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

Canadian Institute for Health Information
495 Richmond Road, Suite 600
Ottawa, Ontario K2A 4H6
Phone: 613-241-7860
Fax: 613-241-8120
cihi.ca
copyright@cihi.ca

Quick facts about the Continuing Care Reporting System

1.1.T8.8999 5(ee Rg S)11.699ystem (CCRS) i th ctu-Canadian databases standardized informubtyp yp publicly

2 Background

CCRS is a pan-Canadian database that captures standardized information on continuing care services provided by public facilities as well as private facilities contracted by the government WR SURYLGH FDUH WR WKH SXEOLF &&56 ZDV GHYHORSHG WR comparable data about continuing care services in Canada. Data collection began in 2003.

CCRS captures the above information from 2 types of facilities:

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

In some provinces/territories, publicly funded home care programs provide services in assisted RU VXSSRUWLYH OLYLQJ HQYLURQPHQWV WKDW GDWD LV RXW RI VFRSH IRU out of scope for CCRS.

Facilities collect data in the process of providing care and then submit data to CCRS. Facilities collect data at various points in time before a resident's discharge from the facility, providing CCRS with a picture of the resident's changes over time.

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 their outcomes.

2.1 Data collection

Facilities use a standardized assessment instrument to gather comprehensive clinical information from residents. This instrument, the Resident Assessment Instrument–Minimum Data Set 2.0 (RAI-MDS 2.0), is developed by interRAI — a collaborative network of

3 Privacy analysis

3.1 Privacy and Security Risk Management Program

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

Privacy and security risks may be identified from a variety of sources. For example, one identified risk event may be 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 have deficiencies.
- Medium: Medium probability of risk occurring, and/or controls and strategies are somewhat reliable or have deficiencies.
- Low: Low probability of risk occurring and/or reliable controls and strategies exist.

The likelihood and impact of the identified risk are used to assess the level of low, medium or high, where the 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

3.2 Authorities governing CCRS data

General

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

Privacy legislation

&,+, LV D VHFRQGDU\ GDWD FROOHFWRU RI KHDOWK LQIRUPDWL
management of the health system, including statistical analysis and reporting. Data providers
DUH UHVSRQVLEOH IRU PHHWLQJ WKH VWDWXWRU\ UHTXLUHPHQ
applicable, at the time the data is collected.

3.3 Principle 1: Accountability for personal health information

&,+,¶V SUHVLGHQW DQG FKLHI H[HFXWLYH R ̂FHU LV DFFRXQWDE
CIHI's *Privacy Policy, 2010* &,+, KDV D FKLHI SULYDF\ R ̂FHU DQG JHQHUD
3ULYDF\ &RQ¿GHQWLDOLW\ DQG 6HFXULW\ &RPPLWWHH D *RYH
Board of Directors, and an external chief privacy advisor.

Organization and governance

7KH IROORZLQJ WDEOH LGHQWL¿HV NH\ LQWHUQDO VHQLRU SRV
in terms of privacy and security risk management:

Table Key positions and responsibilities

Position/group	Responsibilities
Vice President, Data Strategies and Statistics	Responsible for the overall strategic direction of CCRS
Director, Specialized Care	Responsible for the overall operations and strategic business decisions of CCRS
Vice President, Data Strategies and Statistics Director, Specialized Care	Responsible for overall operations and maintenance of CCRS
Chief Information Security Officer	Responsible for the strategic direction and overall implementation of CIHI's Information Security Program
Chief Privacy Officer	Responsible for the strategic direction and overall implementation of CIHI's Privacy Program

3.4 Principle 2: Identifying purposes for personal health information

CIHI's mandate is to deliver comparable and actionable information to accelerate improvements in health care, health care systems' performance, and population health across the continuum of care — and this includes producing information about publicly funded continuing care services LQ RUGHU WR VXSSRUW WKH SODQQLQJ DQG PDQDJHPHQW RI WKH these goals, CIHI collects the following types of CCRS data for the purposes indicated.

Personal identifiers

Health facility identifiers

Examples include the names/codes of the facility that provides continuing care to the individual. CIHI uses this information to compare facilities and groups of facilities.

Free (open) text fields

Fields are designed to permit the collection of unstructured data. For example, special SURMHFW ¿HOGV PD\ SHUPLW WKH FDSWXUH RI LQIRUPDWLRQ Q WKH SURYLQFHV WHUULWRULHV RU KHDOWK FDUH IDFLOLWLHV intended to contain personal health information; CIHI regularly evaluates the risk of a facility HQWHULQJ SHUVRQDO KHDOWK LQIRUPDWLRQ H J KHDOWK FD WDNHV VWHSV WR DGGUHVV WKLV ULVN H J FKHFNLQJ WKHVH UHVWULFWLQJ LQWHUQDO DQG H[WHUQDO DFFHVV WR VXFK ¿HO are currently being evaluated using CIHI's Privacy and Security Risk Management Program, discussed in Section 3.1.

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.

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

Limiting use

Clients

CIHI limits the use of CCRS data to authorized purposes, as described in sections 2.1
DQG DERYH 7KHVH LQFOXGH FRPSDUDWLYH DQDO\VHV ZLWK
DQDO\VHV WR DVVHVV PRQLWRU WKH LPSDFW RI GL‡HUHQFHV L
and production of statistics to support planning, management and quality improvement.

CIHI staff

&,+, VWD‡ DUH SHUPLWWHG WR DFFHVV DQG XVH GDWD RQ D QHH
GDWD SURFHVVLQJ DQG TXDOLW\ PDQDJHPHQW SURGXFLQJ VWD
DQDO\VHV $OO &,+, VWD‡ DUH UHTXLUHG WR VLJQ D FRQ¿GHQWL
of employment, and they are subsequently required to renew their commitment to privacy yearly.

6WD‡ DFFHVV WR WKH 6$6 DQDO\WLFDO HQYLURQPHQW LV SURY
Data Access process managed through CIHI's Service Desk. This environment is a separate,
VHFXUH VSDFH IRU DQDO\WLFDO GDWD ¿OHV LQFOXGLQJ JHQH
to conduct and store the outputs from their analytical work.

7KH JHQHUDO XVH GDWD ¿OHV DUH SUH SURFHVVHG ¿OHV WKDV

Data linkage

Data linkages are performed between the CCRS data and other CIHI data sources. While this S R W H Q W L D O O \ F D X V H V J U H D W H U U L V N R I L G H Q W L ¿ F D W L R Q R I D V W H S V W R U H G X F H W K H U L V N V H J E \ U H P R Y L Q J S D W L H Q W L G transaction numbers).

Sections 14 to 31 of CIHI's *Privacy Policy, 2010* govern the 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 R Z Q S X U S R V H V D Q G D O O W K L U G S D U W \ U H T X H V W V I R U G D W D O

Limiting disclosure

CIHI provides comparative CCRS eReports to all data providers on a quarterly basis. These reports provide data aggregated at facility, provincial and national levels, allowing facilities to benchmark data over time and compare themselves with other similar service providers. Facilities also receive quarterly case-mix reports, including a report containing personal health information about the facility's own data submissions.

Before being provided with access to CCRS eReports, organizations must sign CIHI's *Electronic Reporting Services Agreement* which, among other things,

- Restricts use of the data to non-commercial purposes limited to the organization's internal management, data quality, planning, research, analysis or evidence-based

Agreement with interRAI

CIHI signed a licence agreement with interRAI, a network of researchers and practitioners committed to improving care for persons who are disabled or medically complex. This licence grants CIHI an exclusive right to use interRAI's assessment instrument in Canada for the purposes of national statistical reporting. The licence agreement also commits CIHI to supply LQWHU5$, ZLWK DQ DQQXDO FRS\ LQ GH LGHQWL¿HG IRUP RI W assessment instrument — including data submitted to CCRS. Accordingly, CIHI provides LQWHU5$, ZLWK GH LGHQWL¿HG GDWD IURP &&56 XQGHU D GDWD the purposes for which interRAI may use the data (e.g., to develop assessment forms), along with interRAI's responsibilities to protect the data.

Public release

As part of its mandate, CIHI publicly releases aggregated data only in a manner designed WR PLQLPL]H DQ\ ULVN RI UH LGHQWL¿FDWLRQ DQG UHVLGXDO 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.

Limiting retention

CCRS forms part of CIHI's data holdings and, consistent with its mandate and core functions, &,+, UHWDLQV VXFK LQIRUPDWLRQ IRU DV ORQJ DV QHFHVVDU\

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.

6LPLODU WR RWKHU &,+, GDWD KROGLQJV &&56 LV VXEMHFW W 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 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 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 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, JXLGHOLQHV DQG RSHUDWLQJ SURFHGXUHV UHÀHFW EHVW SUDI UHFRUGV PDQDJHPHQW IRU WKH SURWHFWLRQ RI WKH FRQ¿GHQ 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 FRQGXFWHG ZLWK WKH XVH RI GH LGHQWL¿HG UHFRUG OHYHO EHHQ UHPRYHG RU HQFU\SWHG XSRQ ¿UVW UHFHLSW ,Q H[FHSV 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:

•

Appendix

Text alternative for figure

)LJXUH &&56 GDWD ÀRZ

&&56 GDWD ÀRZV DUH DV IROORZV

1. 7KH IDFLOLW\ VXEPLWV UHFRUGV WR &&56 ,Q VRPH FDVHV W
2. CCRS makes available submission reports to help the facility correct errors in the records (e.g., missing data elements).
3. A copy of the records as accepted by CCRS, as well as certain reports that include personal health information, are available to the facility and the ministry.
4. Via CCRS eReports, CIHI provides record-level and aggregate data to facilities that submit data to CCRS and to the ministry. CIHI provides aggregate data to health authorities.
5. &&56 GLVFORVHV GH LGHQWL¿HG UHFRUG OHYHO DQG DJJUHJD
6. CCRS releases aggregate data to the public.