National Rehabilitation Reporting System Privacy Impact Assessment

2022

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

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

Unless otherwise indicated, this product uses data provided by Canada's provinces and territories.

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. *National Rehabilitation Reporting System Privacy Impact Assessment, 2022*. Ottawa, ON: CIHI; 2022.

Cette publication est aussi disponible en français sous le titre *Évaluation des incidences sur la vie privée du Système national d'information sur la réadaptation, 2022*.

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

- *National Rehabilitation Reporting System Privacy Impact Assessment, 2022*

Approved by

Brent Diverty
Vice President, Data Strategies and Statistics

Rhonda Wing
Chief Privacy Officer and General Counsel

Ottawa, March 2022

Table of contents

Quick facts about the National Rehabilitation Reporting System

1. Inpatient rehabilitation is an important component in the continuum of health services. Patients receive multi-dimensional (physical, cognitive, psychosocial) diagnostic, assessment, treatment and service planning interventions to improve their function. These services are commonly inter- or multi-disciplinary in nature. The rehabilitation process helps patients return to the community following illness or injury.
2. The Canadian Institute for Health Information (CIHI) operates the National Rehabilitation Reporting System (NRS) to support the planning and management of publicly funded inpatient rehabilitation services in Canada.
3. In 1995, CIHI initiated a major project to develop and evaluate a minimum data set and grouping methodology for rehabilitation services across service settings in Canada. By 1998, CIHI had collected and analyzed a large sample of rehabilitation clinical data from more than 30 sites across Canada and had consulted with more than 350 experts and key stakeholders in the rehabilitation field. The results of the statistical analysis, the pilot site evaluations and the external field review provided solid evidence that the data set was reliable and valid for a range of adult Rehabilitation Client Groups in inpatient facilities. In 1999, a prototype NRS was implemented (a milestone for Canada in rehabilitation data standards), which transitioned into a regular production database in fall 2001.
4. As of 2020, about 100 inpatient rehabilitation facilities/organizations were submitting data to the NRS. The facilities/organizations are located in Newfoundland and Labrador, Prince Edward Island, Nova Scotia, New Brunswick, Ontario, Manitoba, Saskatchewan, Alberta and British Columbia. Also as of 2020, the NRS included more than 670,000 complete sets of admission and discharge records (i.e., episodes of care).
5. The NRS collects data about rehabilitation patients from rehabilitation facilities/ organizations. For greater comparability, the NRS groups the records according to the nature of the illness or injury requiring rehabilitation (e.g., stroke, arthritis). The records are submitted to CIHI in accordance with the NRS minimum data set and include
   - Information about the individual;
   - Information about the individual’s health characteristics;
   - Administrative data (e.g., dates of admission and discharge from rehabilitation);
   - Health facility identifiers; and
   - Health service provider identifiers.
6. The NRS uses the information it collects to produce accurate, timely and comparable information about matters such as how long patients wait to receive rehabilitation services, the effectiveness of rehabilitation services and the resources consumed while providing rehabilitation services.

7. Facilities/organizations, ministries of health, regional health authorities, researchers and the public use the information the NRS produces. The NRS provides this information in a variety of forms, such as interactive electronic reports (e.g., data tables, graphs) at the facility/organization, regional and provincial levels. The reports include a wide array of attributes and metrics to assist users in their work. NRS data also contributes to various publicly available reports (e.g., Quick Stats) that paint a picture of inpatient rehabilitation services across Canada.

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/organizations, long-term care homes, regional health authorities, medical practitioners and governments. This data includes information about health services provided to individuals, the health professionals who provide those services and the cost of the health services.

The purpose of this privacy impact assessment (PIA) is to examine the privacy, confidentiality and security risks associated with the National Rehabilitation Reporting System (NRS). This PIA, which replaces the September 2015 version, includes both a review of the 10 privacy principles set out in the Canadian Standards Association's *Model Code for the Protection of Personal Information* and how the principles apply to the NRS, as well as a look at the application of CIHI's *Privacy and Security Risk Management Framework*.

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

2 Background

2.1 Introduction to the National Rehabilitation Reporting System

Rehabilitation is an important component in the continuum of health services. Health service providers such as nurses, physiotherapists, occupational therapists and physicians help patients improve their physical and cognitive functioning through training and education. The rehabilitation process helps patients return to the community following illness or injury.

In 1995, CIHI initiated a major project to develop and evaluate a minimum data set and grouping methodology for rehabilitation services across service settings in Canada. By 1998, CIHI had collected and analyzed a large sample of rehabilitation clinical data from more than 30 sites across Canada and had consulted with more than 350 experts and key stakeholders in the rehabilitation field. The results of the statistical analysis, the pilot site evaluations and the external field review provided solid evidence that the data set was reliable and valid for a range of adult Rehabilitation Client Groups in inpatient facilities. In 1999, a prototype NRS was implemented (a milestone for Canada in rehabilitation data standards), which transitioned into a regular production database in fall 2001.

CIHI operates the NRS to support the planning and management of publicly funded inpatient rehabilitation services in Canada.[i] CIHI is a secondary data collector and relies on the submission of data originally collected by rehabilitation facilities/organizations. The data the NRS collects concerns whether and how patients' physical and cognitive functioning improves during the inpatient rehabilitation process. This information is used to produce accurate, timely and comparable information about matters such as

- How long patients wait to receive rehabilitation services;
- The effectiveness of rehabilitation services; and
- The resources consumed while providing rehabilitation services.

Facilities/organizations, ministries of health, regional health authorities, researchers and the public use the information the NRS produces. The NRS provides this information in a variety of forms, such as interactive electronic reports (e.g., data tables, graphs) at the facility/organization, regional and provincial levels. The reports include a wide array of attributes and metrics to assist users in their work. NRS data also contributes to various publicly available reports (e.g., Quick Stats) that paint a picture of inpatient rehabilitation services across Canada.

i. Rehabilitation for mental health conditions such as addictions is addressed in the *Hospital Mental Health Database PIA*.

2.2 Data collection

As of 2020, about 100 inpatient rehabilitation facilities/organizations were submitting data to the NRS. Those facilities/organizations are located in Newfoundland and Labrador, Prince Edward Island, Nova Scotia, New Brunswick, Ontario, Manitoba, Saskatchewan, Alberta and British Columbia. Most facilities/organizations submit data to the NRS voluntarily, though some facilities/organizations are required to do so by their ministry of health or regional health authority. Also as of 2020, the NRS included more than 670,000 complete sets of admission and discharge records (i.e., episodes of care).

The NRS minimum data set is targeted primarily at patients age 18 and older, though the NRS accepts data for individuals age 13 and older. For greater comparability, patient records in the NRS are grouped according to the nature of the illness or injury. These patient groups, referred to as Rehabilitation Client Groups (RCGs), are based on patient characteristics such as impairments and/or activity limitations associated with various types of conditions. A list of RCGs follows.

Rehabilitation Client Groups

- Stroke
- Brain Dysfunction
- Neurological Conditions
- Spinal Cord Dysfunction
- Amputation of Limb
- Arthritis
- Pain Syndromes
- Developmental Disabilities
- Medically Complex
- Orthopedic Conditions
- Cardiac Conditions
- Pulmonary Conditions
- Burns
- Congenital Deformities
- Other Disabling Impairments
- Major Multiple Trauma
- Debility

The 2 most commonly seen RCGs are Orthopedic Conditions and Stroke, representing more than half of all records. Most patients admitted to facilities/organizations participating in the NRS (more than 90%) are admitted from acute care units at the same hospital or from another hospital.

Each record submitted to the NRS reflects the minimum data set and includes personal identifiers/demographic information, health characteristics, administrative information, health facility identifiers, health service provider identifiers and free text fields. A full list of the data elements included in the NRS minimum data set can be found on CIHI's website.

2.3 Access management, data submission and flow for the National Rehabilitation Reporting System

Access management

Access to CIHI's secure applications is subject to CIHI's role-based access management process. This process determines access to CIHI's secure applications using established access management system (AMS) processes for granting and revoking access.

Data flows

Once authenticated through CIHI's AMS, NRS facilities/organizations submit data, which is electronically captured using specialized software, through CIHI's secure web-based systems.

At the time of processing, all submitted NRS data automatically undergoes validation and a data quality check for errors and inconsistencies against specifications outlined in the *Rehabilitation Minimum Data Set Manual*. The data processing system is internal to CIHI, with no external connection.

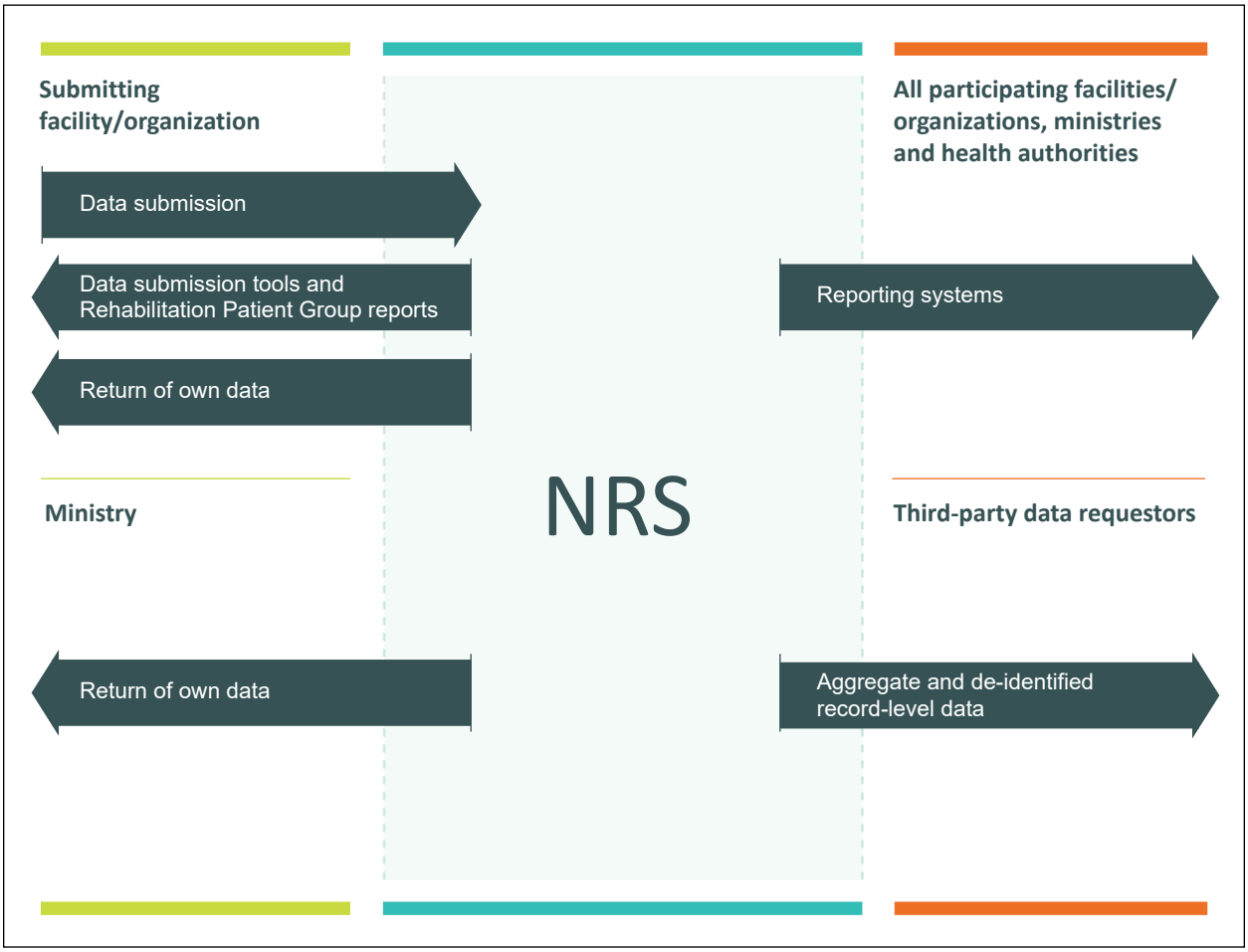
Error and validation reports generated at the time of processing are made available to the respective facility/organization via a secure web-based tool in compliance with CIHI's *Secure Information Transfer Standard*. These reports identify records (using chart numbers and admission dates) with errors; specify the number of records a facility/organization has successfully submitted; indicate the reason records were rejected or the relevant warning message; and permit the facility/organization to correct errors in the records and resubmit them to the NRS.

All records successfully processed without errors are added to the NRS, and data submitters can query the inclusion of their records using a verification audit report in a secure web-based tool. This tool returns a limited set of data elements including Chart Number, Admission Date and Discharge Date.

A de-identified copy of the NRS data set is made available in CIHI's analytical environment for use by approved CIHI staff. CIHI returns NRS data to the facility/organization that originally submitted the data, on request, as well as to the respective ministry of health on request and/or according to agreement. CIHI also discloses aggregate and de-identified record-level data to third-party requesters upon request, as well as aggregate data to the public. The figure below illustrates this data flow at a high level for the NRS.

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

Figure Overview of typical data flows for the NRS



3 Privacy analysis

3.1 Privacy and Security Risk Management Program

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

Privacy and security risks may be identified from a variety of sources, including PIAs, 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.

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

3.3 Principle 1: Accountability for personal health information

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

Organization and governance

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

Table Key positions and responsibilities

Position/group	Roles/responsibilities
Vice President, Data Strategies and Statistics	Responsible for the overall strategic direction of the NRS
Director, Specialized Care	Responsible for the overall operations and strategic business decisions of the NRS
Manager, Data Management, Specialized Care	Responsible for ongoing management of NRS data, including data quality and reporting
Chief Information Security Officer	Responsible for the strategic direction and overall implementation of CIHI's Information Security Program
Chief Privacy Officer	Responsible for the strategic direction and overall implementation of CIHI's Privacy Program
Manager, ITS Health Information Applications	Responsible for ensuring the availability of technical resources and solutions for ongoing operations and enhancements of NRS data
Manager, Product Management and Client Experience	Responsible for managing access to the web-based applications used to exchange NRS data

3.4 Principle 2: Identifying purposes for personal health information

CIHI's mandate is to deliver comparable and actionable information to accelerate improvements in health care, health system performance and population health across the continuum of care. This includes producing information about inpatient rehabilitation services to support the planning and management of publicly funded inpatient rehabilitation services in Canada. In order to fulfill these goals, CIHI collects the following types of NRS data for the purposes indicated.

Personal identifiers/demographic information

Examples include health care number, facility chart number, birthdate, postal code, sex, language, vocational status and Indigenous identity. CIHI uses this information to develop a complete picture of the care provided to the individual, by linking records that describe the different types of care provided to the individual at different times by different facilities. In order to link the individual's records, CIHI needs to know which records pertain to the individual. Accordingly, all records must include some identifying information — especially the individual's health care number. CIHI uses age (calculated using date of birth), geographic information derived from postal code, sex, language, vocational status and Indigenous identity for demographic analysis of health care services and outcomes.

Health characteristics

Examples include diagnoses and related comorbidities at admission and discharge. CIHI uses this information to evaluate the types of conditions that require rehabilitation, the quality of care provided to the individual and costs associated with treatment.

Administrative information

Examples include the dates the patient became a candidate for rehabilitation, was admitted to the facility/organization and was discharged from the facility/organization. CIHI uses this information to evaluate wait times for care and resources consumed while providing care.

Health facility identifiers

Examples include the names/codes of the hospital or residential care facility that referred the individual for rehabilitation, provided the rehabilitation or was the individual's destination following rehabilitation. CIHI uses this information to compare facilities and groups of facilities.

Health service provider identifiers

An example is the number assigned to each service provider (e.g., health professional) who contributed to the person's care. CIHI uses this information to determine the types of human resources involved in the individual's care.

Free (open) text fields

An example is project data fields. This information supports any special projects required to meet the needs of CIHI, the provinces/territories or health care facilities.

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

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

3.6 Principle 4: Limiting collection of personal health information

CIHI is committed to the principle of data minimization. Under sections 1 and 2 of CIHI's *Privacy Policy, 2010*, CIHI collects from data providers only the information that is reasonably required for health system uses, including statistical analysis and reporting, in support of the management, evaluation or monitoring of the health care system. The information necessary for these purposes that is collected by the NRS is described in Section 2.2.

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

Limiting use

CIHI limits the use of NRS data to authorized purposes, as described in sections 2.1, 2.2 and 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, which is managed through CIHI's Service Desk. This environment is a separate, secure space for analytical data files, including general use data files, where staff are required to conduct and store the outputs from their analytical work.

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

The process ensures that all requests for access, including access to NRS 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 NRS data.

Data linkage

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

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

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

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

Section 24 All of the following criteria are met:

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

Client linkage standard

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

Destruction of linked data

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

Section 29 of CIHI's *Privacy Policy, 2010* further requires that for time-limited specific projects, the secure destruction of linked data will occur within 1 year after publication of the resulting analysis or 3 years after the linkage, whichever is sooner, in a manner consistent with CIHI's *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

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

In addition to submission reports, submitting facilities/organizations may also access Rehabilitation Patient Group (RPG) Reports. Through these secure web-based reports, the user can view certain data elements in records that the facility/organization has submitted to the NRS, such as scores for cognitive and motor functioning, admission and discharge dates, and estimates of the resources consumed while providing rehabilitation services. RPG Reports identify records using chart numbers.

Upon request, CIHI will provide a facility/organization with a copy of any data it has submitted to the NRS as a return of own data. In addition to returning data to submitting facilities/ organizations, 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). The return of own data is considered a use and not a disclosure.

Limiting disclosure

NRS eReports is a secure, web-based analytical reporting tool that provides authorized users with facility-/organization-identifiable, aggregated information regarding rehabilitation services. NRS eReports is available to facilities/organizations that submit data to the NRS, ministries of health, regional health authorities and other approved organizations. The reports provide the following types of information:

- How many patients received rehabilitation for each type of health condition (e.g., stroke);
- How many days patients waited to receive rehabilitation services;
- How many days of rehabilitation services were provided;
- How much patients' physical and cognitive functioning improved through rehabilitation;
- Estimates of the resources consumed while providing rehabilitation services; and
- Patients' socio-demographic characteristics (e.g., language, vocational status), relevant to rehabilitation.

Authorized users can customize the content and appearance of the reports to suit their business needs. For example, users can customize reports to focus on

- Rehabilitation for a particular type of health condition;
- A specific rehabilitation facility/organization, or facilities/organizations of a particular size, type or region; and
- Rehabilitation activity occurring at a particular time of the year.

Before being provided with access to reports containing NRS data, users must sign a service agreement that, among other things,

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

Third-party data requests

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

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 3.4 of this PIA, the NRS contains a field for 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 Quick Stats.

Limiting retention

The NRS 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, the NRS 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 NRS 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 NRS 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 the NRS did not identify any privacy or security risks.

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

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

12020-0322