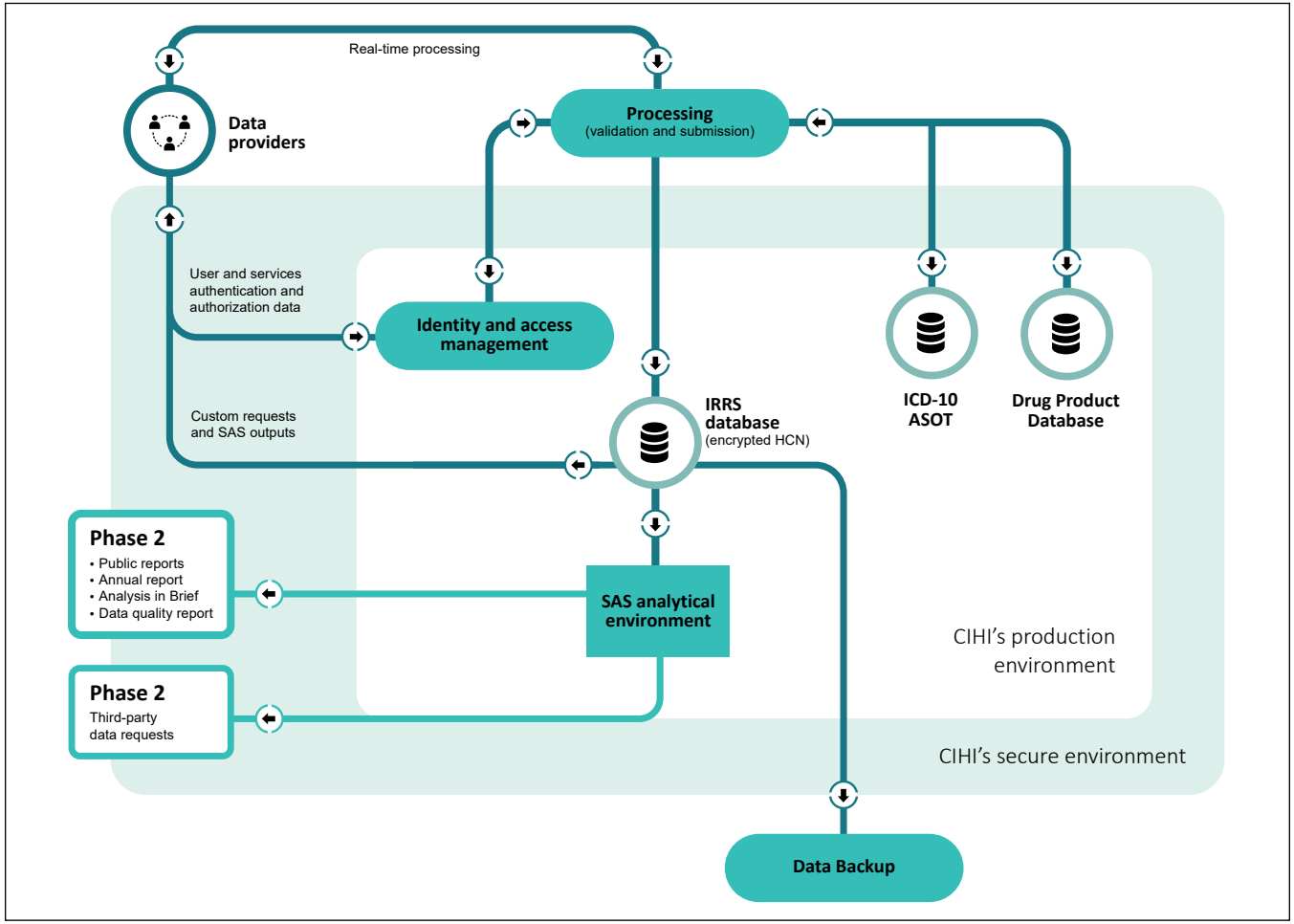
Data flows

All the IRRS data flows are highlighted in the following figure.

ii. CIHI's Health Information Standards and Specifications Agreement includes Schedule B, which consists of forms for terminating use of the product.

iii. **Products** means the CIHI products, specifications, documentation, software and other materials and related services, including but not limited to support and updates, selected by the customer pursuant to this agreement. For greater certainty, this also includes all methods, techniques, algorithms, information and data disclosed within the products.

Figure Overview of data flows for IRRS



Notes

HCN: Health care number.

ICD-10 ASOT: International Statistical Classification of Diseases and Related Health Problems, 10th Revision analytical source of truth.

During the normal course of delivering services, users collect data at the point of care. These users have been trained in the use of the interRAI instruments and are guided by user manuals containing the standards for each interRAI instrument. Users enter the necessary data directly into their organization's information system, which is designed for use with IRRS, and manage (create, retrieve, update, correct, delete and query) submitted IRRS records. This is achieved through API calls, which are logged for auditing purposes.

Upon submission, all data submitted to IRRS automatically undergoes data validation in CIHI's secure environment for errors and inconsistencies against the IRRS FHIR[iv] submission specifications. Data processing transactions are augmented by validating ICD-10-CA diagnosis and procedure codes through the use of published API calls to copies of ICD libraries from the ICD-10 analytical source of truth, and by validating drug formulary entries through the use of published API calls to the NPDUIS formulary information (drug identification numbers) from the Drug Product Database, both which are replicated in CIHI's secure environment. Rejected records are flagged in near real time, and details of failed validation results are returned to data providers' information systems so users can correct and resubmit them. Results of failure, as well as the original submission data, are stored in CIHI's secure environment for use in operational support activities.

Records that pass validation checks are saved in the IRRS production database until an authorized CIHI analytical staff member loads a copy of the data set to the IRRS-specific portion of CIHI's SAS analytical environment. Data that is considered sensitive (i.e., fields that hold, or that have the potential to hold, personal health information) is stored separately in this environment so that access may be permitted only to CIHI staff who require it for approved operational or analytical purposes. Staff access to IRRS data of any type is managed through the centralized SAS Data Access Process in alignment with CIHI's policies for data access.

Upon request, CIHI returns IRRS data to the data providers that originally supplied it, as well as to their respective provincial or territorial ministries. Organizations that submit interRAI LTCF data to CIHI, as well as their governing provincial or territorial ministries/departments of health or social services, regional health authorities and other approved organizations, are also entitled to access CIHI-generated reports that are based on this data. These private reports provide aggregated information regarding resident populations and outcomes (e.g., quality of care indicators) and are accessible from within the CCRS eReporting environment (which now includes CCRS and IRRS data) — a secure, web-based business intelligence tool that allows authorized users to view and manipulate data in an interactive manner.

In Phase 2, CIHI will also disclose aggregate and record-level data to approved third-party requesters and aggregate data to the public, in accordance with provincial/territorial data-sharing agreements and CIHI's privacy and information security policies.

Copies of CIHI data and applications are retained on backup systems.

---

iv. FHIR is a standard that describes data formats and elements (known as "resources") and an API for exchanging electronic health records. The standard was created by the HL7 health care standards organization.[4]

3 Privacy analysis

3.1 Privacy and Security Risk Management Program

Privacy and security risk management (PSRM) is a formal, repeatable process for identifying, assessing, treating and monitoring risks in order to minimize the probability of such risks materializing and/or their impact should they occur. In 2015, CIHI approved its Privacy and Security Risk Management Framework and implemented the associated *Policy on Privacy and Security Risk Management*. CIHI's chief privacy officer and chief information security officer, in collaboration with senior managers, are responsible for identifying, assessing, treating, monitoring and reviewing privacy and security risks.

Privacy and security risks may be identified from a variety of sources, including PIAs, for example. Once identified, risks are entered into the Privacy and Security Risk Register and categorized as **high**, **medium** or **low**, based on the likelihood and impact of a risk event:

- **High:** High probability of risk occurring, and/or controls and strategies are not reliable or effective;
- **Medium:** Medium probability of risk occurring, and/or controls and strategies are somewhat reliable or effective; or
- **Low:** Low probability of risk occurring, and/or reliable, effective controls and strategies exist.

The likelihood and impact of the identified risk are used to create a risk score. The risk assessment score of low, medium or high defines the seriousness of a risk. A higher risk ranking indicates a more serious threat and a greater imperative for treatment. Once an initial risk treatment is applied, the residual risk (the new calculation of the likelihood and impact of the risk, given the treatment) is assessed and compared against CIHI's privacy and security risk tolerance statement, which indicates that CIHI's privacy and security risk tolerance is low. If the risk score for the residual risk is still greater than low, additional risk treatment is necessary until the risk is low or the untreated/residual risk is accepted by CIHI's Executive Committee on behalf of the corporation.

As a result of this PIA, 7 privacy and security risks were identified in the areas of system registration and authentication. These risks were added to CIHI's Privacy and Security Risk Register, and all risks were assessed and mitigated to a residual risk score of low in accordance with the PSRM methodology.

3.2 Authorities governing IRRS data

General

CIHI adheres to its *Privacy Policy, 2010* and to any applicable privacy legislation and/or legal agreements.

Privacy legislation

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

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

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

Agreements

At CIHI, IRRS 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.

Data-sharing agreement

CIHI signed a license agreement with interRAI in 1996, granting CIHI an exclusive right to use interRAI's assessment forms in Canada for the purposes of national statistical reporting. The license agreement also commits CIHI to supplying interRAI with an annual copy, in de-identified form, of the data collected with the interRAI assessment forms and captured by IRRS for interRAI's purposes. These purposes include refining the interRAI works and their associated applications, and preparing analyses and reports regarding clinical practice, population health and the health care system.

Health Information Standards and Specifications Agreement[v] (including Schedule A — Product Terms and Conditions) for access to and use of CIHI's environment and the products)

Data providers or their authorized software vendors must sign the Health Information Standards and Specifications Agreement, which governs access to and use of CIHI's specifications, standards and other materials to develop the IRRS software.

CIHI's Electronic Reporting Services Agreement

Authorized data providers that submit LTC data to CCRS or IRRS must sign CIHI's Electronic Reporting Services Agreement to access the CCRS eReporting service. The agreement outlines obligations around access to the data, as well as security, use and disclosure. It is signed at a senior level in the organization to ensure users are aware of their organizational responsibilities. Compliance with the terms and conditions of the agreement is mandatory.

v. CIHI's Health Information Standards and Specifications Agreement includes Schedule B, which consists of forms for terminating use of the product that must be completed in accordance with Section 9.2 of the agreement.

3.3 Principle 1: Accountability for personal health information

CIHI's president and chief executive officer is accountable for ensuring compliance with CIHI's *Privacy Policy, 2010*. CIHI has a chief privacy officer and general counsel, a corporate Privacy, Confidentiality and Security Committee, a Governance and Privacy Committee of its Board of Directors, and an external chief privacy advisor.

Organization and governance

The following table identifies key internal senior positions with responsibilities for IRRS data in terms of PSRM:

Table Key positions and responsibilities

Position/group	Roles/responsibilities
Vice president, Data Strategies and Statistics	Responsible for the overall strategic direction of IRRS
Director, Specialized Care	Responsible for operations and strategic business decisions about IRRS
Manager, Specialized Care Data Management	Responsible for overall operations and maintenance of IRRS
Manager, Product Development	Responsible for the overall development and implementation of the IRRS project from a technical perspective
Manager, ITS Health Information Applications	Responsible for ensuring availability of technical resources and solutions for ongoing operations and enhancements of IRRS data
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

3.4 Principle 2: Identifying purposes for personal health information

CIHI collects IRRS data for purposes consistent with those identified in Section 2.2 above.

The purposes for collecting home care and facility-based LTC data are to support service providers and decision-makers in these sectors in their efforts to

- Manage access to services;
- Identify gaps between the services clients require and the care they receive;
- Assess clients/residents, plan and manage their care and monitor outcomes;
- Monitor the results of quality of care improvement initiatives;
- Compare outcomes for services provided by various organizations;
- Help identify user training requirements based on the needs of the client population;
- Improve coordination of care between hospitals that discharge vulnerable individuals and the agencies or facilities responsible for providing those individuals with services; and
- Manage the resources required to deliver services.

Below is a list of identifiers collected by IRRS and their definitions. (See Section 2.3 and Section 3.7 for more details about how CIHI manages personal health information.)

Personal (client) identifiers

- **Health Care Identification Number:** The person's health care number as assigned by their provincial or territorial government.
- **Case Record Number:** A primary identifier for a person in IRRS. It links assessments for a given person across multiple encounters in the same organization. It may be a chart number or any other unique person identifier that would meet CIHI's specifications. It cannot be the person's provincial/territorial health care identification number and must not contain the person's name, partial name, birthdate or sex. It must remain unchanged for a person with multiple admissions, returns and discharges from a single health facility or agency. It is checked against other personal identifiers (e.g., Health Care Identification Number, Birthdate) on each record to ensure the longitudinal integrity of the database.
- **Birthdate:** The year, month and day the person was born.
- **Postal Code of Usual Living Arrangement:** A 6-digit alphanumeric postal code assigned by Canada Post for the permanent dwelling in which the person/client lives or lived prior to admission.

Indigenous identifiers: Information that may identify an Indigenous individual (for more information, see First Nations, Inuit and Métis)

- **Indigenous Identity:** Self-identification as a member of an Indigenous community. Does not require proof (i.e., a status card).
- **Current Payment Sources:** The organization(s) or government program(s) responsible for paying for the services rendered by the agency caring for this person. The person may be receiving services paid for by a mix of publicly or privately funded organizations or programs.

Health facility/agency identifiers

- **Facility/Agency Identifier:** Determined at the time of IRRS implementation based on jurisdictional submission and reporting needs. This uniquely identifies the organization (e.g., facility, agency, hospital, zone, region, provincial/territorial authority) that is responsible for the client and encounter information. This organization may also be conducting the interRAI assessments.
- **Site Identifier:** Determined at the time of IRRS implementation based on jurisdictional submission and reporting needs. This uniquely identifies the organization (e.g., facility, hospital, home care office, site) that is responsible for conducting the interRAI assessments.

Free (open) text

The instruments supported in IRRS contain free-text fields to capture clinically relevant information (see list below); users could potentially enter personal health information or other sensitive information in these fields. Not all of these fields are a part of each instrument. Validation checks have been built into IRRS to prevent a client's case record number, health care identification number and birthdate from being entered into any of these fields. Regardless, data from these fields is sequestered in CIHI's analytical environment, separate from other data, to ensure that access is provided only on an approved, need-to-know basis.

- **Goals of Care — Primary Goal:** Captures the person's primary goal of care.
- **Person's Expressed Goals of Care:** Captures the person's reasons for seeking care or services. This item provides an opportunity for the person to voice their own goals so the provider can understand better what the person expects or hopes to experience and how to better individualize care. As the person's goals for care may change over time, this item is included in the initial assessment and subsequent reassessments.
- **Person self-identified gender as:** This free-text field is available when the person selects the gender option "OTH." For the interRAI HC and interRAI LTCF, if the person responds "Other," the free-text box is used to record the person's verbatim response.
- **External business identifiers (EBIs):** Identifiers generated by the vendor software if the jurisdiction is unable to use CIHI-generated identifiers for patient, encounter and assessment (questionnaire) resources. The EBIs are sent by the vendor system to CIHI to correlate with CIHI's business identifiers for the associated resources. Users can use the identifiers to correct, update or delete records. Use of these identifiers is required for facility/agency systems to clearly identify the person, encounter or assessment data being referenced.

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

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

3.6 Principle 4: Limiting collection of personal health information

CIHI is committed to the principle of data minimization. Under sections 1 and 2 of CIHI's *Privacy Policy, 2010*, CIHI collects from data providers only the information that is reasonably required for health system uses, including statistical analysis and reporting, in support of the management, evaluation or monitoring of the health care system.

HCRS and CCRS, implemented in 2005 and 2003, respectively, were developed in consultation with stakeholders from across the country and contain only those data elements determined to be necessary to achieve the goals and purposes of those databases.

IRRS is similarly limited to data elements that capture information on the client's health, cognitive and functional status; demographic and administrative information; and information on resources used in providing care and services, which are necessary to achieve the goals and purposes of IRRS, as outlined in Section 3.4.

See Section 3.7 for a description of how CIHI minimizes the collection, use and disclosure of personal health information that may be included in the limited number of free-text fields.

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

Limiting use

CIHI limits the use of the IRRS data to authorized purposes, as described in Section 3.4. These include comparative analyses within and among jurisdictions; trend analyses to assess/monitor the impact of differences in policy, practices and service delivery; and production of statistics to support planning, management and quality improvement.

CIHI staff

CIHI staff are permitted to access and use data on a need-to-know basis only, including for data processing and quality management, producing statistics and data files, and conducting analyses. All CIHI staff are required to sign a confidentiality agreement at the commencement of employment, and they are subsequently required to renew their commitment to privacy yearly.

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

The general use data files are pre-processed files that are designed specifically to support internal analytical users' needs, including the removal of the original health care number (replaced with an encrypted health care number), and full birthdate and full postal code (replaced by a set of standard derived variables). Production of the IRRS general use files is planned for 2021–2022.

The process ensures that all requests for access, including access to the IRRS data, are traceable and authorized, in compliance with Section 10 of CIHI's *Privacy Policy, 2010*. The SAS Data Access System is subject to an annual audit to ensure that staff are accessing data on a need-to-know basis. Section 3.9 includes additional information about how the various procedural and technical measures are deployed to prevent unauthorized access and otherwise secure the IRRS data.

- Users who input information at the point of care receive training, which includes how to complete and code an assessment, and how to avoid collecting personal identifiers (e.g., full or partial names, the person's health care identification number) in free-text fields. See Section 3.4 for more information about free-text fields in IRRS. Specifically for the field **Person self-identifies gender as**, IRRS coding instructions for users inform them that entries in this text-filled item must not contain any names (full or partial) or the

person's health care identification number or birthdate. For the field **Person's Expressed Goals of Care**, coding instructions direct users to not enter any names (full or partial) or the person's health care identification number, birthdate, sex or gender. For **Case Record Number**, vendor specifications include instructions that the field must not include the person's health care identification number, birthdate, sex, or full or partial names.

- CIHI conducts automated validation checks to determine whether full health care numbers, full birthdates and full 6-digit postal codes for clients have been entered in any free-text field. An assessment of free-text fields was done through CIHI's formal PSRM assessment, and mitigating strategies were put in place to minimize the collection, use, disclosure and retention of personal health information in them.
- Information collected in the free-text fields is segregated from the rest of the IRRS data. Internal access to and use of the above free-text fields is restricted. SAS analytical files used by staff in CIHI's Specialized Care department do not contain the data entries collected in these fields. Data contained in these free-text fields is available on a need-to-know basis only and must be approved by the director of Specialized Care. Further access to and use of this data by any internal CIHI system or database (see Section 3.2) requires director approval. Any release to an external third party would require a review of the fields to ensure they do not contain personal health information. This requirement is written into the standard operating procedures associated with fulfilling requests for IRRS data.

In addition, a client support tool was developed for a limited number of Specialized Care staff so that they can provide client support for data submissions and assist with vendor testing activities. This stand-alone tool limits access to data by excluding birthdates, health care numbers, postal codes and free-text fields.

Data linkage

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

Sections 14 to 31 of CIHI's *Privacy Policy, 2010* govern linkage of records of personal health information. Pursuant to this policy, CIHI permits the linkage of personal health information under certain circumstances. Data linkage within a single data holding for CIHI's own purposes is generally permitted. Data linkage across data holdings for CIHI's own purposes and all third-party requests for data linkage are subject to an internal review and approval process. When carrying out data linkages, CIHI will generally do so using consistently encrypted health care numbers. The linked data remains subject to the use and disclosure provisions in the *Privacy Policy, 2010*.

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

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

Section 24 All of the following criteria are met:

a) The purpose of the data linkage is consistent with CIHI's mandate;

b) The public benefits of the linkage significantly offset any risks to the privacy of individuals;

c) The results of the data linkage will not be used for any purpose that would be detrimental to the individuals that the personal health information concerns;

d) The data linkage is for a time-limited specific project and the linked data will be subsequently destroyed in a manner consistent with sections 28 and 29; or

e) The data linkage is for purposes of an approved CIHI ongoing program of work where the linked data will be retained for as long as necessary to meet the identified purposes and, when no longer required, will be destroyed in a manner consistent with sections 28 and 29; and

f) The data linkage has demonstrable savings over other alternatives or is the only practical alternative.

CIHI's client linkage standard

In 2015, CIHI implemented a corporate-wide client linkage standard to be used when linking records created in 2010–2011 or later, where the records include the encrypted health care number and the province or territory that issued the health care number. For the linkage of records that do not satisfy these criteria, the linkage mechanism is determined on a case-by-case basis.

Destruction of linked data

Section 28 of CIHI's *Privacy Policy, 2010* sets out the requirement that CIHI will destroy personal health information and de-identified data in a secure manner, using destruction methodologies appropriate to the format, media or device such that reconstruction is not reasonably foreseeable.

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

Return of own data

In addition to returning data to submitting facilities, Section 34 of CIHI's *Privacy Policy, 2010* establishes that CIHI may return records to the relevant ministry for data quality purposes and for purposes consistent with its mandate (e.g., for health services and population health management, including planning, evaluation and resource allocation) or as directed in the data-sharing agreement or other legal instrument The return of own data is considered a use and not a disclosure.

Limiting disclosure

As previously mentioned, information collected in free-text fields identified in Section 3.7 will be stored in a separate table in the IRRS database. Further access to this data for the purpose of disclosing it externally to any individual (e.g., external consultant), third-party researchers or interRAI under the data-sharing agreement (see Section 3.2) also requires director approval. Any disclosure would require a review of the fields to ensure they do not contain personal health information.

Data providers that submit interRAI LTCF data must sign CIHI's Electronic Reporting Service Agreement in order to access CCRS eReports. The agreement includes requirements with respect to the disclosure of health facility–identifiable information and the suppression of small cell sizes.

Third-party data requests

Customized de-identified record-level and/or aggregated data from IRRS may be requested by a variety of third parties, such as government, health care decision-makers and researchers.

CIHI administers the Third-Party Data Request Program, which establishes privacy and security controls that must be met by the recipient organization. Furthermore, as set out in sections 37 to 57 of CIHI's *Privacy Policy, 2010*, CIHI discloses health information in a manner consistent with its mandate and core functions, and CIHI data disclosures are made at the highest degree of anonymity possible while still meeting the research and/or analytical purposes of the requester. This means that, whenever possible, data is aggregated. When aggregated data is not sufficiently detailed for the intended purpose, record-level de-identified data or personal health information (in limited circumstances, for example, with individual consent) may be disclosed to the recipient on a case-by-case basis, when the recipient has entered into a data protection agreement or other legally binding instrument with CIHI. Only those data elements necessary to meet the intended purpose may be disclosed.

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

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

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

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

As noted in Section 2.2, IRRS contains the field Indigenous Identity. The disclosure of this identifier is governed by CIHI's *Policy on the Release and Disclosure of Indigenous-Identifiable Data*, which requires that any request for Indigenous-identifiable data at CIHI be accompanied by approvals from appropriate Indigenous authorities. (For more information, see *A Path Forward: Toward Respectful Governance of First Nations, Inuit and Métis Data Housed at CIHI*.)

Public release

As part of its mandate, CIHI publicly releases aggregated data only in a manner designed to minimize any risk of re-identification and residual disclosure. This generally requires a minimum of 5 observations per cell in accordance with Section 33 of CIHI's *Privacy Policy, 2010*. Aggregated statistics and analyses are made available in publications and on CIHI's website through tools such as Your Health System: In Depth and Quick Stats.

Limiting retention

IRRS 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, IRRS 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 the IRRS 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 the IRRS 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 IRRS identified 7 privacy/security risks in the areas of system registration and authentication, all of which were added to CIHI's Privacy and Security Risk Register. All risks were assessed and mitigated to a residual risk score of low in accordance with CIHI's PSRM methodology.

This PIA will be updated or renewed in compliance with CIHI's *Privacy Impact Assessment Policy*.

References

1. interRAI. Instruments overview: Home Care (HC). Accessed August 30, 2021.
2. interRAI. Instruments overview: Long-Term Care Facilities (LTCF). Accessed August 30, 2021.
3. interRAI. Instruments overview. Accessed August 30, 2021.
4. Wikipedia. Fast Healthcare Interoperability Resources. Accessed August 30, 2021.

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

53029-0524