Canadian Joint Replacement Registry

Privacy Impact Assessment

March 2021

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

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

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

How to cite this document:
Canadian Institute for Health Information. *Canadian Joint Replacement Registry Privacy Impact Assessment, March 2021*. Ottawa, ON: CIHI; 2021.

Cette publication est aussi disponible en français sous le titre *Registre canadien des remplacements articulaires : évaluation des incidences sur la vie privée, mars 2021*.

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

- *Canadian Joint Replacement Registry, March 2021*

Approved by

Brent Diverty
Vice President, Data Strategies and Statistics

Rhonda Wing
Chief Privacy Officer and General Counsel

Ottawa, February 2021

Table of contents

Quick facts about CJRR

1. The Canadian Joint Replacement Registry (CJRR), maintained by the Canadian Institute for Health Information (CIHI), is a national medical registry that collects patient-specific information (clinical, surgical and prosthesis) on hip and knee replacement surgeries performed in Canada. Nationally, CJRR's coverage is 72% as of 2019–2020, and reporting is mandatory in several provinces.
2. CJRR began in 2001 as an initiative championed by CIHI and the Canadian Orthopaedic Association. The registry is guided by the external CJRR Advisory Committee, which includes orthopedic surgeons, government representatives, and representatives of allied health professional associations and not-for-profit organizations. The committee provides guidance and advice to CIHI about CJRR, either directly or through the establishment of temporary working groups (e.g., scientific working group).
3. The goals of CJRR are to improve the quality of care and clinical outcomes of hip and knee replacement patients, to improve the quality of surgical practices and to study the risk factors that affect outcomes of joint replacement procedures.
4. CJRR data is submitted to CIHI from health facilities or from regional health authorities, provincial registries or ministries of health through the CJRR electronic file system or — as of 2018–2019 — through CIHI's Discharge Abstract Database (DAD).

Note: This privacy impact assessment (PIA) does not cover privacy, confidentiality and security risks associated with the DAD. That information can be found in the Clinical Administrative Databases PIA on CIHI's website.

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 the health services.

The purpose of this privacy impact assessment (PIA) is to examine the privacy, confidentiality and security risks associated with the Canadian Joint Replacement Registry (CJRR). This PIA replaces the 2017 version. It 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 CJRR. It also looks 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.

Major changes since the 2017 PIA include

- Transitioning CJRR data submission from surgeons to health facilities, regional health authorities, provincial registries or ministries of health; and
- Decommissioning the CJRR web-based tool. Data providers can submit via electronic files to CJRR or CIHI's Discharge Abstract Database (DAD).

Note: This PIA does not cover privacy, confidentiality and security risks associated with the DAD. That information can be found in the Clinical Administrative Databases PIA on CIHI's website.

2 Background

2.1 Introduction to CJRR

CJRR is a pan-Canadian source of information about hip and knee replacements. It was launched in 2001 as a collaborative effort between CIHI and the Canadian Orthopaedic Association. CJRR was established to record and analyze clinical information and outcomes of primary and revision hip and knee replacements over time to improve care for patients who receive these procedures.

The registry is guided by the pan-Canadian CJRR Advisory Committee, which includes orthopedic clinical leaders and representatives of government and non-government organizations (e.g., Canadian Orthopaedic Nurses Association, Arthritis Society). Participation in the registry was voluntary at first. Several jurisdictions have since mandated reporting to CJRR, where data is collected by health facilities under the premise that they meet their data collection, use and disclosure rules and responsibilities, including those related to consent and notification. Data on joint replacement procedures is increasingly used by jurisdictions to measure access and quality, and to inform resource allocation.

Currently, CJRR's goals are to

- Work with jurisdictions to expand CJRR prosthesis coverage to 90% nationally;
- Improve the quality of care and clinical outcomes of hip and knee replacement patients;
- Reduce revision rates; and
- Support prosthesis monitoring activities and procurement functions in Canada.

Currently, more than 137,000 hip and knee replacement procedures are performed annually in Canada, representing 2 of the 3 most common inpatient surgeries by volume in Canada.[1]

2.2 Data collection

CJRR collects the following patient-level data on hip and knee replacements performed in acute inpatient and day surgery settings in Canada:

- Patient demographics;
- Surgeon and facility information;
- Surgery details, such as type of replacement (primary or revision procedure), type of primary procedure, joint side, diagnosis grouping or reason for revision; and
- Prosthesis details, including implant and cement identifiers (manufacturers/names, product/lot numbers).

Direct identifiers (personal health information)

The following direct personal identifiers are collected in CJRR (see Section 3.4 for the purposes of collecting them):

Patient

- First and last names
- Full date of birth
- Health care number and jurisdiction issuing health care number

Note: As of 2021–2022, CJRR will no longer collect patient names.

Physician (surgeon)

- First and last names

Indirect personal identifiers (patient)

The following indirect personal identifiers about patients are collected in CJRR:

- Gender
- Postal code
- Chart number

Health facility identifiers

The following health facility identifiers are collected in CJRR:

- Facility name
- Facility number

2.3 Access management, data submission and flow for CJRR

All CJRR data flows in and out of CIHI through secure web-based applications. Data providers can submit CJRR data directly to the CJRR electronic file system or through the DAD. See the figure below for an illustration of the high-level data flows for CJRR. (For information about DAD data flows that supplement CJRR data, refer to the Clinical Administrative Databases PIA.)

CJRR data that is captured in local hospital or vendor-based information systems is submitted to CIHI in the form of flat ASCII files directly from

- Facilities;
- Vendors on behalf of facilities;
- The relevant health authority;
- A provincial registry; or
- The ministry of health accountable for the facility/facilities.

Access to CIHI's secure applications is subject to CIHI's role-based access management process, which is managed by CIHI's Client Engagement and Support (CES) department. CES manages access to CIHI's secure applications using established access management system (AMS) processes for granting and revoking access.

Once authenticated through CIHI's AMS, CJRR data providers can log in on CIHI's website, access the applications they are authorized to access and submit record-level data that has been electronically captured using specialized software, through CIHI's secure web-based electronic Data Submission Services (eDSS).

At the time of processing, all submitted CJRR data automatically undergoes validation and a data quality check for errors and inconsistencies against specifications outlined in the *CJRR Minimum Data Set Manual* and Vendor Specification Package. 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 data providers through Operational Reports via the Common Data Dissemination Services, in compliance with CIHI's *Secure Information Transfer Standard*. These reports identify records with errors, specify the number of records a data provider has successfully submitted, indicate the reason records were rejected or the relevant warning message, and permit the data provider to correct errors in the records and resubmit them to CJRR.

Following the data quality checks and corrections, names (e.g., patient names) and/or direct identifiers (e.g., unencrypted health care numbers) are removed from the data set before it moves into CJRR's production database. Afterward, a complete copy of the CJRR data set is uploaded to CIHI's SAS analytical environment, where it is made available to approved CIHI staff for CIHI purposes (see Section 3.7 for more details).

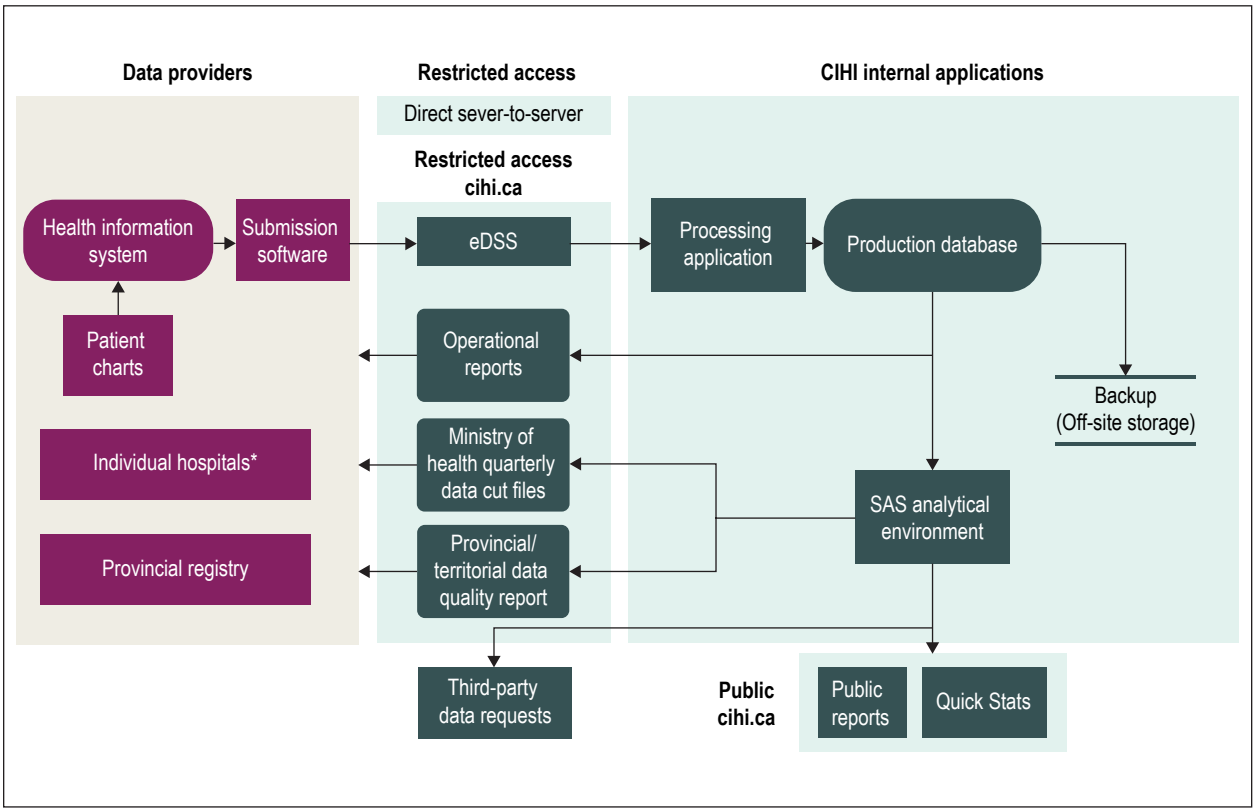
CIHI returns CJRR data to the data provider that originally supplied it, as well as to the respective ministry of health. CIHI also discloses aggregate and record-level data to third-party requesters and aggregate data to the public. The figure below is a high-level illustration of the data flows for CJRR.

Once data has been successfully submitted, processed and stored in CJRR, staff are able to access the data through CIHI's SAS analytical environment, which is managed through a centralized SAS data access process in alignment with CIHI's policies for data access.

Data flows

All CJRR data flows in and out of CIHI through a secure web-based application (see the figure).

Figure Overview of CJRR data flows



Note

* Some provinces submit CJRR data through the DAD. Please refer to the Clinical Administrative Databases PIA for more information.

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. 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 CJRR 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, CJRR 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

CJRR is guided by its Advisory Committee, which includes orthopedic surgeons and representatives from provincial ministries of health, the Canadian Orthopaedic Association, the Canadian Orthopaedic Nurses Association and the Arthritis Society.

Functional responsibility for CJRR falls under the Acute and Ambulatory Care Information Services branch at CIHI.

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

Table Key positions and responsibilities

Position/group	Roles/responsibilities
CJRR Advisory Committee	The external CJRR Advisory Committee — which includes orthopedic surgeons and representatives of governments, allied health professional associations and not-for-profit organizations — provides guidance and advice to CIHI on CJRR, either directly or through the establishment of temporary working groups (e.g., scientific working group).
Vice president, Data Strategies and Statistics	The vice president is responsible for the overall strategic direction of CJRR.
Director, Acute and Ambulatory Care Information Services	The director is responsible for the overall operations and strategic business decisions of CJRR. They ensure CJRR's continued successful development and manage the strategic relationship with the CJRR Advisory Committee and other stakeholders.
Manager, Joint Replacement Registry, Patient-Reported Outcomes and Experiences	The manager is responsible for management oversight of CJRR operations and projects. They support the CJRR Advisory Committee and consult both internally and with external CJRR stakeholders as appropriate.

Position/group	Roles/responsibilities
Program lead, CJRR	The program lead coordinates operational and analytical activities related to the functioning of CJRR and serves as the main day-to-day contact for stakeholders. They ensure the timely delivery of results and services that satisfy business and user requirements.
Chief information security officer	This person is responsible for the strategic direction and overall implementation of CIHI's Information Security Program.
Chief privacy officer	This person is responsible for the strategic direction and overall implementation of CIHI's Privacy Program.
Manager, ITS Health Information Applications	This manager is responsible for ensuring the availability of technical resources and solutions for ongoing operations and enhancements of CJRR data.

3.4 Principle 2: Identifying purposes for personal health information

CIHI collects only the personal health information that is required to achieve the goals of CJRR (see Section 2.1) once the purpose has been identified in consultation with appropriate stakeholders. The purposes are clearly stated in the CJRR program documentation. For example, below is a list of data elements collected by CJRR and the rationale for their collection. (See Section 2.3 and Section 3.7 for more details about how CIHI manages personal health information and privacy-sensitive variables.)

Personal health information (direct personal identifiers)

- **Patient first and last names** are used for second-level verification only if needed (e.g., to identify and remove patient and procedure duplicates). See Section 3.6 for changes regarding the collection of patient name as of 2021–2022.
- The patient's **provincial health care number** is collected to facilitate accurate identification, which enables linkage of their primary and revision surgery data as well as linkage to other hospitalization or rehabilitation data for longitudinal follow-up or a more comprehensive picture of related health care visits (where available).
- **Surgeon name** is collected to assign a unique CJRR-specific surgeon identification number (Surgeon ID) associated with the hip or knee replacement procedure. See Section 3.7 for changes regarding limiting the use of surgeon name as of 2021–2022.

Privacy-sensitive variables

- **Birth date** is collected to analyze the effects of age on surgery.
- **Patient home postal code** is collected to determine patient province or territory of residence and to enable aggregate calculations, such as distance from residence to hospital where surgery occurred.

Other sensitive variables

- **Gender** is collected to identify gender differences in patient outcomes.
- **Chart number** may be used to identify patients and procedures and for follow-up with hospitals on data quality–related issues.
- **Diagnosis and surgical details** are used to describe the patient population and to conduct analyses to help inform health service performance questions, such as relationships between diagnoses and surgical details and outcomes, and their relationships to the types of prostheses used.

Only information relevant to the goals of CJRR is gathered. The *CJRR Minimum Data Set Manual* lists data elements and describes their purpose. This document is revised yearly and is publicly available on CIHI's website.

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 health care systems.

In accordance with this principle, CJRR collects only the information necessary to achieve the goals and purposes of CJRR, as outlined in Section 3.4.

The *CJRR Minimum Data Set* implemented on April 1, 2012, was developed in consultation with the CJRR Advisory Committee and in accordance with the standards recommended by International Society of Arthroplasty Registries (ISAR).

As of 2018–2019, CJRR hip and knee prosthesis data can be submitted to either the DAD or CJRR. Patient name is not collected in the DAD, so as of 2021–2022, CJRR will stop collecting patient name as well. Access to historical CJRR data containing patient names is governed by Section 10 of CIHI's *Privacy Policy and Procedures, 2010*.

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

Limiting use

Clients

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

CIHI

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

Staff access to the SAS analytical environment is provided through CIHI's centralized SAS data access process managed through CIHI's Service Desk. This environment is a separate, secure space for the storage of general use data and other analytical data files, where staff can 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; the pre-processing includes removing personal health information (e.g., unencrypted health care number) and privacy-sensitive variables (e.g., date of birth, full postal code), which are replaced by a set of standard derived variables (e.g., patient's full birth date is removed and a derived age variable is added). The process ensures that all requests for access, including access to the CJRR data, are traceable and authorized, in compliance with Section 10 of CIHI's *Privacy Policy, 2010*. The SAS data access process 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 the CJRR data.

Section 3.4 identifies that CJRR collects surgeons' first and last names. These are mandatory elements used to uniquely assign a CJRR-specific Surgeon ID and are required for the CJRR system to accept the record. Once assigned, both the surgeon name and the CJRR Surgeon ID are stored in the production database. As of 2021–2022, only the CJRR Surgeon ID will be accessible in the SAS analytical environment. Access to surgeon name is governed by Section 10 of CIHI's *Privacy Policy and Procedures, 2010*.

Data linkage

Data linkages are performed between the CJRR data and other CIHI data sources, particularly the DAD and the National Ambulatory Care Reporting System. 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 the 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, medium 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 *Secure 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 *Secure Destruction Standard*. These requirements apply to data linkages both for CIHI's own purposes and for third-party data requests.

Return of own data

When ministries of health request own data cuts, they are usually provided in SAS format; however, another file format (e.g., CSV) may be provided based on the clients' needs. CIHI uses secure electronic file transfer processes to disseminate these data files using industry standard, encrypted, secure socket layer (SSL) sessions.

CJRR also returns own data to data providers in the form of Submission Reports for purposes of data quality and correction (see Section 2.3). CJRR disseminates these reports to data providers using CIHI's Operational Reports, in a manner that complies with CIHI's *Secure Information Transfer Standard*.

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 (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.

Third-party data requests

Customized record-level and/or aggregated data from CJRR 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.

CIHI disseminates data files to third-party requestors in a manner that complies with its *Secure Information Transfer Standard* (i.e., via the Data Dissemination Tool [DDT]). CJRR uses the DDT for one-way transmissions (i.e., CIHI sends to data providers) of a variety of electronic files (e.g., data files, reports, bulletins).

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 annually 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.

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.

Limiting retention

CJRR 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.

The collection of CJRR data began in 2001. Paper forms were the original method of submitting CJRR data; however, this practice stopped for procedures performed on or after April 1, 2013. In 2012, CIHI made the decision to retain CJRR paper records for 5 years. As of 2019, all CJRR paper forms have been securely destroyed in accordance with CIHI's *Secure Destruction Policy* and *Secure Destruction Standard*.

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, CJRR 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 CJRR data.

3.9 Principle 7: Safeguards for personal health information

CIHI's Privacy and Security Framework

CIHI has developed a Privacy and Security Framework to provide a comprehensive approach to enterprise privacy and security management. Based on best practices from across the public, private and health sectors, the framework is designed to coordinate CIHI's privacy and security policies and to provide an integrated view of the organization's information management practices. Key aspects of CIHI's system security with respect to the CJRR 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 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 CJRR did not identify any privacy or security risks.

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

Reference

1. Canadian Institute for Health Information. *Hip and Knee Replacements in Canada: CJRR Annual Statistics Summary, 2018–2019*. 2020.

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

23888-0321