Canadian Patient Experiences Reporting System Privacy Impact Assessment

August 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.

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

How to cite this document:
Canadian Institute for Health Information. *Canadian Patient Experiences Reporting System Privacy Impact Assessment, August 2020*. Ottawa, ON: CIHI; 2020.

Cette publication est aussi disponible en français sous le titre *Évaluation des incidences sur la vie privée du Système de déclaration de l'expérience des patients canadiens, août 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*:

- *Canadian Patient Experiences Reporting System Privacy Impact Assessment, August 2020*

Approved by

Brent Diverty
Vice President, Data Strategies and Statistics

Rhonda Wing
Chief Privacy Officer and General Counsel

Ottawa, August 2020

Table of contents

Quick facts about the Canadian Patient Experiences Reporting System

1. Launched in April 2015, the Canadian Patient Experiences Reporting System (CPERS) collects and reports on patient experiences within the health care system in Canada, beginning with inpatient acute care hospitals. The purpose of CPERS is to provide standardized patient experience information from across Canada to inform and improve patient-centred care and patient outcomes.

   Information from CPERS will be used by health care providers, health system managers, policy-makers and patients to

   - Analyze the patient experience aspect of quality of care for reporting, monitoring and comparing performance; and
   - Identify and inform quality and efficiency improvements and assess the effectiveness of health interventions to better support the integration of care for improved patient-centred care.

2. The Canadian Institute for Health Information (CIHI), with input from a broad range of experts, led the development of the standardized Canadian Patient Experiences Survey — Inpatient Care (CPES-IC). CPES-IC data submitted to CPERS is focused on patient experiences with inpatient acute care hospital stays.
3. CPERS contains personal health information (health card number and birth date), as well as responses to CPES-IC survey questions and demographic information. Special project fields are used to collect supplemental information required to meet specific needs as identified by CIHI, the jurisdiction and/or facility needs.
4. Participating hospitals, health regions, health quality councils and/or ministries of health, or their designates, contact patients following discharge from a hospital to collect information about their inpatient care experience, and then submit the data to CPERS based on the CPES-IC minimum data set and pre-set specifications. Survey collection approaches (e.g., mode of collection) as well as survey frequency and duration vary across jurisdictions.
5. As of June 2020, CPERS contained more than 320,000 inpatient experience surveys submitted by 6 jurisdictions (Nova Scotia, New Brunswick, Ontario, Manitoba, Alberta and British Columbia).
6. CPERS data is used for standardized reporting and analysis, as well as linkage of person-level data across data holdings and across time. CIHI currently makes hospital-comparative CPERS data available to submitting jurisdictions via the CPES: Comparative Results tool. CIHI is working toward publicly reporting a core set (3 to 5) of patient experience indicators in the Your Health System: In Depth web tool anticipated for release in 2022.

1 Introduction

The Canadian Institute for Health Information (CIHI) collects and analyzes information on health and health care in Canada. Its mandate is to deliver comparable and actionable information to accelerate improvements in health care, health system performance and population health across the continuum of care. CIHI obtains data from hospitals and other health care facilities, long-term care homes, regional health authorities, medical practitioners and governments. This data includes information about health services provided to individuals, the health professionals who provide those services and the cost of the health services.

The purpose of this privacy impact assessment (PIA) is to examine the privacy, confidentiality and security risks associated with the Canadian Patient Experiences Reporting System (CPERS). This PIA, which replaces the January 2015 version, 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 CPERS, 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 CPERS

Understanding and improving a patient's experience when he or she receives health services, interventions and care are integral to providing patient-centred care.

To address information gaps and the lack of standardized patient experience information across Canada, CIHI led the development of the standardized Canadian Patient Experiences Survey — Inpatient Care (CPES-IC). CPERS was established to provide standardized, comparable patient experience information from across Canada, starting with acute inpatient care based on the CPES-IC.

Information from CPERS will help us better understand and compare patient perspectives on health services, interventions and care received, to inform and improve patient-centred care and patient outcomes in Canada. It will be used by health care providers, health system managers and policy-makers to

- Provide comparable data on the patient experience aspect of quality of care for reporting, monitoring and comparing performance; and
- Provide data from which to identify and inform quality and efficiency improvements and assess the effectiveness of health interventions, to better support the integration of care for improved patient-centred care.

Future expansions may include other sectors of care beyond inpatient care.

2.2 Data collection

CPERS collects data about patient experiences in inpatient hospital stays across 3 hospital service lines (i.e., medical, surgical, maternity) via the CPES-IC. CPERS collects

- Patients' responses to CPES-IC questions
- Information on the survey methods and processes used to administer the survey
- Administrative information needed to support submissions, analysis and reporting

Participating hospitals, health regions, health quality councils and/or ministries of health, or their designates, contact patients following discharge from a hospital to collect information about their inpatient care experience, and then submit the data to CPERS based on the CPES-IC minimum data set and pre-set specifications. Survey collection approaches (e.g., mode of collection) as well as survey frequency and duration vary across jurisdictions.

As of June 2020, CPERS contained more than 320,000 inpatient experience surveys submitted by 6 jurisdictions (Nova Scotia, New Brunswick, Ontario, Manitoba, Alberta and British Columbia). Data submission to CPERS is voluntary. In 5 jurisdictions, data submission is coordinated at the provincial level (e.g., through the ministry or the health council). Ontario has implemented a voluntary approach at the hospital level whereby hospitals voluntarily submit data via a services contract organized by the Ontario Hospital Association or directly to CIHI.

CPERS contains data elements that could, alone or in combination with other information, lead to the identification of an individual. Below is a list of data elements collected in CPERS that are particularly sensitive. See Table 1, which outlines the rationale for CPERS's collection of personal health information.

Direct identifiers (personal health information)

The following direct personal identifiers are collected in CPERS:

- Full date of birth
- Health care number
- Jurisdiction issuing health care number

Other unique identifiers

The following other unique identifiers are collected in CPERS:

- Organization patient identifier (e.g., chart number)
- Gender
- Race/ethnicity
- Education level

Health facility identifier

The following health facility identifier is collected in CPERS:

- Organization identifier

Table 1 Rationale for the collection of sensitive CPERS data

Element/definition	When collected	Reason for collection/comments
Health Care Number A jurisdictionally unique number used to identify a patient who has received or is receiving health care–related services or goods; this includes the code that identifies the jurisdiction that issued the health care number	Collected from the hospital's administrative system, needed at time of submission to CIHI	To identify unique clients within a jurisdiction To link with other CIHI data holdings to provide an enriched source of data for analysis and reporting
Organization Patient Identifier An organization-assigned unique number (e.g., chart number) that identifies a patient who has received or is receiving health care–related services or goods	Collected from the hospital's administrative system, needed at time of submission to CIHI	To link a CPES-IC record with the corresponding hospital encounter (e.g., Discharge Abstract Database record), when an identifiable Organization Patient Identifier is provided (in conjunction with Discharge Date) To uniquely identify a person within a source organization in the event that health care number is not available
Birthdate The year, month and day that represent the date on which the patient was born or is officially deemed to have been born	Collected from the hospital's administrative system or patient-reported at time of survey completion; may be used when determining survey sample (e.g., identifying patients 18 and older) and at time of submission to CIHI	To calculate age, which is required to conduct analysis by age, and to enhance linkage with other CIHI data holdings
Gender A code used to indicate the gender of the patient	Collected from the hospital's administrative system, or patient-reported at time of survey completion	To permit analysis of differences in patient experiences among genders
Race/Ethnicity A patient's self-declared affiliation with 1 or more social groups that have a common national or cultural tradition	Patient-reported at time of survey completion	To permit analysis of differences in patient experiences across various racial and ethnic groups

2.3 Access management, data submission and flow for CPERS

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, CPERS data providers submit to CIHI record-level data from facilities that is electronically captured using specialized software, through CIHI's secure web-based electronic Data Submission Services (eDSS) and/or CIHI's secure file submission service for processing (SFTP), which are 2 of CIHI's preferred secure data transmission methods. CPERS data is submitted in accordance with the following data collection standards:

Survey standards

- Canadian Patient Experiences Survey — Inpatient Care
- Canadian Patient Experiences Survey — Inpatient Care Procedure Manual

Data submission standards

- Canadian Patient Experiences Survey — Inpatient Care Data Dictionary Manual
- Vendor specifications available upon signing vendor licence agreement

At the time of processing, all submitted CPERS data automatically undergoes validation and a data quality check for errors and inconsistencies against specifications outlined in the *CPES-IC Data Dictionary Manual* and vendor specification package. The data processing system is internal to CIHI, with no external connection.

Error and validation reports generated at the time of processing are made available to the respective data providers via Operational Reports in compliance with CIHI's *Secure Information Transfer Standard*. These detailed submission reports identify records using submitting organization, file name, source organization, survey cycle identifier, survey identifier and data element ID with errors; specify the number of records a data provider has successfully submitted; indicate the reason records were rejected or the relevant warning message; and permit the data provider to correct errors in the records and resubmit them to CPERS.

Once the iterative error correction process is completed, final summary reports of file-processing results are returned to data providers via Operational Reports. A complete copy of the CPERS data set is then uploaded to CIHI's SAS analytical environment where it is made available to approved CIHI staff for CIHI purposes.

Upon request, CIHI returns CPERS data to the data provider that originally supplied the data, as well as to the respective ministry of health. CIHI currently makes hospital-comparative aggregate CPERS data available to submitting jurisdictions via the CPES: Comparative Results tool. This secure web tool allows authorized users to view their results on patient experience measures and compare their results with other participating hospitals. CIHI also discloses aggregated statistics and analyses to the public. In the future, patient experience results (for a core set of measures) will be available through CIHI's Your Health System. The figure below is a high-level illustration of the data flows for CPERS.

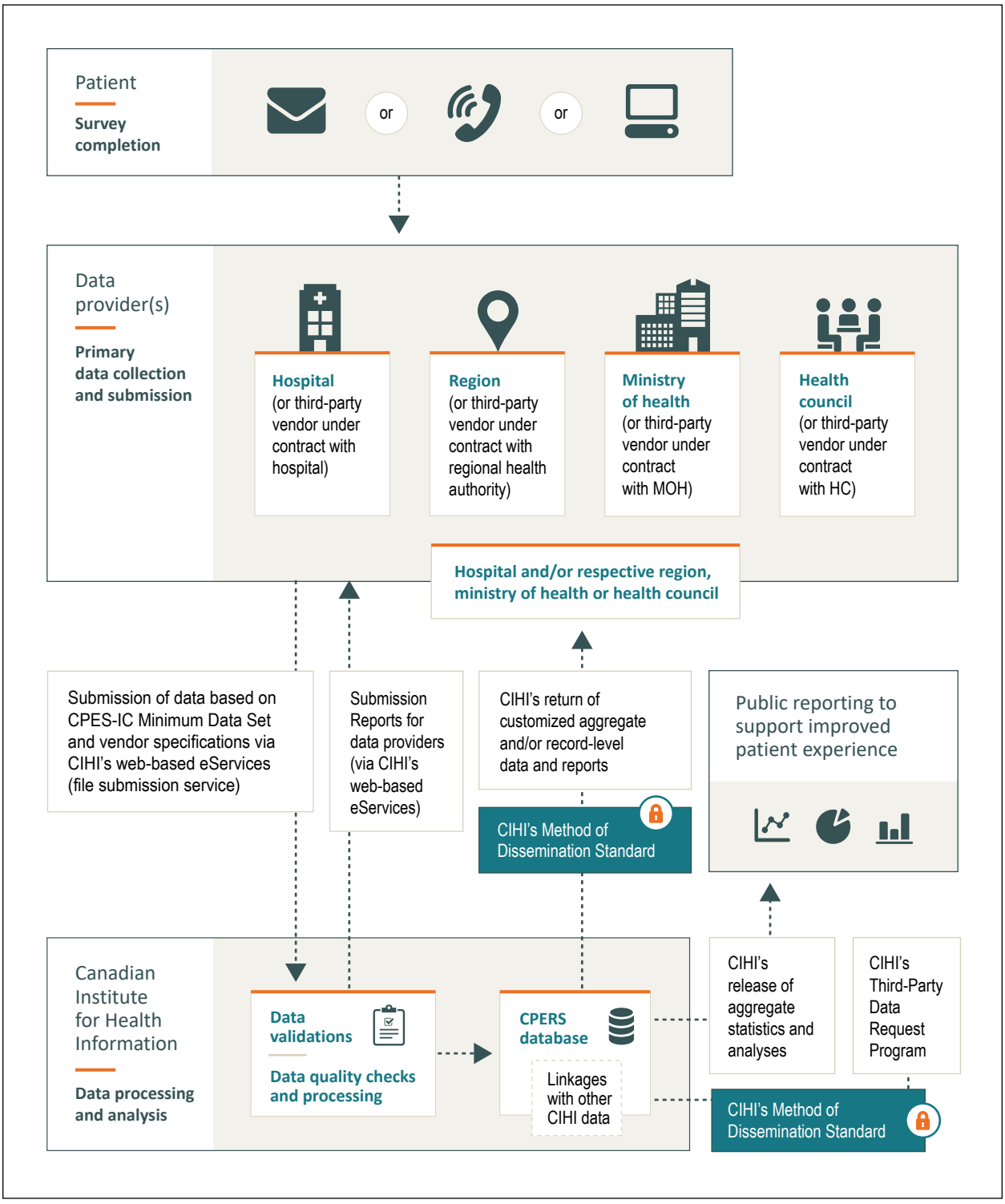
CIHI staff access to CPERS

Staff access to the SAS analytical environment is provided through CIHI's centralized SAS Data Access process. The process ensures that all requests for access, including access to CPERS data, are traceable and authorized. The SAS Data Access system is subject to an annual audit to ensure that staff are accessing data on a need-to-know basis. Section 3.9 includes additional information about how the various procedural and technical measures are deployed to prevent unauthorized access and otherwise secure CPERS data.

Data flows

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

Figure Overview of the data flows for CPERS



3 Privacy analysis

3.1 Privacy and Security Risk Management Program

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

General

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

Privacy legislation

CIHI is a secondary data collector of health information, specifically for the planning and management of the health system, including statistical analysis and reporting. Data providers are responsible for meeting the statutory requirements in their respective jurisdictions, where applicable, at the time the data is collected.

The following provinces and territories have enacted health information–specific privacy legislation: Newfoundland and Labrador, Prince Edward Island, Nova Scotia, New Brunswick, Ontario, Manitoba, Saskatchewan, Alberta, Yukon and the Northwest Territories. Health information–specific privacy legislation authorizes facilities to disclose personal health information without patient consent for the purposes of health system use, provided that certain requirements are met. For example, CIHI is recognized as a prescribed entity under the *Personal Health Information Protection Act* of Ontario, so health information custodians in Ontario may disclose personal health information to CIHI without patient consent pursuant to Section 29 as permitted by Section 45(1) of the act.

In provinces and territories that do not currently have health information–specific privacy legislation in place, facilities are governed by public-sector legislation. This legislation authorizes facilities to disclose personal information for statistical purposes, without an individual's consent.

Agreements

At CIHI, CPERS data is governed by CIHI's Privacy Policy, 2010, by legislation in the jurisdictions and by data-sharing agreements with the provinces and territories. The data-sharing agreements set out the purpose, use, disclosure, retention and disposal requirements of personal health information provided to CIHI, as well as any subsequent disclosures that may be permitted. The agreements also describe the legislative authority under which personal health information is disclosed to CIHI.

3.3 Principle 1: Accountability for personal health information

CIHI's president and chief executive officer is accountable for ensuring compliance with CIHI's Privacy Policy, 2010. CIHI has a chief privacy officer and general counsel, a corporate Privacy, Confidentiality and Security Committee, a Governance and Privacy Committee of its Board of Directors and an external chief privacy advisor.

Organization and governance

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

Table 2 Key positions and responsibilities

Position/group	Roles/responsibilities
Vice president, Data Strategies and Statistics	Responsible for the overall strategic direction of CPERS
Director, Acute and Ambulatory Care Information Services	Responsible for the overall operations and strategic business decisions of CPERS and management of strategic relationships
Manager, Joint Replacement Registry, Patient-Reported Outcomes and Experiences	Responsible for ongoing management and uptake of CPERS; makes day-to-day operational decisions about CPERS and supports CPERS working groups and/or committees
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
Manager, Data Acquisition Products	Responsible for ensuring that technical requirements for ongoing operations and enhancements for CPERS are met; acts as system administrator for CPERS
Manager, Client Engagement and Support	Responsible for managing external client access to restricted web-based eServices

Working groups and committees

CIHI currently convenes 2 external groups to provide advice on CPERS activities. 1 group is the Inter-Jurisdictional Patient-Centred Measurement Advisory Group. This group advises CIHI in the development of a common approach to patient-centred measurement and reporting in Canada; drives peer-to-peer learning and best practice sharing; and provides input and recommendations to increase the use of patient-centred measurement results.

The other group is the CPERS Implementation Working Group, whose membership consists of jurisdictions that participate in CPERS. The purpose of this working group is to obtain jurisdiction-specific patient experience data collection knowledge and input to support sound decision-making on matters related to implementation of the CPES-IC and submission of data to CPERS. It also facilitates the sharing of implementation learnings amongst the participating jurisdictions.

3.4 Principle 2: Identifying purposes for personal health information

CIHI collects only personal health information required for achieving the goals of CPERS (see Section 2.1). An instruction manual for CPERS data providers (*CPES-IC Data Dictionary Manual*) lists data elements and describes their purpose. This document is updated as required and is publicly available on CIHI's website.

3.5 Principle 3: Consent for the collection, use or disclosure of personal health information

CIHI is a secondary collector of data and does not have direct contact with patients. CIHI relies on data providers to abide by and meet their data collection, use and disclosure rules and responsibilities, including those related to consent and notification, as outlined in jurisdiction-applicable laws, regulations and policies.

3.6 Principle 4: Limiting collection of personal health information

CIHI is committed to the principle of data minimization. Under sections 1 and 2 of CIHI's Privacy Policy, 2010, CIHI collects from data providers only the information that is reasonably required for health system uses, including statistical analysis and reporting, in support of the management, evaluation or monitoring of the health care system.

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

The CPES-IC minimum data set (MDS) consists of patient experience survey information and other information, representing the minimum information necessary to address CPERS' purposes.

CIHI developed the CPES-IC with input from a broad range of stakeholders, using the Hospital Consumer Assessment of Healthcare Providers and Systems (HCAHPS) survey as a base. Stakeholders included the Inter-Jurisdictional Patient Satisfaction Group, Accreditation Canada, the Canadian Patient Safety Institute, The Change Foundation and the CPERS Development Working Group.

The submission information portion of the CPES-IC MDS contains data elements to facilitate submissions to CIHI (e.g., Submitting Organization Identifier) and survey methodology–related data elements necessary for analysis and reporting (e.g., Sample Size, Number of Eligible Discharges, Sampling Method).

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

Limiting use

Clients

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

CIHI

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

Data sets used for internal CIHI analysis purposes do not contain names or direct identifiers, such as unencrypted health care numbers. They are removed from records before being moved to CPERS analytical environment (see Section 2.3 above). Health care numbers 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 Policy and Procedures, 2010.

Data linkage

Data linkages are performed between the CPERS data and other CIHI data sources. The value of patient experience data is enhanced when linked to the acute care service episode record it pertains to, as this provides information about the complexity and other aspects relevant to the experience, such as adverse events. It also enables the development and application of methodologies (e.g., weighting, adjustments) to help ensure comparability of results. While this potentially causes greater risk of identification of an individual, CIHI undertakes mitigating steps to reduce the risks.

Sections 14 to 31 of CIHI's Privacy Policy, 2010 govern linkage of records of personal health information. Pursuant to this policy, CIHI permits the linkage of personal health information under certain circumstances. Data linkage within a single data holding for CIHI's own purposes is generally permitted. Data linkage across data holdings for CIHI's own purposes and all third-party requests for data linkage are subject to an internal review and approval process. When carrying out data linkages, CIHI will generally do so using consistently encrypted health care numbers. The linked data remains subject to the use and disclosure provisions in the Privacy Policy, 2010.

Criteria for approval of data linkages are set out in sections 23 and 24 of CIHI's Privacy Policy, 2010, as follows:

Section 23 The individuals whose personal health information is used for data linkage have consented to the data linkage; or

Section 24 All of the following criteria are met:

a) The purpose of the data linkage is consistent with CIHI's mandate;
b) The public benefits of the linkage significantly offset any risks to the privacy of individuals;
c) The results of the data linkage will not be used for any purpose that would be detrimental to the individuals that the personal health information concerns;
d) The data linkage is for a time-limited specific project and the linked data will be subsequently destroyed in a manner consistent with sections 28 and 29; or
e) The data linkage is for purposes of an approved CIHI ongoing program of work where the linked data will be retained for as long as necessary to meet the identified purposes and, when no longer required, will be destroyed in a manner consistent with sections 28 and 29; and
f) The data linkage has demonstrable savings over other alternatives or is the only practical alternative.

Client linkage standard

In 2015, CIHI implemented a corporate-wide client linkage standard to be used for the linkage of records created in 2010–2011 or later, where the records include the following data elements: encrypted health care number, and the province/territory that issued the health care number. For the linkage of records that do not satisfy these criteria, the linkage mechanism is determined on a case-by-case basis.

Destruction of linked data

Section 28 of CIHI's Privacy Policy, 2010 sets out the requirement that CIHI will destroy personal health information and de-identified data in a secure manner, using destruction methodologies appropriate to the format, 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 Information 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 Information Destruction Standard. These requirements apply to data linkages both 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.

Limiting disclosure

As described in Section 2.3, results from CPERS are made available to participating jurisdictions via the CPES: Comparative Results tool.

Before being provided with access to the CPES: Comparative Results tool, users must sign a service agreement that includes rules regarding health facility–identifiable information and the suppression of small cell sizes.

Third-party data requests

Customized record-level and/or aggregated data from CPERS may be requested by a variety of third parties. CIHI administers the 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, Privacy and Legal Services (PLS) has developed and is responsible for the ongoing compliance monitoring process whereby all data sets that are disclosed to third-party data recipients are tracked and monitored for secure destruction at the end of their life cycle. Prior to disclosing data, third-party recipients sign a data protection agreement and agree to comply with the conditions and restrictions imposed by CIHI relating to the collection, purpose, use, security, disclosure and return or disposal of data.

Data requesters are required to complete and submit a data request form. They must also sign an agreement wherein they agree to use the data for only the purpose specified. All data protection agreements with third parties specify that receiving organizations must keep record-level data strictly confidential and not disclose such data to anyone outside the organization. Moreover, CIHI imposes obligations on these third-party recipients, including

- Secure destruction requirements;
- CIHI's right to audit;
- Restriction on the publication of cell sizes less than 5; and
- Strong encryption technology that meets or exceeds CIHI's standards where mobile computing devices are used.

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 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.

As part of CIHI's phased approach to publicly reporting patient experience data, CIHI is working toward reporting a core set (3 to 5) of patient experience indicators in the Your Health System: In Depth web tool. When published, the data for these indicators will enable comparisons at the national, provincial, regional and facility levels. The anticipated release of these indicators is 2022.

Limiting retention

CPERS forms part of CIHI's data holdings and, consistent with its mandate and core functions, CIHI retains such information for as long as necessary to meet the identified purposes.

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, CPERS is subject to a data quality assessment on a regular basis, based on CIHI's Information Quality Framework. The process of completing the framework includes numerous activities to assess the various dimensions of quality, including the accuracy of CPERS data.

3.9 Principle 7: Safeguards for personal health information

CIHI's Privacy and Security Framework

CIHI has developed a Privacy and Security Framework to provide a comprehensive approach to enterprise privacy and security management. Based on best practices from across the public, private and health sectors, the framework is designed to coordinate CIHI's privacy and security policies and to provide an integrated view of the organization's information management practices. Key aspects of CIHI's system security with respect to the CPERS data are highlighted below.

System security

CIHI recognizes that information is secure only if it is secure throughout its entire life cycle: creation and collection, access, retention and storage, use, disclosure and destruction. Accordingly, CIHI has a comprehensive suite of policies that specify the necessary controls for the protection of information in both physical and electronic formats, up to and including robust encryption and secure destruction. This suite of policies and the associated standards, guidelines and operating procedures reflect best practices in privacy, information security and records management for the protection of the confidentiality, integrity and availability of CIHI's information assets.

System control and audit logs are an integral component of CIHI's Information Security Program. CIHI's system control and audit logs are immutable. Analysis at CIHI is generally conducted with the use of de-identified record-level data, where the health care number has been removed or encrypted upon first receipt. In exceptional instances, staff will require access to original health care numbers. CIHI's internal Privacy Policy and Procedures, 2010 sets out strict controls to ensure that access is approved at the appropriate level and in the appropriate circumstances, and that the principle of data minimization is adhered to at all times. CIHI logs access to data as follows:

- Access to health care numbers and patient names (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 the mandatory Privacy and Security Training Program and through ongoing communications about CIHI's privacy and security policies and procedures. Employees attempting to access a CIHI information system must confirm, prior to each logon attempt, their understanding that they may not access or use the computer system without CIHI's express prior authority or in excess of that authority.

CIHI is committed to safeguarding its information technology ecosystem, securing its data holdings and protecting information with administrative, physical and technical security safeguards appropriate to the sensitivity of the information. Audits are an important component of CIHI's overall Information Security Program; they are intended to ensure that best practices are being followed and to assess compliance with all information security policies, procedures and practices implemented by CIHI. Audits are used to assess, among other things, the technical compliance of information-processing systems with best practices and published architectural and security standards; CIHI's ability to safeguard its information and information-processing systems against threats and vulnerabilities; and the overall security posture of CIHI's technical infrastructure, including networks, servers, firewalls, software and applications.

An important component of CIHI's Audit Program is regular third-party vulnerability assessments and penetration tests of its infrastructure and selected applications. All recommendations resulting from third-party audits are tracked in the Corporate Action Plan Master Log of Recommendations, and action is taken accordingly.

3.10 Principle 8: Openness about the management of personal health information

CIHI makes information available about its privacy policies, data practices and programs relating to the management of personal health information. Specifically, CIHI's Privacy and Security Framework and Privacy Policy, 2010 are available to the public on its corporate website (cihi.ca).

3.11 Principle 9: Individual access to, and amendment of, personal health information

Personal health information held by CIHI is not used by CIHI to make any administrative or personal decisions affecting individuals. Requests from individuals seeking access to their personal health information will be processed in accordance with sections 60 to 63 of CIHI's Privacy Policy, 2010.

3.12 Principle 10: Complaints about CIHI's handling of personal health information

As set out in sections 64 and 65 of CIHI's Privacy Policy, 2010, questions, concerns or complaints about CIHI's handling of information are investigated by the chief privacy officer, who may direct an inquiry or complaint to the privacy commissioner of the jurisdiction of the person making the inquiry or complaint.

4 Conclusion

CIHI's assessment of CPERS 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: Overview of the data flows for CPERS

This figure shows the flow of CPERS data into the CPERS program, within CIHI and out of the program.

Following discharge from hospitals, inpatients who received medical, surgical or maternity care are surveyed via phone, or mailed hard-copy or electronic surveys by data providers (e.g., hospitals, health regions, ministries of health, health councils and/or third-party vendors) to collect information about their experience based on the CPES-IC. The collected CPERS data is submitted electronically through CIHI's secure file submission service to CIHI for processing, which includes activities such as data validation and data quality checks for errors and inconsistencies. Submission reports are returned to data providers for review, and data providers are required to correct files with identified errors and inconsistencies

Following data validation and data quality processing, CPERS data is processed into the CPERS database. The data file is then used by CIHI staff for analysis and can be linked with other CIHI data holdings such as the Discharge Abstract Data for the delivery of customized aggregate and/or record-level data and reports.

help@cihi.ca

CIHI Ottawa
495 Richmond Road
Suite 600
Ottawa, Ont.
K2A 4H6
613-241-7860

CIHI Toronto
4110 Yonge Street
Suite 300
Toronto, Ont.
M2P 2B7
416-481-2002

CIHI Victoria
880 Douglas Street
Suite 600
Victoria, B.C.
V8W 2B7
250-220-4100

CIHI Montréal
1010 Sherbrooke Street West
Suite 602
Montréal, Que.
H3A 2R7
514-842-2226

cihi.ca

22790-1020