National Rehabilitation Reporting System Privacy Impact Assessment, September 2015

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

Our vision

Better data. Better decisions.
Healthier Canadians.

Our mandate

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

Our values

Respect, Integrity, Collaboration, Excellence, Innovation

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, September 2015

Approved by:

Brent Diverty
Vice President, Programs

Anne-Mari Phillips
Chief Privacy Officer & General Counsel

Ottawa – September 2015

Table of contents

Quick facts about CIHI and the National Rehabilitation Reporting System

- Rehabilitation is an important component in the continuum of health services. CIHI operates the National Rehabilitation Reporting System (NRS) in order to support the planning and management of rehabilitation services in Canada.
- The NRS collects standardized data about inpatient rehabilitation services. As of 2015, about 100 inpatient rehabilitation facilities were submitting data to the NRS. These facilities may be free-standing rehabilitation hospitals or rehabilitation units of acute care hospitals. The facilities are located in Newfoundland and Labrador, Prince Edward Island, Nova Scotia, New Brunswick, Ontario, Manitoba, Saskatchewan, Alberta and British Columbia.
- The facilities submit records to CIHI in accordance with the NRS minimum data set, which consists of data elements grouped into the following major categories: Patient Identifiers, Socio-Demographics, Administrative, Health Characteristics, and Activities and Participation. For greater comparability, records in the NRS are grouped according to nature of the illness or injury (e.g., stroke, arthritis). As of 2015, the NRS included more than 450,000 complete sets of admission and discharge records (i.e., episodes of care).
- The NRS analyzes the data it collects from the facilities and produces accurate, timely and comparable information about matters such as wait times for rehabilitation services, the effectiveness of those services and the resources consumed, regional health authorities, researchers and the public to make better decisions about rehabilitation.

1 Introduction

The Canadian Institute for Health Information (CIHI) collects and analyzes information on health and health care in Canada. Its mandate is to lead the development and maintenance of comprehensive and integrated health information that enables sound policy and effective health system management that improve health and health care. CIHI obtains data from hospitals and other health care facilities, long-term care homes, regional health authorities, medical practitioners and governments. This data includes information about health services provided to individuals, the health professionals who provide those services and the cost of the health services.

The purpose of this privacy impact assessment (PIA) is to examine the privacy, confidentiality and security risks associated with the National Rehabilitation Reporting System (NRS). This PIA, which replaces the 2009 version, includes a review of the 10 privacy principles set out in the Canadian Standards Association's *Model Code for the Protection of Personal Information*, as the principles apply to the NRS. The primary driver for this PIA is compliance with CIHI's *Privacy Impact Assessment Policy*.

2 Background

Rehabilitation is an important component in the continuum of health services. Health professionals 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.

CIHI operates the NRS to support the planning and management of publicly funded inpatient rehabilitation services in Canada. CIHI is a secondary data collector and relies on the submission of data collected originally by rehabilitation facilities. The data the NRS collects concerns 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 the following:

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

The information the NRS produces permits facilities, ministries of health, regional health authorities, researchers and the public to make better decisions about rehabilitation.

2.1 Data providers

All facilities that submit data to the NRS provide hospital-based inpatient rehabilitation services. These services may be provided in free-standing rehabilitation hospitals or within rehabilitation units of acute care hospitals. Facilities participating in the NRS are self-classified as either *general* or *specialty* facilities. This classification is specific to the NRS and is intended to facilitate comparative reporting; it is not necessarily consistent with facility classification methods used in various provinces or regions.

According to NRS definitions, a general rehabilitation facility is a rehabilitation unit or a collection of beds designated for rehabilitation purposes that are part of a general hospital offering multiple levels or types of care. A specialty rehabilitation facility is one that may provide more extensive and specialized inpatient rehabilitation services and is commonly a free-standing facility or a specialized unit within a hospital. The rehabilitation team at the facility decides which profile most closely represents its rehabilitation program(s) and categorizes itself as general or specialty when beginning submissions to the NRS.

As of 2015, about 100 inpatient rehabilitation facilities were submitting data to the NRS. Those facilities are located in Newfoundland and Labrador, Prince Edward Island, Nova Scotia, New Brunswick, Ontario, Manitoba, Saskatchewan, Alberta and British Columbia. Most facilities submit data to the NRS voluntarily, though some facilities are required to do so by their ministry of health or regional health authority.

2.2 Data collected

The NRS collects information from facilities about the extent of improvement in patients' physical and cognitive functioning during the inpatient rehabilitation process, and also collects a range of supporting information such as when a patient's rehabilitation services begin and end, estimates of the resources consumed in providing rehabilitation services, and patients' socio-demographic characteristics, relevant to rehabilitation.

The NRS minimum data set (see Section 3.5) 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. Patient groups include those with impairments, activity limitations and/or participation restrictions associated with various types of conditions, referred to as Rehabilitation Client Groups (RCGs). 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. These 2 groups represent more than half of all records. Most patients admitted to facilities participating in the NRS (more than 90%) are admitted from acute care units at the same hospital or in another hospital. As of 2015, the NRS included more than 450,000 complete sets of admission and discharge records (i.e., episodes of care).

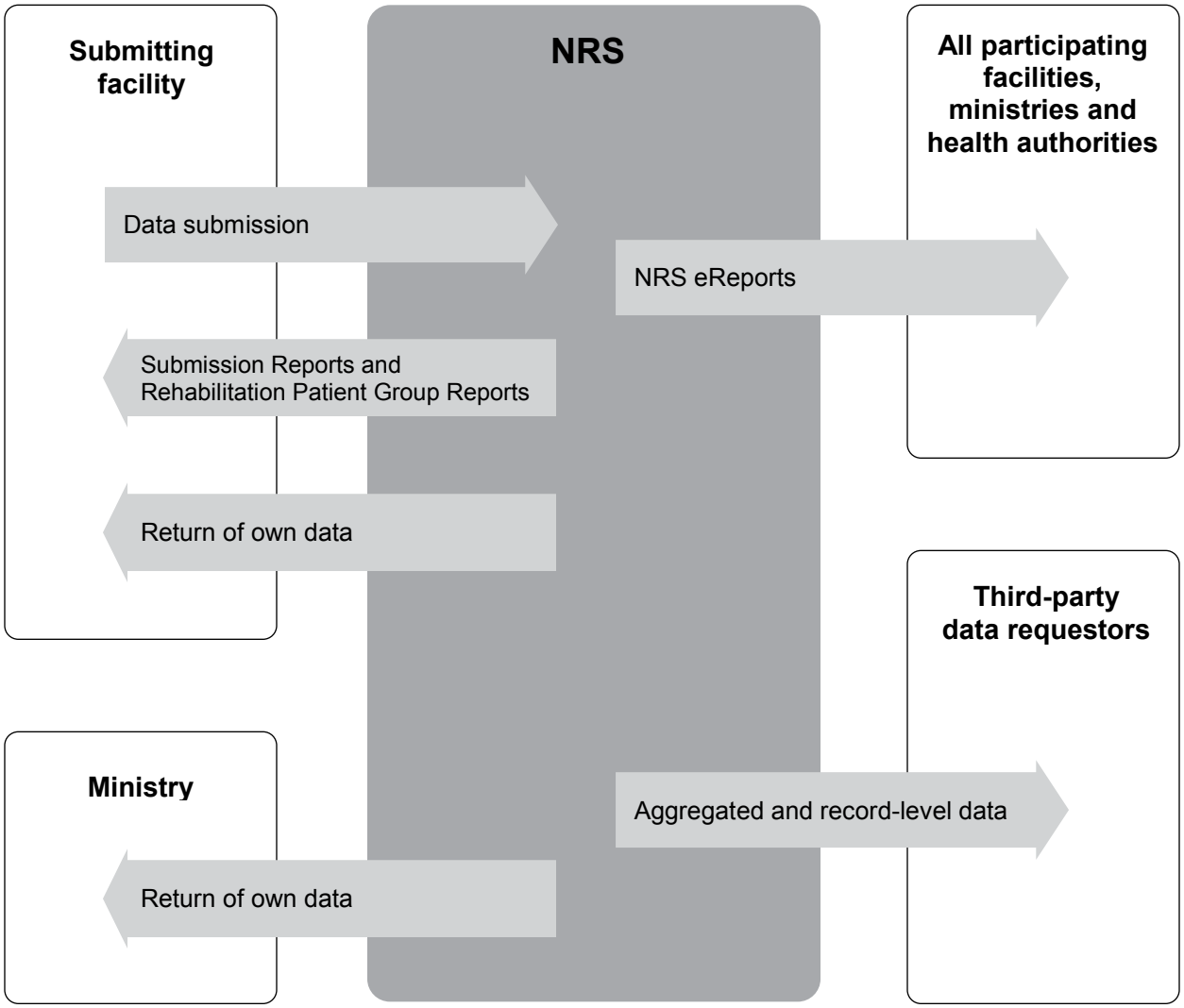
Rehabilitation for mental health conditions such as addictions are addressed in the *Hospital Mental Health Database PIA*.

2.3 Data flows

Facilities submit data to the NRS through CIHI's secure web-based data submission application. Data specifications and other associated documentation, such as file layouts, are available from CIHI. All submissions to CIHI must conform to its submission and edit specifications.

Sections 3.5 and 3.6 include a more detailed discussion of how data flows into and out of the NRS. Figure 1 illustrates the data flows at a high level.

Figure 1 NRS data flows



3 Privacy analysis

3.1 Authorities governing NRS data

General

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

Legislation

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

The following provinces and territories have enacted health information–specific privacy legislation: Newfoundland and Labrador, Nova Scotia, New Brunswick, Ontario, Manitoba, Saskatchewan and Alberta (Yukon, the Northwest Territories and Prince Edward Island are also in the process of implementing such legislation). Health information–specific privacy legislation authorizes facilities to disclose personal health information without patient consent for 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.

For 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 existing 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.

3.2 Principle 1: Accountability for personal health information

CIHI's president and chief executive officer is accountable for ensuring compliance with CIHI's Privacy Policy, 2010. CIHI has a chief privacy officer and general counsel, a corporate Privacy, Confidentiality and Security team, a 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:

Position/group	Roles/responsibilities
Vice president, Programs	Responsible for providing overall leadership and oversight regarding the acquisition, management and reporting of NRS data
Director, Methodologies and Specialized Care	Responsible for operational and strategic decisions regarding NRS data
Manager, Rehabilitation and Mental Health	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 availability of technical resources and solutions for ongoing operations and enhancements of NRS data
Manager, Central Client Services	Responsible for managing access to the web-based applications used to exchange NRS data

3.3 Principle 2: Identifying purposes for personal health information

The data the NRS collects is used to produce accurate, timely and comparable reports about inpatient rehabilitation services. This information permits facilities, ministries of health, regional health authorities, researchers and the public to make better decisions about rehabilitation. The types of data the NRS collects, and why they are required, are discussed in Section 3.5.

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

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

3.5 Principle 4: Limiting collection of personal health information

CIHI is committed to the principle of data minimization. Per sections 1 and 2 of CIHI's *Privacy Policy, 2010*, CIHI collects from data providers only 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. In accordance with this principle, the NRS collects only the information necessary to support the planning and management of publicly funded inpatient rehabilitation services in Canada.

The NRS minimum data set consists of data elements grouped into the following major categories:

- Patient Identifiers: These are data elements used to identify individual records. Patient names are never collected for the NRS.
- Socio-Demographics: Information such as full date of birth, sex, living arrangements and vocational status are collected to provide valuable information on the types of patients admitted to rehabilitation programs.
- Administrative: Data is collected on wait times for admission and discharge, service interruptions and provider types in order to better understand access to rehabilitation, factors influencing length of stay, and resource utilization.
- Health Characteristics: Diagnoses and related comorbidities at admission provide information on conditions most often seen in a rehabilitation setting and on conditions that may affect a patient's ability to progress in the rehabilitation program.
- Activities and Participation: This section of the minimum data set provides clinical data on the motor and cognitive functional abilities of rehabilitation patients. The FIM®[i] instrument is used to measure outcomes of functional independence at admission and discharge, and optionally on follow-up after discharge. It is composed of 18 items (13 motor items and 5 cognitive items) that are rated on a 7-level scale representing gradations from independent (7) to dependent (1) function, for an overall maximum score of 126 (18 items x 7). The FIM® instrument measures disability and looks at the caregiver burden associated with the level of disability. The overall FIM® instrument score can be broken down into motor and cognitive subscales to provide further detail on identifying areas of functional loss.

  In addition to the data collected using the FIM® instrument, additional cognitive elements and elements assessing instrumental activities of daily living and health status, socio-demographic, administrative, and health characteristics information are also collected for each rehabilitation patient.

A full list of data elements included in the NRS can be found on CIHI's website.

i. The FIM® instrument and impairment codes referenced herein are reproduced with permission of UB Foundation Activities, Inc. and are the property of Uniform Data System for Medical Rehabilitation (UDSMR), a division of UB Foundation Activities, Inc. The Rehabilitation Client Groups have been adapted from the impairment codes, with permission of UB Foundation Activities, Inc. The FIM® instrument is a trademark of Uniform Data System for Medical Rehabilitation, a division of UB Foundation Activities, Inc.

3.6 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 Section 3.3. 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 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.

Since 2009, data sets used for internal CIHI analysis purposes do not contain direct identifiers, such as unencrypted health card numbers. Health card numbers in an unencrypted form are available to CIHI staff on an exceptional, need-to-know basis only, subject to internal approval processes, as set out in CIHI's internal *Privacy Policy and Procedures, 2010*.

Data linkage

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

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 card numbers. The linked data remains subject to the use and disclosure provisions in CIHI's *Privacy Policy, 2010*.

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

1. The individuals whose personal health information is used for data linkage have consented to the data linkage; or
2. 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.

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 linked data, secure destruction will occur within 1 year after publication of the resulting analysis, or 3 years after the linkage, whichever is sooner, in a manner consistent with CIHI's *Information Destruction Standard*. For linked data resulting from a CIHI ongoing program of work, secure destruction will occur when the linked data is no longer required to meet the identified purposes, in a manner consistent with CIHI's *Information Destruction Standard*. This requirement applies to both data linkages for CIHI's own purposes and for third-party data requests.

Return of own data

Section 34 of CIHI's *Privacy Policy, 2010* establishes that the return of data to the facility that originally provided it to CIHI is not considered a disclosure; rather, it is considered a use. Accordingly, the NRS returns data to submitting facilities in the following contexts.

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

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

Upon request, CIHI will also provide a facility with a copy of any data the facility submitted to the NRS, as a 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 of health for data quality purposes and for purposes consistent with its mandate, for example, for health services and population health management, including planning, evaluation and resource allocation.

Limiting disclosure

Disclosures to data provider community

The NRS makes data available to the data provider community via NRS eReports, a secure, web-based, analytical reporting tool that provides users with facility-identifiable, aggregated information regarding rehabilitation services. NRS eReports is available to facilities that submit data to the NRS, ministries of health, regional health authorities and other approved organizations.

NRS eReports provides information that addresses issues such as

- How many patients received rehabilitation for each type of health condition (e.g., strokes);
- 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 in providing rehabilitation services; and
- Patients' demographic characteristics (e.g., vocational status), relevant to rehabilitation.

The reports are accessed through a secure web-based business intelligence tool that allows authorized users to view and customize reports to suit their business needs. For example, users can customize reports so as to focus on

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

Before being able to access NRS eReports, organizations must sign a service agreement with CIHI. The service agreement is signed at a senior level of the organization to ensure that the organization is aware of both its responsibilities and those of its users. The service agreement includes rules regarding issues such as

- Limiting use of the reporting system to the stated purposes;
- Prohibiting users from trying to identify an individual represented in a report;
- Restricting the publication of cell sizes less than 5;
- Ensuring information security (e.g., protecting user passwords);
- Notifying CIHI of any unauthorized access to the reporting system; and
- Establishing an Organization Contact who is responsible to identify Designated Users to CIHI's Central Client Services (CCS).

Requests for access to NRS eReports are made to CIHI's CCS group, which

- Verifies that the user is affiliated with the organization;
- Verifies, through the Organization Contact, that the requestor is a Designated User and the level of access associated with the Designated User's profile; and
- Grants the Designated User the appropriate level of access.

Each time a Designated User logs on to NRS eReports, the user must agree to terms of use which impose rules similar to those found in the service agreement.

In addition to NRS eReports, authorized users can also access aggregated, facility-identifiable NRS data through CIHI Portal, another analytical reporting tool which has included NRS data since 2011. CIHI Portal is discussed in a separate CIHI Portal PIA.

Public release of NRS data

As part of its mandate, CIHI publicly releases aggregated data only, and in a manner designed to minimize any risk of identification and residual disclosure. Aggregated statistics and analyses are made available in publications and on CIHI's website. This generally requires a minimum of 5 observations per cell.

Third-party data requests

Customized de-identified record-level and/or aggregated data from the NRS may be requested by a variety of users, such as various levels of government, health care decision-makers and researchers.

CIHI administers a third-party data request program that contains and ensures appropriate privacy and security controls within the recipient organization. Furthermore, as set out in sections 45 to 47 of CIHI's *Privacy Policy, 2010*, CIHI's 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 data that has been de-identified 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.

In 2009, CIHI adopted a complete lifecycle approach to data management. As part of that lifecycle, 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 lifecycle. 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 requestors are required to complete and submit a 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 de-identified 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.

As of January 2011, in addition to the compliance monitoring process, which leverages data captured to monitor compliance with data destruction requirements, 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.

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.

3.7 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 *Data Quality Framework*. The process of completing the framework includes numerous activities to assess the various dimensions of quality, including the accuracy of NRS data.

3.8 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 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 NRS data are highlighted below.

System security

CIHI recognizes that information is secure only if it is secure throughout its entire lifecycle: 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 card number has been removed or encrypted upon first receipt. In exceptional instances, staff will require access to original health card 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 card 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 a 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.

3.9 Principle 8: Openness about the management of personal health information

CIHI makes information available about its privacy policies, data practices and programs relating to the management of personal health information. Specifically, CIHI's *Privacy and Security Framework* and *Privacy Policy, 2010* are available to the public on its corporate website (www.cihi.ca).

3.10 Principle 9: Individual access to, and amendment of, personal health information

Personal health information held by CIHI is not used by CIHI to make any administrative or personal 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*.

3.11 Principle 10: Complaints about CIHI's handling of personal health information

As set out in sections 64 and 65 of CIHI's *Privacy Policy, 2010*, complaints about CIHI's handling of 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

There are no recommendations at this time, and privacy risks identified during this assessment have been mitigated. This PIA will be updated or renewed in compliance with CIHI's *Privacy Impact Assessment Policy*.

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
www.cihi.ca
copyright@cihi.ca

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, septembre 2015*.

Talk to Us

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

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

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

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

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

11411-1015

www.cihi.ca
At the heart of data

Canadian Institute
for Health Information

Institut canadien
d'information sur la santé