



Canadian Patient Cost Database

Privacy Impact Assessment

January 2019



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.

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

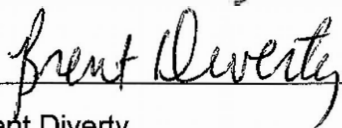
© 2019 Canadian Institute for Health Information

Cette publication est aussi disponible en français sous le titre *Base de données canadienne sur les coûts par patient : évaluation des incidences sur la vie privée, janvier 2019*.

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 Cost Database**

Approved by:



Brent Diverty
Vice President, Programs



Rhonda Wing
Chief Privacy Officer & General Counsel

Ottawa, January 2019

Table of contents

Quick facts about the Canadian Patient Cost Database.	5
1 Introduction	6
2 Background	7
2.1 Introduction to the CPCD	7
2.2 Data collection	8
2.3 Data flow	12
3 Privacy analysis	14
3.1 Privacy and Security Risk Management Program	14
3.2 Authorities governing CPCD data	15
3.3 Principle 1: Accountability for personal health information	16
3.4 Principle 2: Identifying purposes for personal health information	17
3.5 Principle 3: Consent for the collection, use or disclosure of personal health information	17
3.6 Principle 4: Limiting collection of personal health information	18
3.7 Principle 5: Limiting use, disclosure and retention of personal health information	18
3.8 Principle 6: Accuracy of personal health information	22
3.9 Principle 7: Safeguards for personal health information	22
3.10 Principle 8: Openness about the management of personal health information.	24
3.11 Principle 9: Individual access to, and amendment of, personal health information	24
3.12 Principle 10: Complaints about CIHI's handling of personal health information	25
4 Conclusion	25
Appendix: Data quality measures	25

Quick facts about the Canadian Patient Cost Database

1. Patient costing is a health care–specific term describing an activity-based costing model that tracks and costs service delivery to individual service recipients.
2. Patient costing provides detailed financial information by visit that cannot be obtained from departmental management and financial information alone, and it provides a standard for comparisons among health service organizations.
3. Patient cost data has been submitted to the Canadian Institute for Health Information (CIHI) on a voluntary basis since 1994. In 2016–2017, data was received from 4 data providers, representing over 135 health service organizations in Nova Scotia, Ontario, Alberta and British Columbia.
4. The *Standards for Management Information Systems in Canadian Health Service Organizations* (MIS Standards) is a national financial accounting standard that provides the necessary accounting structure for data collection.
5. Data providers submit patient cost data for at least 1 of 5 clinical data holdings: the Discharge Abstract Database–Hospital Morbidity Database (DAD-HMDB), the National Ambulatory Care Reporting System (NACRS), the Continuing Care Reporting System (CCRS), the Ontario Mental Health Reporting System (OMHRS) and the National Rehabilitation Reporting System (NRS).
6. For each patient encounter, health service organizations submitting to the Canadian Patient Cost Database (CPCD) generate a joint record that contains both clinical and patient cost data. To limit the transmission of clinical data, and to reduce data submission burden, data providers disassemble the records and submit them to CIHI separately. Clinical data is reported separately to the relevant CIHI database.
7. The CPCD currently holds more than 2 billion records and grows by approximately 400 million records every year.
8. The CPCD is designed to accept only patient-level cost data and, where necessary and approved, to reassemble or link it to existing records in clinical databases held by CIHI.
9. Patient cost data disclosed to CIHI does not include personal health information but contains other meaningless but unique numbers (identifiers) such as batch number, abstract number and record identifier.

10. Currently, the created CPCD file is used by CIHI to
 - a. Adjust case-mix grouping methodologies for inpatients and ambulatory care patients, and to calibrate Resource Intensity Weights (RIWs);
 - b. Support other CIHI products using case-mix tools, such as the Patient Cost Estimator;
 - c. Calculate the functional area RIW proportions;
 - d. Support the development of new products, such as the Population Grouping Methodology;
 - e. Calculate outpatient reimbursement rates and high-cost procedure rates (e.g., transplants) to support the Interprovincial Health Insurance Agreements Coordinating Committee (IHIACC);
 - f. Respond to third-party data requests; and
 - g. Support health care system planning in Canada.

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 Cost Database (CPCD), including its ongoing expansion in terms of an increased volume of records and greater diversity in the types of service recipients. This PIA, which replaces the 2012 version, 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 CPCD, and 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

Universal health care is a priority for Canadians, and health care expenditures represent a significant share of gross domestic product, estimated at 11.3% in 2018. It is the single largest program administered by provincial and territorial governments. As such, the cost of health care is a topic of considerable interest to Canadians, federal and provincial/territorial governments, and every health care facility tasked with front-line delivery of services.

Product costing is an essential tool in all industries, as a means of identifying cost components that can be addressed specifically in order to reduce product cost by purchasing, redesigning, reengineering, retooling, packaging and other interventions by management at whatever stage. In the health care industry, this is referred to as patient costing, a health care-specific term describing an activity-based costing model that tracks and costs service delivery to individual service recipients.

Patient costing is conducted in a variety of health care settings, both hospital and non-hospital,ⁱ by health service organizations. The objective of patient costing is to determine the cost of the care delivered to each service recipient by determining the cost of the services provided and allocating them to each recipient. In other words, patient costing is the process of estimating the actual cost of care for individual service recipient encounters, such as inpatient admissions, emergency visits, ambulatory visits and health centre visits.

2.1 Introduction to the CPCD

Patient cost data has been submitted to CIHI on a voluntary basis since 1994. In 2016–2017, data was received from over 135 health service organizations in Nova Scotia, Ontario, Alberta and British Columbia. Data is collected at the facility level in accordance with a national financial accounting standard: the *Standards for Management Information Systems in Canadian Health Service Organizations* (MIS Standards). The MIS Standards provides the necessary accounting structure and is already in place at most health service organizations in Canada.

The database currently holds more than 2 billion records and grows by approximately 400 million records annually. Every year, CIHI receives requests from organizations interested in understanding, and potentially undertaking, patient costing activities.

i. Examples of non-hospital health service organizations where patient costing may be conducted include long-term care facilities and inpatient rehabilitation facilities.

For each patient encounter, health service organizations submitting to the CPCD generate a joint record that contains both clinical and patient cost data. To limit the transmission of clinical data, and to reduce data submission burden, data providers disassemble the records and submit them to CIHI's clinical databases and the CPCD separately. For example, inpatient hospital data is submitted to the DAD on a monthly basis, and the associated patient cost records are submitted annually to the CPCD.

Data providers submit patient cost data for at least 1 of 5 clinical data holdings: the DAD (Discharge Abstract Database), NACRS (National Ambulatory Care Reporting System), CCRS (Continuing Care Reporting System), OMHRS (Ontario Mental Health Reporting System) and the NRS (National Rehabilitation Reporting System). Each patient encounter is described by a series of records, which are unique at the service date and cost-type levels.

CIHI links the patient cost records to the appropriate clinical databases, resulting in production of a CPCD file that contains cost data enriched with some clinical and case-mix information. In addition, a unique but meaningless identifier defined by CIHI (e.g., DAD_Transaction_ID for the DAD and Am_Care_Key for NACRS) is added to the file. This identifier can be used to link CPCD data to corresponding clinical records.

Currently, the created CPCD file is used by CIHI to

- Adjust case-mix grouping methodologies for inpatients and ambulatory care patients, and calibrate Resource Intensity Weights (RIWs);
- Support other CIHI products using case-mix tools, such as the Patient Cost Estimator;
- Calculate the functional area RIW proportions;
- Support the development of new products, such as the Population Grouping Methodology;
- Calculate outpatient reimbursement rates and high-cost procedure rates (e.g., transplants) to support the Interprovincial Health Insurance Agreements Coordinating Committee (IHIACC);
- Respond to third-party data requests; and
- Support health care system planning in Canada.

2.2 Data collection

Not all health service organizations have patient costing systems. And not all health service organizations that perform patient costing cost every clinical record. Where possible, CIHI works with existing costing facilities to receive their costing data; CIHI works with jurisdictions to recruit new costing facilities. The following table displays the number of organizations that submitted cost data by care type from Nova Scotia, Ontario, Alberta and British Columbia for 2016–2017.

Table 1 Number of organizations submitting cost data by care type, Nova Scotia, Ontario, Alberta and British Columbia, 2016–2017

Province	Number of organizations submitting cost data, by care type*				
	DAD	NACRS	CCRS	OMHRS	NRS
Nova Scotia	8	5	—	—	—
Ontario	59	69	35	46	34
Alberta	17	27	—	—	—
British Columbia	2	1	—	—	—
Total	86	102	35	46	34

Note

* Some hospitals submit data for multiple care types.

— Not applicable/not available.

The MIS Standards provides the standard for financial data collection, and the MIS Patient Costing Methodology provides further detail on how to distribute costs to the patient, known as the encounter level.

Patient-level cost data is submitted at the functional centre (cost centre) level by patient encounter and, in some cases, by date of service. Consequently, there are many records for each patient visit to a health service organization. The information can be summed up to cost periods and cost groups using the service dates and functional centre information.

The following common data elements are submitted directly to the CPCD by data providers for all 5 care types:

Table 2 Common data elements submitted by data providers to the CPCD

Data element	Purpose/rationale
Record Type	Indicates whether the record is a new submission or a correction of a previously submitted record
Record Identification Number	A data provider-generated meaningless but unique number to identify the record and facilitate the submission of correction records
Functional Centre	A subdivision of an organization used in a functional accounting system to record the budget and actual direct expenses, statistics and/or revenues, if any, that pertain to the function or activity being carried out
Cost Group Code	A breakdown of variable and fixed direct and indirect costs into a more detailed grouping, such as medical personnel compensation, using the MIS secondary accounts
Cost Value	A dollar value of the submitted cost record

Data providers do not submit clinical data to the CPCD. However, data providers are expected to submit the necessary information to allow the reassembly or linkage of cost records to the existing clinical data held by CIHI.

The following 5 tables identify the care type–specific data elements submitted to the CPCD, which permit the linkage of cost and clinical data.

Table 3 Inpatient data elements that permit the linkage of cost and clinical data

Data element	Purpose/rationale*
Fiscal Year	The fiscal year of the cost data being submitted
Fiscal Period	The fiscal period of the cost data being submitted
Batch Number	A number generated by the data provider that identifies a group of abstracts. Batches are numbered consecutively so no 2 batches have the same number within a reporting period for the same institution code.
Institution Code	A 5-digit code assigned to a reporting facility by a provincial/territorial ministry of health identifying the facility and the level of care of the data being submitted
Abstract Number	A number generated by the data provider that identifies each abstract within a batch. Abstracts are numbered consecutively within a batch.
Province Code	Identifies the province/territory of the facility for which the data is being submitted

Note

* Definitions for linkage variables have been developed by each of CIHI's clinical database program areas. Thus there may be differences in definition and nomenclature from one series of linkage variables to another.

Table 4 Ambulatory data elements that permit the linkage of cost and clinical data

Data element	Purpose/rationale
Fiscal Year	The fiscal year of the cost data being submitted
Fiscal Period	The fiscal period of the cost data being submitted
Facility's Ambulatory Care Number	The number assigned to facilities by the provincial/territorial ministry of health
Abstract Identification Number	A number generated by the vendor's software system that allows for the unique identification of each abstract submitted

Table 5 Continuing care data elements that permit the linkage of cost and clinical data

Data element	Purpose/rationale
Facility Code	A 5-character code assigned by a provincial/territorial government to identify a facility
Unique Registration Identifier	A 20-digit number assigned by the vendor's software system that uniquely identifies a resident admission. It consists of the facility number, a digit date and a digit number. It cannot contain a health card number, date of birth or any other personal identifier.
Assessment Type Code	Identifies the type of assessment conducted (annual full assessment, quarterly assessment, etc.)
Assessment Reference Date	The last day of the resident's observation period

Table 6 Rehabilitation data elements that permit the linkage of cost and clinical data

Data element	Purpose/rationale
Fiscal Year	The fiscal year of the cost data being submitted
Facility Number	A 5-character code assigned to identify the facility
Admission Date	The day the person was admitted to a facility/agency for services
Chart Number	A unique number assigned to a patient by the facility to differentiate an individual within a given facility. It is not the same as the individual's provincial/territorial Health Card Number. A person's Chart Number remains unchanged with multiple admissions, readmissions and discharges within a given facility.

Table 7 Mental health data elements that permit the linkage of cost and clinical data

Data element	Purpose/rationale
Facility Number	A 5-character code assigned to identify the facility
Chart Number	A unique number assigned to a patient by the facility to differentiate an individual within a given facility. It is not the same as the individual's provincial/territorial Health Card Number. A person's Chart Number remains unchanged with multiple admissions, readmissions and discharges within a given facility.
Case Record Number	A unique admitting number assigned to a patient by the facility upon admission. It cannot identify an individual on its own.
Assessment Type Code	Identifies the type of assessment conducted (short-stay assessment, quarterly assessment, etc.)
Assessment Reference Date	The last day of the resident's observation period

2.3 Data flow

Following is a description of CPCD data flow, which is illustrated in Figure 1.

Data submission

Annually, data providers submit a full year of costing data for the previous fiscal year to CIHI for each clinical data holding (the DAD, NACRS, CCRS, OMHRS and the NRS) through CIHI's secure electronic Data Submission Services (eDSS).

Data validation

The system validates the content of the data submission against established edit rules based on standards set out in documents, such as the MIS Standards for data collection and the MIS Patient Costing Methodology. Records are accepted or rejected based on the validations (e.g., invalid field values, duplicate records). Submission-specific error reports are generated for access through CIHI's website by the submitting facility to identify rejected records and the reason for rejection. Facilities use these reports to address the deficiencies and resubmit corrected records via the eDSS. The process repeats and new submission reports are generated for the clients until the data is satisfactory to both CIHI and the clients.

Data linkage

The validated patient cost data is reassembled (linked) with the clinical data by taking a cut of the CPCD data, which includes the data holding encounter keys, and linking/matching these keys to the specific clinical data holding for the fiscal year. The result is a file that contains the CPCD costing data enriched with a unique identifier defined by CIHI (e.g., DAD_Transaction_ID for the DAD, Am_Care_Key for NACRS). CPCD data or linked data sets used for internal CIHI analysis purposes do not contain names or direct identifiers, such as unencrypted health care numbers.

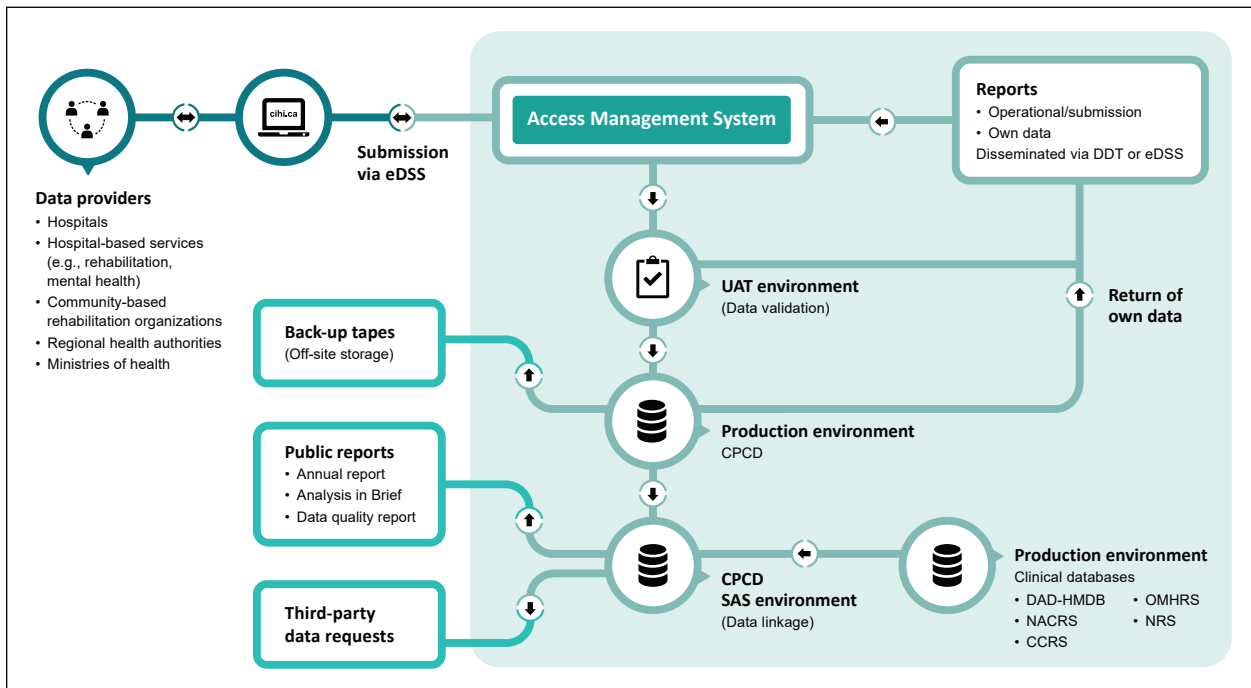
Data quality

Once the cost and clinical data is linked, the data is put through an intensive set of data quality checks. These checks, listed in the appendix, are based on the indicators reported in the CPCD Provincial/Territorial Data Quality reports as well as those identified as important by CPCD stakeholders. The process is managed by program area analysts in SAS; it results in Excel outputs that are shared with the clients via DDT. Clients are given an opportunity to correct and resubmit their data if deemed necessary.

Analysis

The linked CPCD data is used for various analytical purposes. One of the major purposes is the annual update of RIWs in CIHI's case-mix products. The RIW forms the backbone of estimates used in costing of most activities, including the Patient Cost Estimator tool and the Cost of a Standard Hospital Stay indicator. Other CIHI health planning tools rely on patient cost data, including the Comprehensive Ambulatory Classification System and Case Mix Group+ (the acute inpatient methodology).

Figure 1 Canadian Patient Cost Database data flow



3 Privacy analysis

3.1 Privacy and Security Risk Management Program

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

Privacy and security risks may be identified from a variety of sources, including PIAs. Once identified, risks are entered into the Privacy and Security Risk Register and categorized as **high, medium** or **low** based on the likelihood and impact of a risk event.

- **High:** High probability of risk occurring and/or controls and strategies are not reliable or effective.
- **Medium:** Medium probability of risk occurring and/or controls and strategies are somewhat reliable or effective.
- **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 how serious a risk is. A higher risk ranking indicates a more serious threat and a greater imperative for treatment. Once an initial risk treatment is applied, the residual risk (the new calculation of the likelihood and impact of the risk given the treatment) is assessed and compared against CIHI's privacy and security risk tolerance statement, which indicates that CIHI's privacy and security risk tolerance is low. If the risk score for the residual risk is still greater than low, additional risk treatment is necessary until the risk is low or the untreated/residual risk is accepted by CIHI's Senior Management Committee on behalf of the corporation.

3.2 Authorities governing CPCD 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.

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

Agreements

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

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

Table 8 identifies key internal senior positions with responsibilities for CPCD data in terms of privacy and security risk management:

Table 8 Key positions and responsibilities

Position/group	Roles/responsibilities
Vice President, Programs	Responsible for the overall strategic direction of the Patient Cost Program
Director, Spending, Primary Care and Strategic Initiatives	Responsible for overall operations and strategic business decisions regarding the CPCD
Manager, Financial Standards and Information	Responsible for decisions regarding the CPCD and CPCD data dissemination
Program Lead, Financial Standards and Information	Responsible for day-to-day decisions regarding the CPCD and manages the team of analysts who work with the CPCD daily and complete the data management-related processes
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

3.4 Principle 2: Identifying purposes for personal health information

The CPCD does not collect personal health information.

The purpose of the CPCD is clearly outlined in this PIA (see [Section 2.1](#)) and in methodological documents currently available on CIHI's website.

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

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

3.6 Principle 4: Limiting collection of personal health information

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

The data elements collected and their purpose are consistent with the MIS Standards for data collection and the MIS Patient Costing Methodology. The CPCD does not collect personal health information.

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

Limiting use

CIHI limits the use of CPCD data to authorized purposes, as described in [Section 2.1](#). 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.

CPCD data or linked data sets used for internal CIHI analysis purposes do not contain names or direct identifiers, such as unencrypted health care numbers.

Data linkage

The CPCD is designed to accept patient-level cost data and, where necessary and approved, to reassemble or link it to existing records in clinical databases. The CPCD does not contain personal health identifiers. The linkage between cost and clinical data is developed using the data elements listed in tables 3 to 7 above. While the clinical databases contain encrypted Health Card Numbers and other identifiers such as postal code and date of birth, these elements are not retained for analytical use of the linked file. Instead, a meaningless transaction number that is common between cost and clinical data is used to develop and maintain linkage. Additionally, the resulting linked data set includes the following: admission- and discharge-related data elements, patient demographics, traceable supplies and drug costs, direct and indirect costs, fixed and variable costs, and clinical information related to the relevant grouping methodology.ⁱⁱ

Sections 14 to 31 of CIHI's [Privacy Policy, 2010](#) govern linkage of records of personal health information. Pursuant to this policy, CIHI permits the linkage of personal health information under certain circumstances. Data linkage within a single data holding for CIHI's own purposes is generally permitted. Data linkage across data holdings for CIHI's own purposes and all third-party requests for data linkage are subject to an internal review and approval process. When carrying out data linkages, CIHI will generally do so using consistently encrypted Health Card Numbers. The linked data remains subject to the use and disclosure provisions in CIHI's [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 associated with the personal health information.
- 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.
- f. The data linkage has demonstrable savings over other alternatives or is the only practical alternative.

ii. Occasionally, the need will arise to retain some patient identifiers such as chart number for analytical purposes; in those cases, the reason will be documented.

The proposal to link CPCD cost data to clinical data in the 5 care types was presented to CIHI's Privacy, Confidentiality and Security team in August 2011. The proposal was approved based on the assessment that all necessary criteria stipulated in Section 24 of CIHI's [Privacy Policy, 2010](#) had been met. In addition, the CPCD program area was identified as having an ongoing need for linked data (see 2e above). Thus sections 28 and 29 will apply when the linked data is no longer required to meet the identified purposes of the program area.

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 Province/Territory That Issued 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 *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.

On an annual basis, CIHI makes available to data providers reports on the outcome of their data submissions, including details of records that contain errors, in order for these organizations to investigate and, where necessary, correct and resubmit data.

Limiting disclosure

Third-party data requests

Customized de-identified record-level and/or aggregated data from the CPCD may be requested by a variety of third parties.

CIHI administers a third-party data request program that contains and establishes privacy and security controls that must be met by the recipient organization. Furthermore, as set out in sections 45 to 47 of CIHI's [Privacy Policy, 2010](#), CIHI's data disclosures are made at the highest degree of anonymity possible while still meeting the research and/or analytical purposes of the requester. This means that, whenever possible, data is aggregated. When aggregated data is not sufficiently detailed for the intended purpose, record-level data that has been de-identified may be disclosed to the recipient on a case-by-case basis, when the recipient has entered into a data protection agreement or other legally binding instrument with CIHI. Only those data elements necessary to meet the intended purpose may be disclosed.

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 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 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 de-identified record-level data strictly confidential and not disclose such data to anyone outside the organization. Moreover, CIHI imposes obligations on these third-party recipients, including

- Secure destruction requirements;
- CIHI's right to audit;
- Restriction 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 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 — Privacy and Legal Services 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 of CPCD data

As part of its mandate, CIHI publicly releases aggregate 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](#). Aggregate statistics and analyses (e.g., Functional Area RIWs) are made available in publications and on CIHI's website.

Limiting retention

The CPCD 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 (see also Destruction of linked data in Section 3.7).

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 CPCD 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 CPCD 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 CPCD 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 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 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

This assessment summarizes the privacy implications associated with the current operations of the CPCD. No privacy risks were identified in this assessment.

This PIA will be updated or renewed in compliance with CIHI's [Privacy Impact Assessment Policy](#).

Appendix: Data quality measures

List of measures reported in the annual CPCD Provincial/Territorial Data Quality Report and the CPCD Preliminary Data Quality Report

Contextual measures

Number of Participating Sites

Number of Costed Abstracts

Accuracy and reliability

Completeness of Participation: Records

Coverage of Costed Abstracts: Submitting Organizations

Records Rejected Due to Hard Edits

Consistency of Data Submission

 Sites reporting data in previous year and not in current year

 Sites reporting data in current year and not in previous year

Reporting of Nursing Costs Inpatient Services

Comparability and coherence

Compliance With MIS Chart of Accounts



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

19280-0219

