Canadian Joint Replacement Registry

Privacy Impact Assessment

June 2017
Canadian Joint Replacement Registry

PRIVACY IMPACT ASSESSMENT

(June 2017)

Approved by:

Brent Diverty
Vice President, Programs

Anne-Mari Phillips
Chief Privacy Officer & General Counsel

Ottawa – June 2017
# Table of contents

Quick facts about the Canadian Joint Replacement Registry .............................................................. 6

1 Introduction ..................................................................................................................................... 7

2 Background ................................................................................................................................... 8
    2.1 Introduction to CJRR ........................................................................................................... 8
    2.2 Data collection ..................................................................................................................... 9
    2.3 CJRR data flow .................................................................................................................... 10
    2.4 Access management .......................................................................................................... 13

3 Privacy analysis .......................................................................................................................... 15
    3.1 Privacy and Security Risk Management Program ............................................................. 15
    3.2 Authorities governing CJRR data ....................................................................................... 16
    3.3 Principle 1: Accountability for personal health information ............................................. 17
    3.4 Principle 2: Identifying purposes for personal health information ..................................... 19
    3.5 Principle 3: Consent for the collection, use or disclosure of personal health information .......................................................... 20
    3.6 Principle 4: Limiting collection of personal health information .......................................... 20
    3.7 Principle 5: Limiting use, disclosure and retention of personal health information .......... 21
    3.8 Principle 6: Accuracy of personal health information ......................................................... 26
    3.9 Principle 7: Safeguards for personal health information .................................................... 26
    3.10 Principle 8: Openness about the management of personal health information ................. 28
    3.11 Principle 9: Individual access to, and amendment of, personal health information .......... 28
    3.12 Principle 10: Complaints about CIHI’s handling of personal health information ............. 29

4 Conclusion .................................................................................................................................... 29

Appendix: Text alternative for figure .................................................................................................. 30
Quick facts about the Canadian Joint Replacement Registry

1. The Canadian Joint Replacement Registry (CJRR), maintained by the Canadian Institute for Health Information (CIHI), is a national registry that collects patient-specific information (clinical, surgical and prosthesis) on hip and knee replacement surgeries performed in Canada.

2. CJRR began in 2001 as an initiative championed by CIHI and the Canadian Orthopaedic Association. The registry is guided by a pan-Canadian Advisory Committee, with membership consisting of orthopedic clinical leaders, as well as government, non-governmental organization and patient representatives.

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 surgeons, health facilities or regional health authorities/provincial registries/ministries of health through secure web-based applications (electronic files or via the CJRR web tool). Submission to CJRR is mandated in several provinces and voluntary in others.
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 (RHAs), 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 CIHI’s Canadian Joint Replacement Registry (CJRR). It updates the previous PIA report published in September 2010 and includes a review of the status of a recommendation made in the report about CJRR’s retention and disposal practices of paper data collection forms. The PIA 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 they apply to CJRR, and the application of CIHI’s Privacy and Security Risk Management Framework (see also Section 3.1 of this PIA). The primary driver for this PIA is compliance with CIHI’s Privacy Impact Assessment Policy.
2  Background

2.1  Introduction to CJRR

The Canadian Joint Replacement Registry, maintained by CIHI, is a national registry that collects patient-specific information (clinical, surgical and prosthesis) on hip and knee replacement surgeries performed in Canada. It is a longitudinal database that allows for joint replacement patients to be followed over time to monitor their revision rates and outcomes.

CJRR began in May 2001 as an initiative championed by CIHI and the Canadian Orthopaedic Association. The registry is guided by a pan-Canadian Advisory Committee, with membership consisting of orthopedic clinical leaders, as well as government, non-governmental organization (NGO) and patient representatives. At the beginning, participation in the registry was voluntary; however, over time, 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, the goals of CJRR are to

- Improve the quality of care and the clinical outcomes of hip and knee replacement recipients;
- Improve the quality of surgical practices; and
- Study the risk factors that affect outcomes of joint replacement procedures.

CJRR augments hospitalization and demographic information contained in CIHI’s Discharge Abstract Database (DAD), Hospital Morbidity Database (HMDB) and National Ambulatory Care Reporting System (NACRS). CJRR collects additional information on the products that are implanted in joint replacement recipients. Together, these databases provide comprehensive surgical information on these procedures.

Currently, more than 117,000 hip and knee replacement procedures are performed annually in Canada.
2.2 Data collection

CJRR collects patient-identifiable record-level data on hip and knee replacement procedures in Canada. A record is defined as a hip or knee procedure performed on one side. Therefore, if a patient has more than one procedure performed during 1 hospitalization, or has surgery on both the left and right sides during 1 operation, these situations are represented as 2 records for CJRR, whereas they would be 1 record in DAD, HMDB and NACRS.

As of April 2012, CJRR implemented the collection of data based on a significantly streamlined minimum data set that aligns with standards recommended by the International Society for Arthroplasty Registries (ISAR) (see the CJRR Minimum Data Set Manual for a list of all data elements).

Data collected in CJRR can be grouped into the following categories:

- Patient information (e.g., name, date of birth, gender, postal code, health care number, chart number);
- Clinical (surgical) information (e.g., joint type, procedure type, side, diagnosis, revision reason);
- Clinical (implant) information (e.g., components, manufacturer, product number, lot number);
- Surgeon information (e.g., name, date the surgeon joined CJRR); and
- Facility information (e.g., facility name, facility number).

CJRR also assigns a number of unique identifiers to assist with internal data management and data quality activities. Examples of such identifiers include

- Patient ID — used to uniquely identify patients;
- Surgeon ID — used to uniquely identify the surgeon who performed the joint replacement, which allows for the tracking of any surgeon across facilities and provinces;
- Surgeon–Patient ID — used to uniquely identify surgeon and patient combinations; and
- Record ID — used to uniquely identify procedure, patient and surgeon combinations.
2.3 CJRR data flow

The figure on page 12 illustrates the data flow for CJRR, which is described in the text that follows.

CJRR data flows in from 3 types of data providers: surgeons, health facilities and RHAs/provincial registries/ministries of health. Data can be submitted to CIHI directly from surgeons who perform hip and knee replacement surgeries, from facilities where hip and knee replacement surgeries are performed, or from the relevant health authority, provincial registry or ministry of health accountable for the facility/facilities (or from a commercial vendor on their behalf).

All CJRR data flows in and out of CIHI through secure web-based applications. To access any of these secure applications, users must be authorized through CIHI’s Central Client Services (see Section 2.4 Access management).

All users adhere to quarterly deadlines for data submission. Data providers can submit CJRR data to CIHI using 1 of 2 methods:

1. **Electronic data file submission**
   Data providers enter the necessary CJRR patient information in local hospital- or vendor-based information systems, then submit flat ASCII files that meet CJRR and CIHI standards. Data is submitted through CIHI’s electronic Data Submission Services (eDSS), which allows for the secure transmission of large data files from the user (i.e., data provider) to CIHI. This typically is the preferred option for large-volume facilities or facilities with their own or a third-party vendor system.

2. **CJRR Web-Based Data Submission and Reports Tool**
   Data providers enter the necessary CJRR information in a record-by-record manner directly into the web tool — a secure, stand-alone web-based system that is provided to CJRR users who do not have a vendor or information system in which to enter and store CJRR data locally. It is not designed to interface with any hospital information system. This typically is the preferred option for small- to medium-volume facilities and individual surgeon offices in situations where IT resources and capabilities for CJRR data capture are limited.

   For their own data, authorized users of the CJRR web tool are able to
   - View and create patient data;
   - View, create and update procedure data;
   - Download in Microsoft Excel format (with an additional approval step); and
   - Generate reports in Adobe PDF format.
All data submitted to CJRR undergoes a data quality check for errors and inconsistencies against specifications outlined in the CJRR Minimum Data Set Manual (file and web) and the Vendor Specification Package (file only). Edit checks are performed automatically by the system upon submission of data.

For electronic file submission users, Submission Reports are generated and made available to data providers via CIHI’s Operational Reports/Common Document Dissemination Service (CDDS) in compliance with CIHI’s Secure Information Transfer Standard. These reports identify records with errors and 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.

For web tool users, validation of the data submitted through the tool is performed at the point of entry when the user attempts to save the data or proceed to the next data entry page. Data deletions and corrections to patient demographic data can be made only by contacting assigned CJRR staff directly, who will make corrections using the internal web tool application. A limited number of CJRR staff have approved access to CJRR data with patient personal identifiers such as names and health card numbers.

Following the data quality check and correction activities, a de-identified copy of the CJRR data set is made available through CIHI’s analytical environment for use by approved CIHI staff.
Figure Overview of CJRR data flow
2.4 Access management

CIHI's Central Client Services (CCS) department is mandated to provide first-tier support to data providers regarding access to CIHI's electronic products and services. Prior to granting access, CIHI determines whether it needs to enter into an agreement with the client. The criteria for determining whether an agreement is needed are based, in part, on the following:

- The applications themselves that need to be accessed and the nature of the activity;
- The sensitivity of the data being accessed;
- The volume of personal health information being returned; and
- Whether health facility–identifiable information by name is being disclosed.

As previously indicated, data providers have 2 options to electronically submit the required information: CIHI's eDSS and CJRR's web tool.

2.4.1 Access to CIHI's eDSS

Authorized users are required to set up a CIHI profile. Once it has been authenticated, users can log in on CIHI's website and, from the My Services page, access the applications they are authorized to access, such as eDSS and CDDS.

2.4.2 Access to the CJRR web-entry form

Access permissions are managed by CIHI's CCS through established Access Management System (AMS) processes for granting and revoking access. The process of granting access permissions to the CJRR web tool is a coordinated effort between data providers (“clients”), the CJRR team and CCS. The approach used to restrict access to authorized users is role-based access control.

The key components of the AMS process include the following:

1. Clients
   - Entering into a service agreement with CIHI, where appropriate;
   - Assigning a designated organization contact (facility- and RHA-based submissions only); and
   - Identifying designated users through the organization contact (facilities/RHAs) or the signatory surgeon (surgeon-based submissions only).
2. CCS

- Authenticating access requests from designated users by
  - Verifying that designated users are affiliated with the correct organization;
  - Contacting the appropriate organization contact to verify the designated user and obtaining approval from the organization contact; and
  - Granting the appropriate access privileges following authentication.

3. The CJRR team auditing the emails generated by AMS Listener (see below) following CCS granting access to users.

AMS Listener

AMS Listener is an optional notification feature developed to further reduce the risk of unauthorized access to CIHI’s restricted services. Manual audits are triggered when access is granted to a new user of the CJRR web tool or when changes are made to an existing user’s access privileges. Program area staff monitor the alert emails sent by the AMS application. If staff suspect or identify that an incorrect type of access was granted, they immediately alert CCS to disable access and send an email to incident@cihi.ca in compliance with CIHI’s Privacy and Security Incident Management Protocol.

Access to CJRR’s web tool requires participating data providers (“clients”) to sign CIHI’s Secure Electronic Reporting Services Agreement (facilities) and CJRR Schedule, or a User Agreement for Surgeons and Designated Users. The signatories and organizational contact may then designate selected employees to access the CJRR web tool on their behalf. Through the use of AMS, CCS can grant granular levels of access as needed, such as to specific surgeons within specific hospitals. The access granted in AMS reflects what the end user is able to view, create and update in the web tool. Users are also granted either the Submitter or Viewer role, which will determine whether the user has full read/write permissions or view-only access (i.e., may not create or update information). Designated users can also be allowed to download cuts of their own data, with permission granted only under an additional, separate approval process (see Table 1 for user roles and access permissions for the CJRR web tool).

---

i. CIHI’s Secure Electronic Reporting Services Agreement: As an employee or permitted contractor of the client (e.g., hospital, health authority or region), the client identifies its designated users, who will have access to records of all surgeons in the client’s facility(ies), as listed in the schedule to the service agreement.

ii. CIHI’s User Agreement for Surgeons and Designated Users: As the client, the surgeon identifies his/her designated users, as listed in the schedule to the agreement, who will have access only to records submitted on behalf of the surgeon at the facility where the surgery was performed.
### Table 1  User roles and access permissions for the CJRR web tool

<table>
<thead>
<tr>
<th>Role of designated user</th>
<th>Description of access permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Submitter</td>
<td>• View, enter, update data</td>
</tr>
<tr>
<td></td>
<td>• Run reports</td>
</tr>
<tr>
<td>Viewer</td>
<td>• View data</td>
</tr>
<tr>
<td></td>
<td>• Run reports</td>
</tr>
<tr>
<td>Own data cut</td>
<td>• Download Own Data Cut report</td>
</tr>
</tbody>
</table>

### 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]*, *[Privacy and Security Risk Management Methodology]* and (an updated) Privacy and Security Risk Register. 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, for example, 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 (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 assessed as low or the untreated/residual risk is accepted by CIHI’s Senior Management Committee on behalf of the corporation.

3.2 Authorities governing CJRR data

General

CIHI adheres to its Privacy Policy, 2010, as well as to legislation in the jurisdictions and data-sharing agreements with the provinces and territories (which are discussed in this section).

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, 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 purposes of health system use, provided that certain requirements are met. For example, CIHI is recognized as a prescribed entity under Ontario’s Personal Health Information Protection Act, 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, CJRR data is governed by CIHI’s Privacy Policy, 2010, legislation in the provinces/territories, 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.

As previously indicated in Section 2.4.2, access to CJRR’s web tool requires participating data providers (“clients”) to sign CIHI’s Secure Electronic Reporting Services Agreement and CJRR Schedule (facilities), or a User Agreement for Surgeons and Designated Users. These agreements are signed at a senior level of the organization or by the surgeon, respectively, to ensure that they are aware of both its responsibilities and those of its users. The service agreements include rules regarding issues such as

- Limiting use of the reporting system to the stated purposes;
- Ensuring information security (e.g., protecting user passwords);
- Notifying CIHI of any unauthorized access to the reporting system; and
- Establishing an organization contact who is responsible for identifying designated users to CIHI’s CCS (facilities only).

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 is made up of members including orthopedic surgeons and representatives from provincial ministries of health, the Canadian Orthopaedic Association, the Canadian Orthopaedic Nurses Association and the Arthritis Society of Canada, as well as a patient representative.
Functional responsibility for CJRR falls under the Acute and Ambulatory Care Information Services branch at CIHI. Table 2 identifies key internal positions with responsibilities for CJRR in terms of privacy and security risk management.

<table>
<thead>
<tr>
<th>Position/group</th>
<th>Role/responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>CJRR Advisory Committee</td>
<td>The external CJRR Advisory Committee, composed of orthopedic surgeons, as well as government, NGO and patient representatives, provides guidance and advice to CIHI on CJRR either directly or through the establishment of temporary working groups (e.g., Scientific Working Group).</td>
</tr>
<tr>
<td>Vice President, Programs</td>
<td>The vice president is responsible for the overall operations and strategic direction of CJRR.</td>
</tr>
<tr>
<td>Director, Acute and Ambulatory Care Information Services</td>
<td>The director is responsible for strategic and operational decisions about CJRR, ensuring its continued successful development and managing the strategic relationship with the CJRR Advisory Committee and other stakeholders.</td>
</tr>
<tr>
<td>Manager, Joint Replacement and Multiple Sclerosis Registries</td>
<td>The manager is responsible for management oversight of CJRR operations and projects. The manager supports the CJRR Advisory Committee and consults both internally and with external CJRR stakeholders as appropriate.</td>
</tr>
<tr>
<td>Program Lead, CJRR</td>
<td>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. He or she ensures the timely delivery of results and services that satisfy business and user requirements.</td>
</tr>
<tr>
<td>Chief Information Security Officer</td>
<td>The chief information security officer is responsible for the strategic direction and overall implementation of CIHI’s Information Security Program.</td>
</tr>
<tr>
<td>Chief Privacy Officer</td>
<td>The chief privacy officer is responsible for the strategic direction and overall implementation of CIHI’s Privacy Program.</td>
</tr>
<tr>
<td>Manager, Product Management Data Acquisition</td>
<td>The manager is responsible for ensuring the availability of technical resources and solutions for ongoing operations and enhancements of CJRR data.</td>
</tr>
<tr>
<td>Manager, Central Client Services</td>
<td>The manager is responsible for managing access to CIHI’s web-based applications, such as the CJRR web tool.</td>
</tr>
</tbody>
</table>
3.4 Principle 2: Identifying purposes for personal health information

CIHI collects only personal health information required for achieving the goals of CJRR (see Section 2.1), including the purposes that have been identified in consultation with appropriate stakeholders. The purposes are clearly stated in the CJRR program documentation. For example, here is the rationale for CJRR's collection of the following personal health information:

- **Provincial health card number** is collected to facilitate accurate identification of a patient to enable linkage of a patient’s 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).
- **Birth date** is collected to analyze the effects of age at surgery.
- **Gender** is collected to identify gender differences in patient outcomes.
- **Patient home postal code** is collected to determine patient province of residence and enable aggregate calculations, such as distance from residence to hospital where surgery occurred.
- **First and last name** are used only for second-level verification if needed (e.g., to identify and remove patient and procedure duplicates).
- **Chart number** may be used to identify patients/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. An instruction manual for CJRR for data providers (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 as part of the CJRR data collection process or involve itself in the consent process. 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.

For data providers that submit data to CJRR via the web tool, CIHI relies on the signatory to the User Agreement (surgeon agreement or facility agreement) to have taken the necessary steps to obtain authority to designate user(s) in accordance with the rules that apply in the organization (i.e., facility) where his/her surgeries are performed and where data collection and submission occurs.

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

The 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 the ISAR. It is intended to complement information held in CIHI’s DAD, HMDB and NACRS.
3.7 Principle 5: Limiting use, disclosure and retention of personal health information

Limiting use

CIHI limits the use of CJRR data to authorized purposes, as described in Section 3.4. These include conducting comparative analyses within and among jurisdictions, and trend analyses to assess/monitor the impact of differences in policy, practices and service delivery; and producing statistics to support planning, management and quality improvement. CIHI staff are permitted to access and use data on a need-to-know basis only, including for data processing and quality management, producing statistics and data files, and conducting analyses. All CIHI staff are required to sign a confidentiality agreement at the commencement of employment, and they are subsequently required to renew their commitment to privacy yearly.

Data sets used for internal CIHI analysis purposes do not contain direct identifiers, such as names or unencrypted health card numbers. They are removed from records before being moved to CJRR’s analytical environment (see Section 2.3 Data flow). Health card numbers in an unencrypted form and other direct identifiers are available to authorized CIHI staff on an exceptional, need-to-know basis only, subject to internal approval processes, as set out in CIHI’s Privacy Policy and Procedures, 2010. An example of needing access to unencrypted health card number is for the purpose of preparing a return of own data file for a client.

Data linkage

Data linkages are performed automatically within the CJRR system, as it is a longitudinal database. When additional records for CJRR are added to the database, they are linked to existing records by assigning matching unique patient identification numbers, which are generated by CJRR by matching submitted health card number, health card issuing authority, date of birth and gender.

Data linkages are performed between CJRR data and other CIHI data sources. While this potentially causes greater risk of identification of an individual, CIHI undertakes mitigating steps to reduce the risk.
Sections 14 to 31 of CIHI’s *Privacy Policy, 2010* govern linkage of records of personal health information. Pursuant to this policy, CIHI permits the linkage of personal health information under certain circumstances. Data linkage within a single data holding for CIHI’s own purposes is generally permitted. Data linkage across data holdings for CIHI’s own purposes and all third-party requests for data linkage are subject to an internal review and approval process. When carrying out data linkages, CIHI will generally do so using consistently encrypted health card numbers. The linked data remains subject to the use and disclosure provisions in 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:

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

**Return of own data**

Section 34 of CIHI’s *Privacy Policy, 2010* establishes the return of data to the relevant ministry of health for data quality purposes and for purposes consistent with their mandate — for example, 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.

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

For facilities and/or surgeons that request own data, the data can be accessed through the CJRR web tool. The CJRR web tool is classified as a high-risk system in view of the sensitive record-level personal health information it contains, specifically patient name and health care number. Therefore, it is critical that users access only information for which they have authorization. In addition to the involvement of CCS in controlling access (as described in *Section 2.4 Access management*), CJRR staff obtain director-level approval, in compliance with CIHI’s internal processes set out in *Privacy Policy and Procedures, 2010*, for all user requests to download files of their own data. For users who require regular complete files of data throughout the year, director-level block approval can be obtained, which authorizes continuous access to the web tool’s Own Data Cut functionality for the current fiscal year.
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. Alternately, electronic file submitters may register for the CJRR web tool and request access to the Own Data Cut functionality.

**Limiting disclosure**

**Public release of CJRR data**

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

**Third-party data requests**

Customized de-identified record-level and/or aggregate data from CJRR 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 requestor. This means that, whenever possible, data is aggregated. When aggregate 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.

To ensure that consistent processes are used for the de-identification of data, CIHI’s third-party data request program has developed a series of forms and checklists that are available to staff who process third-party record-level data requests.

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 requestors are required to submit a written request. 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 of the publication of cell sizes less than 5; and
- The use of 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, a server-to-server application).iii

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 confirm that they are continuing to comply with their obligations as set out in the data request form and data protection agreement signed with CIHI.

**Limiting retention**

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. Submitted CJRR paper forms are 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. All paper records previously submitted by data providers are stored in locked cabinets within CIHI’s secure premises in compliance with CIHI’s *Secure Information Storage Standard*. In the September 2010 CJRR PIA, the following recommendation was made:

**Recommendation:** CJRR should review the practices around retention of paper questionnaires and, in consultation with Records Management, establish a retention/disposal schedule that takes into account any legal requirements or restrictions and redress mechanisms. CJRR should dispose of documents that no longer have a specific purpose and do so in a way that prevents improper or unauthorized use, access, copying, modification or disclosure and is in accordance with CIHI’s policies and procedures.

---

iii. DDT allows for one-way transmission (i.e., CIHI sends to data providers) a variety of electronic files (e.g., data files, reports, bulletins) and in varying formats (e.g., ACCDB, CSV, DOC, EXE, MDB, PDF, TXT, XLS, ZIP).
This recommendation was accepted and addressed. A decision was made to retain CJRR paper records for 5 years. As of February 2017, all CJRR paper forms that are older than 5 years have been securely destroyed in accordance with CIHI’s Secure Destruction Policy and Information Destruction Standard, and will continue to be destroyed on an ongoing basis.

Section 6 of CIHI’s Privacy Policy, 2010 informs staff that they may retain personal health information and de-identified data, regardless of format or media, for as long as necessary to meet the identified purposes.

Data providers are permitted to retain their own data and CJRR’s analytical products in accordance with their organization’s own record retention policies.

### 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.

### 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 provide an integrated view of the organization’s information management practices. Key aspects of CIHI’s system security with respect to 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 disposition. 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. In exceptional instances, staff will require access to original health care numbers. Section 10 of CIHI’s Privacy Policy, 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 communication about CIHI’s privacy and security policies and procedures. 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. 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 on www.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 person making the inquiry or complaint.

4 Conclusion

This PIA summarizes CIHI’s assessment of the privacy implications of CJRR. No privacy risks were identified in this assessment. This PIA will be updated or renewed in compliance with CIHI’s Privacy Impact Assessment Policy.
Appendix: Text alternative for figure

Data can be input to CJRR electronically in 2 ways: through CIHI’s data file submission method or through CJRR’s web tool.

All data submitted to CJRR undergoes a data quality check for errors and inconsistencies before being processed and integrated into the CJRR database.

Data is validated 2 ways:

- For electronic file submission users, processed data — in the form of submission reports — is returned to the respective providers (those who originally submitted the data) via CIHI’s secure Common Document Dissemination Service (CDDS).
- For web tool users, validation of the data submitted through the tool is performed at the point of entry when the user attempts to save the data or proceed to the next data entry page.

Data output from the CJRR database can be used in 2 ways:

- Processed data is used by CJRR staff to fulfill third-party data requests and to produce public reports, such as the annual report, Analysis in Brief reports, data quality reports and Quick Stats.
- Additionally, data files are provided to selected ministries of health per an agreed-upon schedule.