Continuing Care Reporting System Privacy Impact Assessment

December 2016
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.

All rights reserved.

The contents of this publication may be reproduced unaltered, in whole or in part and by any means, solely for non-commercial purposes, provided that the Canadian Institute for Health Information is properly and fully acknowledged as the copyright owner. Any reproduction or use of this publication or its contents for any commercial purpose requires the prior written authorization of the Canadian Institute for Health Information. Reproduction or use that suggests endorsement by, or affiliation with, the Canadian Institute for Health Information is prohibited.

For permission or information, please contact CIHI:

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

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

© 2017 Canadian Institute for Health Information


Cette publication est aussi disponible en français sous le titre Évaluation des incidences sur la vie privée du Système d'information sur les soins de longue durée, décembre 2016.
The Canadian Institute for Health Information (CIHI) is pleased to publish the following privacy impact assessment in accordance with its Privacy Impact Assessment Policy:

- Continuing Care Reporting System

Approved by:

Brent Diverty
Vice President, Programs

March 2017

Anne-Mari Phillips
Chief Privacy Officer and General Counsel
# Table of contents

Quick facts about CIHI and the Continuing Care Reporting System ........................................... 5

1 Introduction ......................................................................................................................... 6

2 Background ......................................................................................................................... 6
   2.1 Introduction to CCRS ................................................................................................. 6
   2.2 Data collection ........................................................................................................... 8
   2.3 CCRS data flow ....................................................................................................... 10

3 Privacy analysis .................................................................................................................11
   3.1 Privacy and Security Risk Management Program .................................................... 11
   3.2 Authorities governing CCRS data ............................................................................ 12
   3.3 Principle 1: Accountability for personal health information ....................................... 13
   3.4 Principle 2: Identifying purposes for personal health information ......................... 14
   3.5 Principle 3: Consent for the collection, use or disclosure of personal health information .........................................................................................................................14
   3.6 Principle 4: Limiting collection of personal health information ............................... 15
   3.7 Principle 5: Limiting use, disclosure and retention of personal health information .... 15
   3.8 Principle 6: Accuracy of personal health information ............................................... 20
   3.9 Principle 7: Safeguards for personal health information .......................................... 20
   3.10 Principle 8: Openness about the management of personal health information ....... 22
   3.11 Principle 9: Individual access to and amendment of personal health information .... 22
   3.12 Principle 10: Complaints about CIHI’s handling of personal health information .... 22

4 Conclusion .........................................................................................................................22

Appendix: Text alternative for figure .......................................................................................... 23
Quick facts about CIHI and the Continuing Care Reporting System

1. The Continuing Care Reporting System (CCRS) is a pan-Canadian database at the Canadian Institute for Health Information (CIHI) that captures standardized information regarding publicly funded continuing care services.

2. CCRS captures clinical, demographic, administrative and resource utilization data about residents of continuing care facilities; the information CCRS captures is resident-specific.

3. CCRS captures the above information from publicly funded facilities, including hospitals with continuing care beds and residential care facilities.

4. CIHI and its stakeholders determined that CCRS data standards should reflect the personal health information that clinicians have already collected, such that no additional personal health information is collected exclusively for CCRS. With these goals in mind, CIHI and its stakeholders selected the resident assessment forms (developed by interRAI) that clinicians use as the basis for the CCRS data collection standards. Clinicians collect data at various points in time before a resident’s discharge from a facility, providing CCRS with a picture of the resident’s changes over time.

5. CCRS began data collection in 2003. CCRS records are longitudinal and contain each resident’s historic record, in some cases going back to the year 1996.

6. Data captured by CCRS is used to develop accurate, timely and comparable information describing the population of residents receiving continuing care services, the services they receive and the residents’ outcomes.

7. Health service administrators, policy-makers, governments, researchers and other stakeholders rely on CCRS for the information they need to manage access to continuing care services, improve the quality of services provided and manage the resources required to deliver services.

8. The value-added information that CCRS derives is available in several ways, including Quick Stats, which are available to the public, and CCRS eReports, which are available to organizations that submit data to CCRS, ministries of health, regional health authorities and other approved organizations.
1 Introduction

The Canadian Institute for Health Information (CIHI) collects and analyzes information on health and health care in Canada. Its mandate is to deliver comparable and actionable information to accelerate improvements in health care, health system performance and population health across the continuum of care. CIHI obtains data from hospitals and other health care facilities, long-term care homes, regional health authorities, medical practitioners and governments. This data includes information about health services provided to individuals, the health professionals who provide those services and the cost of health services.

The purpose of this privacy impact assessment (PIA) is to examine the privacy, confidentiality and security risks associated with the Continuing Care Reporting System (CCRS). This PIA, which replaces the 2012 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 CCRS. The primary driver for this PIA is compliance with CIHI’s Privacy Impact Assessment Policy.

2 Background

2.1 Introduction to CCRS

CCRS is a pan-Canadian database that captures standardized information on publicly funded continuing care services. CCRS was developed to fulfill an identified need for consistent, comparable data about continuing care services in Canada, for accountability and quality purposes. Data collection began in 2003. CCRS records are longitudinal and contain each resident’s historic record, in some cases going back to the year 1996.

CCRS captures a range of information regarding continuing care services, such as

- Data reflecting the results of clinicians’ assessments of residents (e.g., resident’s health, cognitive and functional status, care currently received);
- Resident demographic information (e.g., sex, birthdate, postal code of residence before admission to facility);
- Administrative data (e.g., dates of admission to and discharge from a continuing care facility, information regarding transfers to and from other levels of care such as hospitals);
- Resources used in providing continuing care services to the resident; and
- Information regarding the facility providing continuing care services to the resident.
CCRS captures the above information from 2 types of organizations:

- Hospitals with continuing care beds, commonly known as extended, auxiliary, chronic or complex care beds; and
- Residential care facilities, commonly known as nursing homes, personal care homes or long-term care facilities.

The organizations that submit data to CCRS are either publicly owned or privately owned but receive public funding in return for providing care to the public.

In recent years, new models of delivering continuing care have emerged. For example, in some provinces/territories, publicly funded home care programs provide services in assisted or supportive living environments that do not offer 24-hour nursing care. This activity is currently out of scope for CCRS.

All of the clinical data CCRS captures has already been collected by clinicians during the process of providing care; the data is subsequently shared with CIHI. Clinicians collect data at various points in time before discharge from the facility, providing CCRS with a picture of the resident’s changes over time.

The data captured by CCRS is used to develop accurate, timely and comparable information describing the population of residents receiving continuing care services, the services they receive and the residents’ outcomes. Health service administrators, policy-makers, governments, researchers and other stakeholders rely on CCRS for the information they need to manage access to continuing care services, improve the quality of services provided and manage the resources required to deliver services.
2.2 Data collection

Data collection standards

CIHI and its stakeholders, such as the Home and Continuing Care Advisory Committee that represents ministries of health, determined that the data that CCRS captures should reflect the personal health information that clinicians have already collected, such that no additional personal health information is collected exclusively for CCRS (as discussed in Section 3.6). With these goals in mind, CIHI and its stakeholders selected the resident assessment forms that clinicians use as the basis for the CCRS data collection standards. Specifically, CIHI and its stakeholders selected the Resident Assessment Instrument–Minimum Data Set (RAI-MDS) 2.0 tool developed by interRAI as the basis for the CCRS data collection standard. The RAI-MDS 2.0 is an electronic tool that helps clinicians gather comprehensive and standardized clinical information; this tool is used by all organizations that submit data to CCRS.

Relying upon interRAI’s RAI-MDS 2.0 tool as the basis for CCRS data collection means that the data elements CCRS collects, particularly the clinical data elements, have been carefully selected based on the best available evidence of utility and specificity. Each version of the RAI-MDS tool represents the results of rigorous research and testing to establish the reliability and validity of data elements collected, resident outcome measures, case-mix classifications used to categorize residents based on resource use and quality of care indicators.

Data CCRS ultimately captures

The CCRS data set is a subset of the information that clinicians collect using the RAI-MDS 2.0. The CCRS data set includes both resident clinical and demographic information, and consists of roughly 500 data elements.

Some CCRS data elements provide administrative information regarding the facility providing the care (e.g., type, size, location). This information is used to help evaluate the quality and utilization of services. Facilities typically submit such facility-related information to CCRS annually instead of with each resident record.

A full list of the data elements CCRS captures can be found on CIHI’s website.

---

1. interRAI is a collaborative network of researchers in more than 30 countries committed to improving care for persons who are disabled or medically complex.
Data transfer tools

Organizations may submit data to CCRS in the following ways (by order of CIHI’s preference):

- Through CIHI’s web-based applications or server-to-server application;
- Via courier of an electronic medium containing encrypted and password-protected data; or
- By emailing encrypted and password-protected data.

CIHI uses the same tools when transferring data to a recipient. For information on CIHI’s transfer of data to a recipient, see Section 3.7 under the heading “Return of own data.”

Deriving value-added information

CCRS uses the assessment data it captures to derive value-added information, such as summary measures of residents’ status and clinical outcomes, quality of care indicators and case-mix designations used to categorize residents based on resource use. The value-added information that CCRS derives is available via eReports and Quick Stats, which are discussed in Section 3.7 under the heading “Limiting disclosure.”
2.3 CCRS data flow

2 types of organizations submit data to CCRS: hospitals with continuing care beds and residential care facilities. In some cases, organizations submit data directly to CCRS. In other cases, organizations submit data to a ministry or health authority that submits consolidated data to CCRS. The following figure illustrates CCRS data flow at a high level.
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 (PSRM) 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, and monitoring and reviewing privacy and security risks.

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

- **High:** High probability of risk occurring and/or controls and strategies are not reliable or effective.
- **Medium:** Medium probability of risk occurring and/or controls and strategies are somewhat reliable or effective.
- **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 how serious a risk is. 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 Senior Management Committee on behalf of the corporation.
3.2 Authorities governing CCRS 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 health systems, including statistical analysis and reporting. Data providers are responsible for meeting the statutory requirements in their respective jurisdictions, where applicable, at the time the data is collected.

The following provinces and territories have enacted health information–specific privacy legislation: Newfoundland and Labrador, Nova Scotia, New Brunswick, Ontario, Manitoba, Saskatchewan, Alberta, Yukon and the Northwest Territories (Prince Edward Island is 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, CCRS data is governed by CIHI’s *Privacy Policy, 2010*, legislation in the jurisdictions and 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.
3.3 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 CCRS data in terms of privacy and security risk management:

<table>
<thead>
<tr>
<th>Position/group</th>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vice president, Programs</td>
<td>Overall operations and strategic direction of CCRS</td>
</tr>
<tr>
<td>Director, Methodologies and Specialized Care</td>
<td>Strategic and operational decisions to ensure the continued successful development of CCRS</td>
</tr>
<tr>
<td>Manager, Home and Continuing Care Standards and Support Manager, Home and Continuing Care Data Management</td>
<td>Ongoing development and operation of CCRS</td>
</tr>
<tr>
<td>Chief information security officer</td>
<td>Strategic direction and overall implementation of CIHI’s Information Security Program</td>
</tr>
<tr>
<td>Chief privacy officer</td>
<td>Strategic direction and overall implementation of CIHI’s Privacy Program</td>
</tr>
<tr>
<td>Manager, ITS Health Information Applications</td>
<td>Ensuring availability of technical resources and solutions for ongoing operations and enhancements of CCRS data</td>
</tr>
<tr>
<td>Manager, Central Client Services</td>
<td>Managing access to the web-based applications used to exchange CCRS data</td>
</tr>
</tbody>
</table>
3.4 Principle 2: Identifying purposes for personal health information

CCRS captures a range of information regarding publicly provided or funded continuing care services, including assessment data, data regarding the services provided to residents, demographic information and administrative data.

CCRS uses this data to develop accurate, timely and comparable information describing the population of residents receiving continuing care services, the services they receive and the residents' outcomes. This information is available in various forms to a range of stakeholders, as discussed in Section 3.7 under the heading “Limiting disclosure.”

Health service administrators, policy-makers, governments, researchers and other stakeholders use the information CCRS provides to conduct their work, such as

- Managing access to continuing care services;
- Monitoring the results of quality of care improvement initiatives;
- Comparing resident outcomes for continuing care services provided by various organizations;
- Improving coordination of care between hospitals that discharge vulnerable individuals and the continuing care facilities responsible for providing those individuals with services; and
- Managing the resources required to deliver continuing care services.

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. 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 health care systems.

CCRS collects the only personal health information necessary to facilitate the goals described in Section 3.4, such as managing continuing care services.

The data elements containing personal health information (i.e., the clinical data elements) that CCRS captures have already been collected by clinicians in the course of providing care. Therefore, no personal health information is collected exclusively for CCRS. In this way, CCRS limits the collection of personal health information.

Also, CCRS does not capture all the personal health information that clinicians collect in the course of providing care. Instead, CCRS captures only the data elements that CIHI and its stakeholders identified as necessary for the purposes of CCRS. For example, facilities collect the names of residents and caregivers. These data elements are not necessary for the purposes of CCRS and are not captured by CCRS. In this way, CCRS limits the capture of personal health information.

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

**Limiting use**

CIHI limits the use of CCRS data to authorized purposes, such as those described in Section 3.4. 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.

Data sets used for internal CIHI analytical purposes do not contain direct identifiers, such as unencrypted health care numbers. This limits access to personal health information. Health care numbers in an unencrypted form are available to CIHI staff on an exceptional, need-to-know basis only, subject to approval processes as set out in CIHI’s internal *Privacy Policy and Procedures, 2010*. 
Data linkage

Data linkages are performed between data from CCRS 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 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 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.

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: encrypted health care number, the province/territory that issued the health care number and year of birth. 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 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 data linkages for both CIHI’s own purposes and third-party data requests.

Return of own data

Section 34 of CIHI’s Privacy Policy, 2010 establishes that the return of data to the organization that originally provided it to CIHI is not considered a disclosure; rather, it is considered a use. Accordingly, CCRS returns data to submitting organizations in the following contexts.

A submitting organization can access secure web-based submission reports that identify records that were not accepted by CCRS and that describe the errors associated with the records. Records are referenced by chart number instead of health care number.

Upon request, CIHI will also provide an organization with a copy of any data the organization submitted to CCRS, as a return of own data.

In addition to returning data to submitting organizations, 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

CCRS eReports

CCRS eReports is a secure, web-based, analytical reporting tool that provides aggregated information regarding resident populations, continuing care services provided and resident outcomes (e.g., quality of care indicators). CCRS eReports identifies the region in which the continuing care services were delivered (and for 1 jurisdiction indicates the specific organization that provided the care).

CCRS eReports is available to organizations that submit data to CCRS, ministries of health, regional health authorities and other approved organizations.

Before being provided with access to CCRS eReports, users must sign a service agreement that includes requirements with respect to the disclosure of health facility-identifiable information and the suppression of small cell sizes.

Public release of CCRS data

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. 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.

Third-party data requests

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

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.
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 receiving 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.

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.

**Data provided to interRAI**

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 supply interRAI with an annual copy, in de-identified form, of the data collected with interRAI assessment forms and captured by CCRS. The flow of de-identified data from CIHI to interRAI is governed by non-disclosure/confidentiality agreements that are signed annually.

**Limiting retention**

CCRS 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, CCRS 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 CCRS 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 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 CCRS 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 specifies 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 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.
3.10 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](http://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*, 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 CCRS did not identify any privacy risks.
Appendix: Text alternative for figure

Figure: CCRS data flow

This figure shows the flow of data in to and out of CCRS.

Regarding the data flow in to CCRS, data submitter organizations submit data to CCRS. The data submitter organizations are hospitals with continuing care beds and residential care facilities. In some cases, data submitter organizations submit data to CCRS directly. In other cases, data submitter organizations submit data via an intermediary such as a ministry of health or health authority, which then forwards the data to CCRS.

Data flows out of CCRS in several ways, as follows:

1. CCRS provides submission reports to data submitter organizations that submit data to CCRS. If a data submitter organization submits data to CCRS via an intermediary, then the submission reports flow from CCRS via the same intermediary to the data submitter organization.
2. CCRS provides data submitter organizations with a copy of the original data that they submit to CCRS. Again, if the data submitter organization submits the data via an intermediary, then the data flows back to the data submitter organization via the same intermediary.
3. CCRS makes reports available through CIHI’s reporting systems. The reports are available to organizations, ministries and health authorities.
4. CCRS discloses aggregate and de-identified record-level data to third-party data requestors.
5. CCRS releases aggregate data to the public.