



Patient-Reported Outcome Measures (PROMs) Program for Hip and Knee Arthroplasty

Privacy Impact Assessment

September 2019

(Updated February 2020)



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.

Unless otherwise indicated, this product uses data provided by Canada's provinces and territories.

All rights reserved.

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

For permission or information, please contact CIHI:

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

© 2020 Canadian Institute for Health Information

How to cite this document:

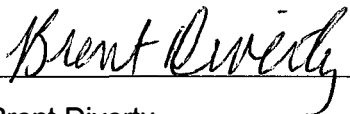
Canadian Institute for Health Information. *Patient-Reported Outcome Measures (PROMs) Program for Hip and Knee Arthroplasty: Privacy Impact Assessment, September 2019 (Updated February 2020)*. Ottawa, ON: CIHI; 2020.

Cette publication est aussi disponible en français sous le titre *Programme sur les mesures des résultats déclarés par les patients (MRDP) pour les arthroplasties de la hanche et du genou : évaluation des incidences sur la vie privée, septembre 2019 (mis à jour en février 2020)*.

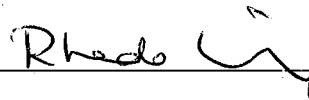
The Canadian Institute for Health Information (CIHI) is pleased to publish the following privacy impact assessment in accordance with its *Privacy Impact Assessment Policy*:

- **Patient-Reported Outcome Measures (PROMs) for Hip and Knee Arthroplasty**

Approved by:



Brent Diverty
Vice President, Programs



Rhonda Wing
Chief Privacy Officer & General Counsel

Ottawa, September 2019

Table of contents

Quick facts about the Patient-Reported Outcome Measures (PROMs) Program for Hip and Knee Arthroplasty	5
1 Introduction	6
2 Background	6
2.1 Introduction to CIHI's PROMs Program for Hip and Knee Arthroplasty	6
2.2 Data collection	7
2.3 Access management, data submission and flow for PROMs	8
3 Privacy analysis	10
3.1 Privacy and Security Risk Management Program	10
3.2 Authorities governing PROMs for hip and knee arthroplasty data	11
3.3 Principle 1: Accountability for personal health information	12
3.4 Principle 2: Identifying purposes for personal health information	13
3.5 Principle 3: Consent for the collection, use or disclosure of personal health information	13
3.6 Principle 4: Limiting collection of personal health information	13
3.7 Principle 5: Limiting use, disclosure and retention of personal health information	14
3.8 Principle 6: Accuracy of personal health information	18
3.9 Principle 7: Safeguards for personal health information	18
3.10 Principle 8: Openness about the management of personal health information	20
3.11 Principle 9: Individual access to, and amendment of, personal health information	20
3.12 Principle 10: Complaints about CIHI's handling of personal health information	20
4 Conclusion	20
Appendix: Text alternative for figure	21

Quick facts about the Patient-Reported Outcome Measures (PROMs) Program for Hip and Knee Arthroplasty

1. The Canadian Institute for Health Information (CIHI) is a not-for-profit, pan-Canadian organization with extensive experience in health data collection and management and works in partnership with a broad range of national and international stakeholders to understand and address information needs of the health systems.
2. Hip and knee joint replacement surgeries (arthroplasty) are among the most effective ways to reduce joint pain and improve functioning for patients with advanced hip and knee problems, most commonly resulting from osteoarthritis. CIHI has launched a national program for the collection and reporting of patient-reported outcome measures (PROMs) for hip and knee arthroplasty, beginning with a pilot in Ontario.
3. As part of the Ontario pilot, PROMs data is captured on hip and knee arthroplasty patients in participating acute care facilities and provided on a regular basis in electronic format to CIHI via Cancer Care Ontario and other authorized submitters. CIHI prepares the data for health system reporting by linking the PROMs data to other CIHI data holdings such as the Discharge Abstract Database (DAD) and National Ambulatory Care Reporting System (NACRS), and provides reporting for the project.
4. PROMs are essential to a patient-centred approach to health care, as they provide the patient's perspective on aspects of their health status that are relevant to their quality of life, including symptoms, function, pain and physical health. PROMs data can be used by governments to inform provincial priorities, including the delivery of patient-centred health care, and to support the transition from a volume-based to a value-based health care system.
5. CIHI is playing a leadership role in standardized collection and reporting of PROMs for hip and knee arthroplasty, both in Canada and internationally. CIHI has also partnered with the Organisation for Economic Co-operation and Development (OECD) in leading an international working group that aims to provide comparable reporting among participating countries as part of a pilot project.

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 PROMs Program for Hip and Knee Arthroplasty. This 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 the principles apply to the PROMs Program for Hip and Knee Arthroplasty, as well as a look 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](#).

2 Background

2.1 Introduction to CIHI's PROMs Program for Hip and Knee Arthroplasty

CIHI launched the [Canadian Joint Replacement Registry](#) (CJRR) in 2001 in collaboration with the Canadian Orthopaedic Association. CJRR aims to improve the outcomes for hip and knee replacement patients in Canada and captures prosthesis information on these surgeries. Analysis of this information together with data from CIHI's hospitalization databases (e.g., DAD, Hospital Morbidity Database) enables the follow-up of joint replacement patients over time to monitor their revision rates and outcomes.

In Canada, several PROMs programs for hip and knee arthroplasty exist but have not been implemented in a standardized manner to allow for national and international comparative reporting. In 2015, CIHI convened a national PROMs forum; an outcome of that meeting was identification of hip and knee arthroplasty as 2 of the clinical areas of focus to advance CIHI's PROMs Program. In 2016, CIHI launched the PROMs Hip and Knee Replacements Working Group to guide the development of common approaches for PROMs data collection and reporting in hip and knee arthroplasty across Canada. Members include provincial government representatives, orthopedic surgeons and senior researchers actively involved in PROMs work.

With support from the CJRR Advisory Committee, CIHI worked with the PROMs Hip and Knee Replacements Working Group to develop national standards for PROMs collection for these clinical areas. Considerations in developing the PROMs standards include alignment with recommendations, guidelines and best practices from existing programs and registries across Canada and internationally, and where feasible, the ability to minimize the burden of data collection for patients and service providers (e.g., cost, resources, time).

National PROMs standards for hip and knee arthroplasty include guidelines for survey time points, a minimum data set (MDS) and recommended PROMs instruments. The PROMs collection standards were approved by the CJRR Advisory Committee and CIHI's PROMs Hip and Knee Replacements Working Group in November 2017 and are available on CIHI's website at www.cihi.ca/proms.

2.2 Data collection

CIHI collects record-level, identifiable data on hip and knee arthroplasty PROMs in Canada, beginning with a pilot in Ontario and expanding to other interested jurisdictions over time. Data elements collected are in the MDS as listed in CIHI's [Patient-Reported Outcome Measures Data Collection Manual: Hip and Knee Arthroplasty, 2019](#). This includes the capture of information from selected licensed survey tools: the [Oxford Hip Score](#), the [Oxford Knee Score](#) and the [EQ-5D-5L](#). These surveys are repeated longitudinally pre- and post-surgery in order to track outcomes from a patient's perspective over time and to monitor gains in improvement.

The following identifiers are included in the PROMs MDS for hip and knee arthroplasty:

Patient Information

- Health Care Number (HCN)
- Jurisdiction Issuing HCN
- Birthdate

Provider Information

- Surgeon Identifier — a unique number that identifies the provider assigned to the patient. This may be a number assigned by the reporting facility or by the province/territory (e.g., from the relevant college of physicians and surgeons).

2.3 Access management, data submission and flow for PROMs

The figure below illustrates the high-level flow for PROMs data. Hospitals, health regions, ministries of health (or third-party organizations under contract to them) survey patients directly through various modes (paper, telephone, online) at established time points relative to their hip or knee surgery in a longitudinal manner to support reporting needs.

Data providers submit this data to CIHI in alignment with CIHI's specifications. CIHI processes the data, performs quality checks and provides feedback regarding any issues with the submitted files.

Specifically for the Ontario pilot, data is collected from hip and knee arthroplasty patients in participating acute care facilities and compiled at Cancer Care Ontario, which sends data on a regular basis in electronic format to CIHI. CIHI links the PROMs data to the DAD and the National Ambulatory Care Reporting System (NACRS) to prepare the data for health system reporting for the project.

Future activities, which align with other data holding programs at CIHI, include provision of PROMs data to third-party requestors and for other reporting purposes.

Access to CIHI's secure applications is subject to CIHI's role-based access management process, which is managed by CIHI's Client Support Applications (CSA) department. CSA 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, PROMs data providers submit to CIHI record-level data from facilities that is electronically captured using specialized software, through CIHI's secure file submission service for processing.

At the time of processing, all submitted PROMs data undergoes validation and a data quality check for errors and inconsistencies against specifications outlined in the [Data Dictionary](#). The data processing system is internal to CIHI, with no external connection.

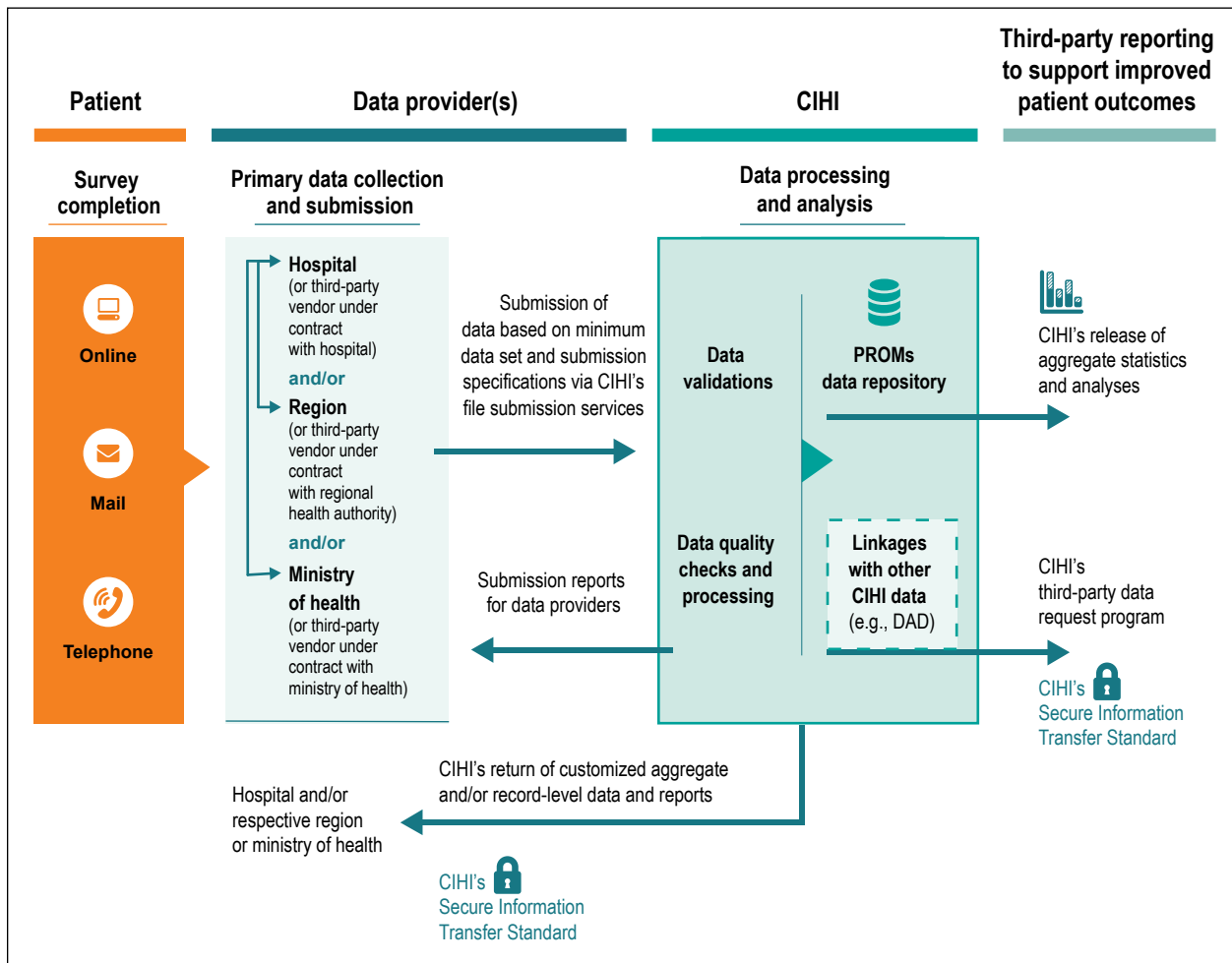
Error and validation reports generated at the time of processing are made available to the respective data providers in compliance with CIHI's *Secure Information Transfer Standard*. These reports identify records with errors; indicate the reason records were rejected or the relevant warning message; and permit the data provider to correct errors in the records and resubmit them.

Once the iterative error correction process is completed, a de-identified copy of the PROMs data set is then uploaded to CIHI's SAS analytical environment where it is made available to approved CIHI staff for CIHI purposes. Analytical activities, including possible linkage with

other data holdings (e.g., DAD, NACRS) will occur within the PROMs data repository. CIHI may return PROMs data to the applicable provider (e.g., ministry, hospital, regions). CIHI may also disclose aggregate and de-identified record-level data to third-party requestors and aggregate data to the public.

Staff access to the PROMs data in the SAS analytical environment is provided through CIHI's centralized access process. The process ensures that all requests for access, including access to PROMs data, are traceable and authorized. The access system is subject to an annual audit to ensure that staff are accessing data on a need-to-know basis. [Section 3.9](#), Principle 7: Safeguards for personal health information, includes additional information about how the various procedural and technical measures are deployed to prevent unauthorized access and otherwise secure PROMs data.

Figure PROMs high-level data flow



3 Privacy analysis

3.1 Privacy and Security Risk Management Program

Privacy and security risk management (PSRM) is a formal, repeatable process for identifying, assessing, treating and monitoring risks in order to minimize the probability of such risks materializing and/or their impact should they occur. In 2015, CIHI approved its [Privacy and Security Risk Management \(PSRM\) Framework](#) and implemented the associated [Policy on Privacy and Security Risk Management](#). CIHI's chief privacy officer and chief information security officer, in collaboration with senior managers, are responsible for identifying, assessing, treating, monitoring and reviewing privacy and security risks.

Privacy and security risks may be identified from a variety of sources, including PIAs, for example. 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 Senior Management Committee on behalf of the corporation.

3.2 Authorities governing PROMs for hip and knee arthroplasty 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 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, the collection of PROMs data for hip and knee arthroplasty 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

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

Table Key positions and responsibilities

Position/group	Roles/responsibilities
Vice president, Programs	Responsible for the overall strategic direction of the PROMs Program for Hip and Knee Arthroplasty
Director, Acute and Ambulatory Care Information Services	Responsible for operations and strategic business decisions about the PROMs Program for Hip and Knee Arthroplasty
Chief information security officer	Responsible for the strategic direction and overall implementation of CIHI's Information Security Program
Chief privacy officer	Responsible for the strategic direction and overall implementation of CIHI's Privacy Program
Commitment Manager, ITS	Responsible for ensuring the availability of technical resources and solutions for ongoing operations and enhancements of the PROMs Program for Hip and Knee Arthroplasty
Manager, Technology Services	Responsible for managing access to the web-based applications used for the PROMs Program for Hip and Knee Arthroplasty

3.4 Principle 2: Identifying purposes for personal health information

CIHI collects only personal health information required for achieving the goals of the PROMs Program for Hip and Knee Arthroplasty, including the purposes that have been identified in consultation with appropriate stakeholders (e.g., ministries of health, regional or jurisdictional health authorities). Direct identifiers (see [Section 2.1](#)) are included in the PROMs MDS to

- Facilitate accurate identification of a patient to enable linkage of a patient's surgery data, as well as for longitudinal follow-up; and
- To analyze the effects of specific identifiers, such as age at the time of surgery.

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 the health care systems. CIHI will ensure that the data elements being collected are directly necessary for the program. All data collected will be used to further the objectives of the PROMs Program. The objectives are as follows:

- Demonstrate the value of collecting PROMs data beginning with hip and knee arthroplasty;
- Launch a standardized approach to the collection of PROMs data;
- Promote alignment with national standards to support comparable reporting;
- Support the OECD patient-reported indicators program of work related to PROMs for hip and knee arthroplasty;
- Develop comparative reports for health system monitoring;
- Provide facility- and surgeon-level reports to own data providers;

- Improve communications between providers and patients, informing treatment decisions and setting appropriate patient expectations on outcomes;
- Complement traditional, clinical outcomes, cost and patient experience data to enable a more comprehensive understanding of their inter-relationships; and
- Support the evaluation of performance and effectiveness of care.

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

Limiting use

CIHI limits the use of PROMs for hip and knee arthroplasty data to the authorized purposes, as described in sections [3.4](#) and [3.6](#). 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 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 names or direct identifiers, such as unencrypted HCNs. They are removed from records before being moved to the PROMs for hip and knee arthroplasty data processing and analysis environment (see [Section 2.3](#)). HCNs in an unencrypted form are available to CIHI staff on an exceptional, need-to-know basis only, subject to approval processes as set out in CIHI's internal Privacy (2010) policy and procedures.

Data linkage

Data linkages are performed between the PROMs for hip and knee arthroplasty data and other CIHI data sources. While this potentially causes greater risk of identification of an individual, CIHI undertakes mitigating steps to reduce the risks (i.e., data can be de-identified by removing patient identifiers and assigning meaningless transaction numbers).

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 HCNs. 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 HCN, and the province/territory that issued the HCN. 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 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 both data linkages for CIHI's own purposes and for third-party data requests.

Return of own data

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 their 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 de-identified record-level and/or aggregated data from the PROMs Program for Hip and Knee Arthroplasty may be requested by a variety of third parties such as government, health care decision-makers and researchers.

CIHI administers a third-party data request program that 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, the Privacy and Legal Services branch 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 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.

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, the Privacy and Legal Services branch contacts third-party data recipients on an annual basis to certify that they continue to comply with their obligations as set out in the data request form and data protection agreement signed with CIHI.

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](#) through tools such as Your Health System: In Depth and Quick Stats.

Limiting retention

The PROMs for hip and knee arthroplasty form part of CIHI's data holdings and, consistent with its mandate and core functions, CIHI retains such information for as long as necessary to meet the identified purposes.

3.8 Principle 6: Accuracy of personal health information

CIHI has a comprehensive data quality program. Any known data quality issues will be addressed by the data provider or documented in data limitations documentation, which CIHI makes available to all users.

Similar to other CIHI data holdings, the PROMs for hip and knee arthroplasty are 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 hip and knee arthroplasty 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 hip and knee arthroplasty 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 HCN has been removed or encrypted upon first receipt. In exceptional instances, staff will require access to original HCNs. 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 HCNs and patient names (rarely collected) within CIHI's operational production databases;
- Access to data files containing personal health information extracted from CIHI's operational production databases and made available to the internal analytical community on an exceptional basis; and
- Changes to permissions in access to operational production databases.

CIHI's employees are made aware of the importance of maintaining the confidentiality of personal health information and other sensitive information through a mandatory privacy and security training program and through ongoing communications about CIHI's privacy and security policies and procedures. Employees attempting to access a CIHI information system must confirm, prior to each login 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.

Finally, regardless of the data collection model used for the program, CIHI will maintain a data repository for PROMs data and store this information securely at CIHI.

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 at 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 the PROMs Program for Hip and Knee Arthroplasty did not identify any privacy or security risks. This PIA will be updated or renewed in compliance with CIHI's [Privacy Impact Assessment Policy](#).

Appendix: Text alternative for figure

Figure: PROMs high-level data flow

Patients undergoing hip and knee arthroplasty are directly surveyed by data providers (e.g., hospitals, health regions, ministries of health) to collect pre- and post-operative information using PROMs tools. The collected PROMs data is submitted to CIHI electronically through CIHI's secure file submission service for processing, which includes activities such as data validation and data quality checks for errors and inconsistencies. Submission reports, which contain identified errors and inconsistencies, are returned to data providers for correction.

Following data validation and data quality processing, PROMs data is transferred to the PROMs data repository, where it is linked with other CIHI data holdings (e.g., DAD, NACRS) to create the analytical file. The linked data file is then used by CIHI staff for analysis and delivery of customized aggregate and/or record-level data and reports.

**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

21560-0220

