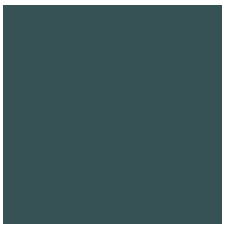


CIHI
ICIS

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

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

Ottawa, February 2021

Table of contents

Quick facts about CJRR

1. The Canadian Joint Replacement Registry (CJRR), maintained by the Canadian Institute

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)
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.

- 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

Note:
the DAD. That information can be found in the Clinical Administrative Databases PIA on CIHI's website.

CJRR data that is captured in local hospital or vendor-based information systems is submitted

- Facilities;
- Vendors on behalf of facilities;
- The relevant health authority;
- A provincial registry; or
-

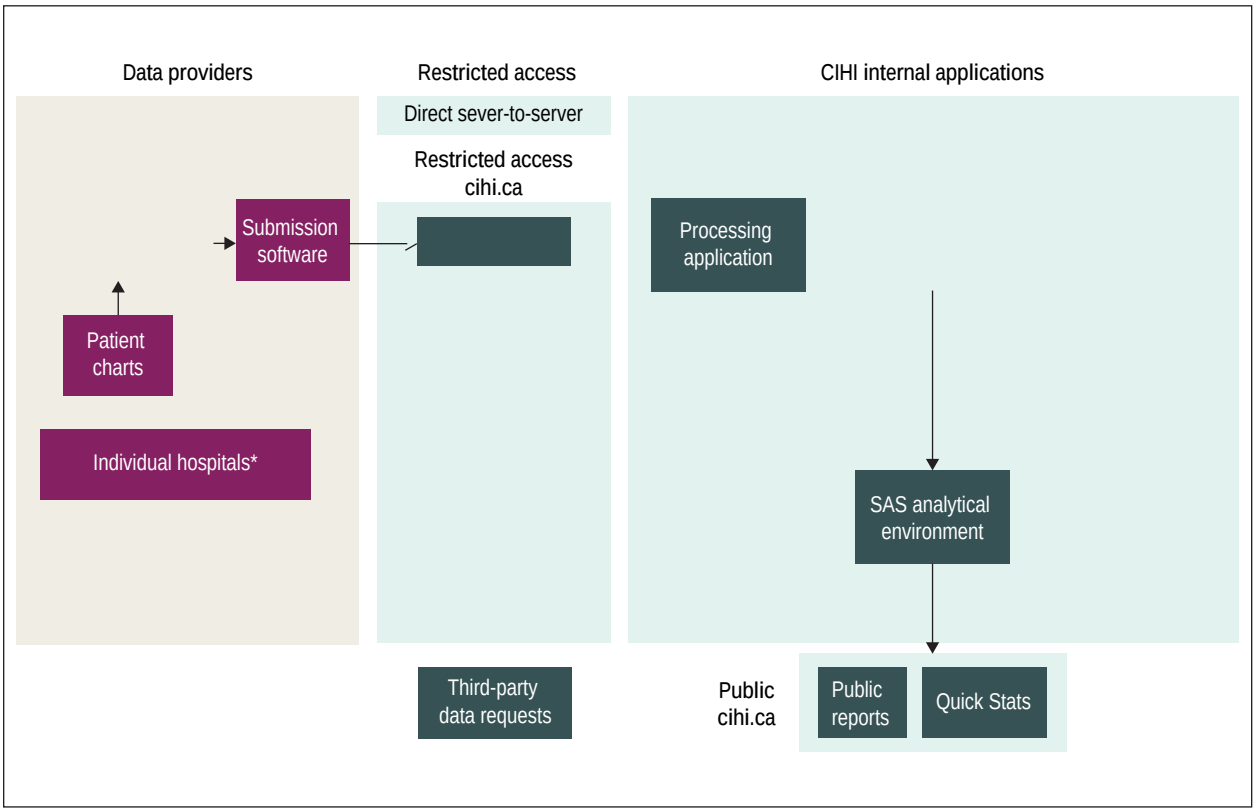
process, which is managed by CIHI's Client Engagement and Support (CES) department. CES manages access to CIHI's secure applications using established access management system (AMS) processes for granting and revoking access.

Once authenticated through CIHI's AMS, CJRR data providers can log in on CIHI's website,

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

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 PDWHULDOL]LQJ DQG RU WKHLU LPSDFW VKRXOG WKH\ RFFXU , Privacy and Security Risk Management Framework and implemented the associated Policy on Privacy and Security Risk Management. &,+,¶V FKLHI SULYDF\ RˆFHU DQG FKLHI LQIR RˆFHU LQ FROODERUDWLRQ ZLWK VHQLRU PDQDJHUV DUH UHV treating, monitoring and reviewing privacy and security risks.

3ULYDF\ DQG VHFXULW\ ULVNV PD\ EH LGHQWL¿HG IURP D YDUL LGHQWL¿HG ULVNV DUH HQWHUHG LQWR WKH 3ULYDF\ DQG 6HF high , medium or low , based on the likelihood and impact of a risk event:

- High: +LJK SUREDELOLW\ RI ULVN RFFXUULQJ DQG RU FRQWURO RU H‡HFWLYH
- Medium: 0HGLXP SUREDELOLW\ RI ULVN RFFXUULQJ DQG RU FRQ UHOLDEOH RU H‡HFWLYH RU
- Low: /RZ SUREDELOLW\ RI ULVN RFFXUULQJ DQG RU UHOLDEOH strategies exist.

7KH OLNHOLKRRG DQG LPSDFW RI WKH LGHQWL¿HG ULVN DUH X DVVHVVPHQW VFRUH RI ORZ PHGLXP RU KLJK GH¿QHV WKH VHU 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 QHFHVVDU\ XQWLO WKH ULVN LV ORZ RU WKH XQWUHDWHG UHV 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

Privacy legislation

management of the health system, including statistical analysis and reporting. Data providers

applicable, at the time the data is collected.

legislation: Newfoundland and Labrador, Prince Edward Island, Nova Scotia, New Brunswick, Ontario, Manitoba, Saskatchewan, Alberta, Yukon and the Northwest Territories. 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.

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.**legislation in place, fce'**

3.3 Principle 1: Accountability for personal health information

Privacy Policy, 2010

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.

Other sensitive variables

- **Gender**
- **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

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.

production of statistics to support planning, management and quality improvement.

CIHI

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

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

process. When carrying out data linkages, CIHI will generally do so using consistently

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)
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)
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

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

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

methodologies appropriate to the format, medium or device such that reconstruction is not reasonably foreseeable.

Section 29 of CIHI's Privacy Policy, 2010
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
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;

Third-party data requests

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

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

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,

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

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

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

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

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 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

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