Canadian Patient Cost Database: Privacy Impact Assessment, August 2012

Canadian Institute for Health Information

Institut canadien d'information sur la santé

Our Vision

Better data. Better decisions.
Healthier Canadians.

Our Mandate

To lead the development and maintenance of comprehensive and integrated health information that enables sound policy and effective health system management that improve health and health care.

Our Values

Respect, Integrity, Collaboration, Excellence, Innovation

CIHI is pleased to publish the following Privacy Impact Assessment pursuant to its Privacy Impact Assessment Policy:

Canadian Patient Cost Database (CPCD)
Privacy Impact Assessment

Approved by:

Jean-Marie Berthelot
Vice President, Programs

Anne-Mari Phillips
Chief Privacy Officer & General Counsel

Ottawa – August 2012

Table of Contents

10 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 CIHI on a voluntary basis since 1994. In 2009–2010, data was received from four data providers, representing more than 50 health service organizations in Ontario, Alberta and British Columbia.
4. The *Standards for Management Information Systems in Canadian Health Care 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 one of five clinical data holdings: the Discharge Abstract Database (DAD), National Ambulatory Care Reporting System (NACRS), Continuing Care Reporting System (CCRS), Ontario Mental Health Reporting System (OMHRS) and National Rehabilitation Reporting System (NRS).
6. For each patient encounter, health service organizations submitting to the Canadian Patient Cost Database (CPCD) generate a single record that contains both clinical and patient cost data. To limit the transmission of clinical data and reduce data submission burden, data providers disassemble the records and submit them to the Canadian Institute for Health Information (CIHI) separately.
7. Clinical data is reported separately to the relevant CIHI database.
8. The CPCD is designed to accept only patient-level cost data and reassemble or link it to existing records in clinical databases held by CIHI that contain personal health information.
9. Patient cost data disclosed to CIHI does not include personal health information, and once linked by CIHI, CPCD files are de-identified by removing patient identifiers.
10. The created CPCD file is used by CIHI to
    a. Calculate case-mix products including grouping methodologies for inpatients and ambulatory care patients and Resource Intensity Weights (RIWs);
    b. Support other CIHI products using case-mix tools, such as the Patient Cost Estimator;
    c. Develop new products, for example, functional area proportions;
    d. Calculate interprovincial reimbursement rates to support the Interprovincial Health Insurance Agreements Coordinating Committee; and
    e. Support health care system planning in Canada.

1 Introduction

The Canadian Institute for Health Information (CIHI) is an independent, not-for-profit organization established to collect and analyze essential information on health and health care in Canada. Its mandate is the provision of timely, accurate and comparable information to inform health policies, support the effective delivery of health services and raise awareness among Canadians of the factors that contribute to good health.

CIHI obtains data directly from hospitals, regional health authorities and ministries of health, including personal health information about recipients of health services, registration and practice information about health professionals and health facility information. CIHI's data and reports focus on health care services, health spending, health human resources and population health.

In 2008, the Canadian Patient Cost Database (CPCD) program area and database were established to perform analyses on patient cost data, providing a number of products and tools used by CIHI, health authorities and third-party researchers to support health care management and planning in Canada. The database recently completed a major redevelopment to address a planned increase in the volume (200% by 2015) and complexity of data submitted by data providers, as well as to standardize data inputs.

1.1 PIA Objectives and Scope

The purpose of this privacy impact assessment (PIA) is to identify the potential privacy, confidentiality and security risks associated with the re-engineering of processes to accommodate an expansion of the CPCD in terms of both an increased volume of records and greater diversity in the types of service recipients being included in costing approaches.

The information flow in focus for this assessment is that from submission of patient cost data to CIHI by data providers, the provision of error reports to the data providers, the linkage of cost data to existing clinical data holdings, statistical analysis and public release of aggregate data, and the release of data to third parties through CIHI's data request process.

This assessment is based on the privacy principles set out in the Canadian Standards Association's *Model Code for the Protection of Personal Information* as they apply to the CPCD. Its key goal is to effectively communicate the privacy risks not addressed through other organizational mechanisms. The PIA is intended to contribute to senior management's ability to make fully informed policy and system design decisions.

1.2 Reference Documents

The following documents were referenced in the development of this privacy impact assessment:

- CPCD Upgrade Project, Business Requirements, October 24, 2011
- CPCD Functional Specifications, Revision 1.2.1, December 21, 2011
- Canadian Patient Cost Database Technical Document: MIS Patient Costing Methodology, November 2011

- Privacy Impact Assessment, Clinical Administrative Databases (Draft), December 2011
- Privacy Impact Assessment, Continuing Care Reporting System, 2006
- Privacy Impact Assessment, National Rehabilitation Reporting System, July 20, 2009
- Privacy Impact Assessment, Ontario Mental Health Reporting System, September 2011
- Canadian Institute for Health Information Privacy Policy on the Collection, Use, Disclosure and Retention of Personal Health Information and De-Identified Data, 2010 (Revised 2011)

2 Canadian Patient Cost Database

2.1 Background

Universal health care is a priority for Canadians, and health care expenditures represent a significant share of GDP, estimated at 12% in 2011. 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 all Canadians, and not least to 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, re-engineering, 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.

Patient cost data has been submitted to CIHI on a voluntary basis since 1994. In 2009–2010, data was received from four data providers, representing more than 50 health service organizations in 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 Care Service Organizations* (MIS Standards). The MIS Standards provides the necessary accounting structure and is already in place at most health service organizations in Canada.

i. Examples of non-hospital health service organizations where patient costing may be conducted include long-term care facilities, rehabilitation facilities and community care access centres (Ontario).

With an increasing focus on the cost of health care, the number of organizations submitting data to the CPCD has been growing by approximately 20% per year and the number of records is expected to double by 2015. The number of records submitted in 2009 alone was 35 million.

For each patient encounter, health service organizations submitting to the CPCD generate a single record that contains both clinical and patient cost data. To limit the transmission of clinical data and reduce data submission burden, data providers disassemble the records and submit them to CIHI separately. For example, inpatient hospital data is submitted to the Discharge Abstract Database (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 one of five clinical data holdings: the DAD, National Ambulatory Care Reporting System (NACRS), Continuing Care Reporting System (CCRS), Ontario Mental Health Reporting System (OMHRS) and National Rehabilitation Reporting System (NRS). Each patient encounter is described by a series of records, which are unique at the date and cost type level.

CIHI uses the patient cost records to link to the appropriate clinical databases, resulting in production of a CPCD file that contains cost data enriched with a number of clinical data elements. This file is used for various analytical purposes, as follows:

- Calculation of case-mix products, including grouping methodologies for inpatients and ambulatory care patients, and Resource Intensity Weights (RIWs);
- Supporting other CIHI products using case-mix tools (for example, the Patient Cost Estimator);
- Developing new products (such as functional area proportions);
- Calculation of interprovincial reimbursement rates; and
- Supporting health care system planning in Canada.

2.2 Information Collected for the CPCD

The CPCD is designed to accept patient-level cost data from all health service organizations. Currently, the following five care types are represented in the data being provided to the CPCD: inpatient, ambulatory, continuing care, rehabilitation and mental health. In addition, the design allows for reassembly or linking of these individual cost records with the related demographic and clinical information from the existing CIHI clinical databases for each of the five care types.

Since not all hospitals are patient costing hospitals, the CPCD's initial goal is to receive data from all hospitals that are costing hospitals. CIHI is working with each jurisdiction to recruit new costing facilities once they become operational. The following table displays the number of organizations submitting cost data by care type from Ontario, Alberta and British Columbia for 2009.

Table 1: Organizations Submitting Cost Data, by Care Type, Ontario, Alberta and British Columbia, 2009

Province	Care Type	Number of Costing Sites*
Alberta	DAD	16
Alberta	NACRS	12
British Columbia	DAD	4
British Columbia	NACRS	4
Ontario	DAD	38
Ontario	NACRS	43
Ontario	CCRS	11
Ontario	OMHRS	20
Ontario	NRS	20

Note

* Some hospitals have multiple sites.

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, or 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 five care types:

Table 2: Common Data Elements Submitted by Data Providers to the CPCD

Data Element	Purpose/Rationale
Record Type	The record type indicates whether the record is a new submission or is correcting a previously submitted record.
Record Identification Number	The record identification number is a data provider–generated meaningless but unique number (MBUN) to identify the record and facilitate the submission of correction records.
Functional Centre	The functional centre is 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	The cost group code is 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	The cost value is a dollar value of the submitted cost record.

Data providers do not submit clinical data to the CPCD. However, data providers must submit the necessary information to allow the reassembly or linkage of cost records to the existing clinical data held by CIHI. The following five tables identify the care type–specific data elements submitted to the CPCD, which permit the linkage of cost and clinical data.

Table 3: Data Elements That Permit the Linkage of Cost and Clinical Data—Inpatient

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	The batch number is used to identify a group of abstracts. Batches are numbered consecutively so no two batches have the same number within a reporting period for the same institution code. This number is generated by the data provider.
Institution Code	The institution code is a five-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	The abstract number is the identification number of each abstract within a batch. The abstracts are numbered consecutively within a batch. This number is generated by the data provider.
Province Code	The 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: Data Elements That Permit the Linkage of Cost and Clinical Data—Ambulatory

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 facility's ambulatory care number is the number assigned to facilities by the provincial/territorial ministry of health.
Abstract Identification Number	The abstract identification number allows for the unique identification of each abstract submitted. This number is generated by the software vendor's system.

Table 5: Data Elements That Permit the Linkage of Cost and Clinical Data—Continuing Care

Data Element	Purpose/Rationale
Facility Code	The facility code is a five-character code assigned by a provincial/territorial government to identify a facility.
Unique Registration Identifier	The unique registration identifier uniquely identifies a resident admission. It is a 20-digit number consisting of the facility number, a digit date and a digit number. This number is assigned by vendor software's system. The unique registration identifier cannot contain a health card number, date of birth or any other personal identifier.
Reason for Assessment	The reason for assessment identifies the reason and type of assessment conducted (annual full assessment, quarterly assessment, etc).
Assessment Reference Date	The assessment reference date records the last day of the resident's observation period.

Table 6: Data Elements That Permit the Linkage of Cost and Clinical Data—Rehabilitation

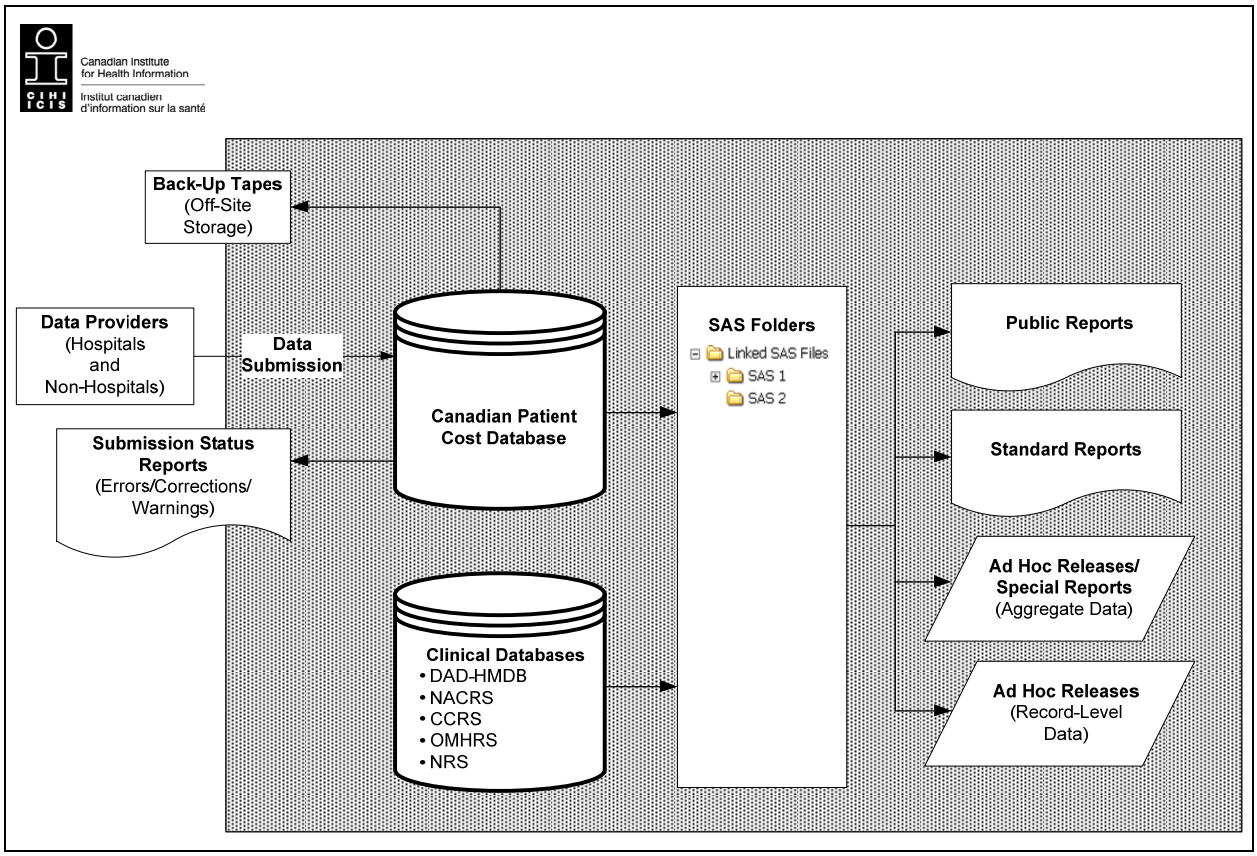
Data Element	Purpose/Rationale
Fiscal Year	The fiscal year of the cost data being submitted.
Facility Number	The facility number is a five-character code assigned to identify the facility.
Admission Date	The admission date records the day the person was admitted to a facility/agency for services.
Chart Number	The chart number is the person's unique identification number as assigned by the provider/delivery organization.

Table 7: Data Elements That Permit the Linkage of Cost and Clinical Data—Mental Health

Data Element	Purpose/Rationale
Facility Number	The facility number is a five-character code assigned to identify the facility.
Chart Number	The Chart Number (CN) is a unique number assigned to a patient by the facility and is not the same as the individual's provincial/territorial health card number. It is required to differentiate an individual within a given facility. The CN for a person remains unchanged with multiple admissions, readmissions and discharges within a given facility.
Case Record Number	The Case Record Number (CRN) is a unique admitting number assigned to patients by the facility upon admission. It cannot identify an individual on its own.
Record Type	The record type code identifies the type of assessment conducted (short-stay assessment, quarterly assessment, etc.).
Assessment Reference Date	The assessment reference date records the last day of the resident's observation period.

2.3 CPCD Data Flow

Figure 1: Canadian Patient Costing Database (CPCD) Data Flow Diagram



Data Submission

Participating health facilities submit a full year of costing data to CIHI for each clinical data holding (DAD, NACRS, CCRS, OMHRS, NRS). Submissions are for the previous fiscal year. Submission is through CIHI's secure electronic Data Submission Services (eDSS). Successful data submissions are moved to CIHI's secure processing environment for further processing.

Data Validation

The system validates the content of the data submission against specified business rules. Records are accepted or rejected based on the validations. Submission-specific error reports are generated for access through CIHI's Common Data Dissemination Services (CDDS) by the submitting facility identifying rejected records and the reason for rejection. The facilities use these reports to address the deficiencies and resubmit corrected records via the eDSS.

Data Linkage

The validated CPCD cost data is reassembled 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 number of clinical data elements (for example, transaction_id, RIW, CMG+ code, most responsible diagnosis main interventions, length of stay, age group).

Analysis

The linked CPCD is used for various analytical purposes. One of the major purposes is the annual Resource Intensity Weight (RIW) methodology process. The RIW forms the backbone of estimates used in the costing of most activities, including the Patient Cost Estimator and the cost per weighted case. Other CIHI health planning tools rely on the patient cost data, including the case-mix grouping methodology, the Comprehensive Ambulatory Classification System and the Day Procedure Groups. Upon completion of these analytical processes, the records used for the RIW process are identified and flagged, and those flags are imported into the CPCD system. Matching records are updated to indicate that they were used in the RIW methodology. Any unmatched records are identified in a report available to the program area.

3 Privacy Analysis

3.1 Authorities Governing CIHI and the CPCD

General

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

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.

All provinces and territories have public-sector privacy legislation in place. Canadian privacy legislation includes provisions that authorize public bodies covered by the acts to disclose person-identifiable data, without the consent of the individual, for statistical purposes. Alberta, Saskatchewan, Manitoba, Ontario, New Brunswick and Newfoundland and Labrador (legislation pending in Nova Scotia) also have health information–specific privacy legislation with express lawful authority to use and disclose personal health information, without individual consent, for purposes of management of the health system, including statistical analysis and reporting.

For example, CIHI is recognized as a prescribed entity under the *Personal Health Information Protection Act* (the Act) of Ontario. 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.

Agreements

As indicated above in Section 2.3, the data flows directly into CIHI via existing applications/ systems from data providers—for example, from provincial and territorial ministries of health, regional health authorities and other entities responsible for delivery and/or administration of publicly funded programs. For the most part, these existing data flows are governed by CIHI's *Privacy Policy, 2010*, existing legislation in the jurisdictions and data-sharing agreements with the provinces and territories. The data-sharing agreements set out the purpose, use, disclosure, retention and disposal requirements as well as any subsequent data sharing which may be permitted. The agreements also describe the legislative authority under which personal health information is disclosed to CIHI.

3.2 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 Team, a Privacy and Data Protection Sub-Committee of its Board of Directors and an external Chief Privacy Advisor.

Organization and Governance

The following table identifies key internal positions and groups with responsibilities for the Canadian Patient Cost Database in terms of privacy and security risk management.

Position/Group	Responsibilities
Vice President, Programs	Responsible for the overall operations and strategic direction of the Patient Cost Program.
Director, Health Spending and Strategic Initiatives	Responsible for strategic business decisions regarding the CPCD.
Vice President and Chief Technology Officer	Responsible for the strategic direction and overall operations/implementation of CIHI's technological and security solutions.
Chief Privacy Officer	Responsible for the strategic direction and the overall implementation of CIHI's privacy program.
Senior Program Consultant, Security	Responsible for providing guidance on maintaining and enhancing security and assisting with documentation such as security impact assessments and threat and risk assessments.
Manager, MIS & Costing	Responsible for decisions regarding the CPCD and CPCD data dissemination.
Program Lead, Patient Costing	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 analysis.

3.3 Principle 2: Identifying Purposes for Personal Health Information

CIHI uses the CPCD for various analytical purposes, as follows:

- Calculation of CIHI's products, including grouping methodologies for inpatients and ambulatory care patients and RIWs;
- Supporting other CIHI products using case-mix tools (for example, the Patient Cost Estimator);
- Developing new products (for example, functional area proportions); and
- Supporting the development of interprovincial reimbursement rates for health services provided out of province.

These uses are clearly outlined in this PIA and in methodological documents available on CIHI's website.

3.4 Principle 3: Consent for the Collection, Use or Disclosure of Personal Health Information

Patient cost data disclosed to CIHI does not include personal health information.

3.5 Principle 4: Limiting Collection of Personal Health Information

CIHI is committed to the principle of data minimization and limits its collection of patient cost data to that which is necessary to support the purposes outlined in Section 3.3 of this PIA. The data elements collected and their purpose are consistent with MIS Standards for data collection and the MIS Patient Costing Methodology. The Canadian Patient Cost Program does not collect personal health information.

3.6 Principle 5: Limiting Use, Disclosure and Retention of Personal Health Information

3.6.1 Limiting Use

CIHI limits the use of patient cost data, including linked files, for authorized purposes as described in Section 3.3. Only authorized staff in the CPCD program area are permitted to access and use patient cost data, including linked files, on a need-to-know basis. All authorized users are made aware of their obligations and responsibilities for privacy and confidentiality. All CIHI staff are required to sign a confidentiality agreement at the commencement of employment and are subsequently required to renew their commitment to privacy yearly.

Data Linkage

The CPCD is designed to accept patient-level cost data and to reassemble or link it to existing records in clinical databases that contain personal health information. Prior to use, the linked datasets are de-identified by removing patient identifiers. Occasionally, the need will arise to retain some patient identifiers, such as chart number, for analytical purposes and in those cases

the reason will be documented. A meaningless transaction number will be used to identify unique records within the linked dataset. The resulting linked datasets will include the following: meaningless transaction number, 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.

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 without using names or personal health 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 Section 24 of CIHI's *Privacy Policy, 2010*, as follows:

(1) The individuals whose personal health information is used for data linkage have consented to the data linkage; or

(2) All of the following criteria are met:

   a. The purpose of the data linkage is consistent with CIHI's mandate;

   b. The public benefits of the linkage significantly offset any risks to the privacy of individuals;

   c. The results of the data linkage will not be used for any purpose that would be detrimental to the individuals that the personal health information concerns;

   d. The data linkage is for a time-limited specific project and the linked data will be subsequently destroyed in a manner consistent with sections 28 and 29; or 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

   e. The data linkage has demonstrable savings over other alternatives or is the only practical alternative.

The proposal to link CPCD cost data to clinical data in the five 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 (2) d. 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.

Section 28 of CIHI's *Privacy Policy, 2010* sets out the requirement that CIHI will destroy personal health information and de-identified data in a secure manner, using destruction methodologies appropriate to the format, media or device, such that reconstruction is not reasonably foreseeable.

Section 29 of CIHI's *Privacy Policy, 2010* further requires that for linked data, secure destruction will occur within one year after publication of the resulting analysis, or three years after the linkage, whichever is sooner, in a manner consistent with CIHI's *Information Destruction Standard*. For linked data resulting from a CIHI ongoing program of work, secure destruction will occur when the linked data is no longer required to meet the identified purposes, in a manner consistent with CIHI's *Information Destruction Standard*. This requirement applies to data linkages for CIHI's own purposes and for third-party data requests.

Return of Own Data

Section 34 of CIHI's *Privacy Policy, 2010* establishes that the return of data to the health care facility that originally provided it to CIHI or the relevant ministry of health is not a disclosure but is considered a use.

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.

3.6.2 Limiting Disclosure

Disclosures to Data Provider Community

CIHI creates and discloses statistics based on the CPCD data and plans to make CPCD data available to the data provider community through a secure web-based application that allows registered users with an online means of trending and comparing utilization and performance indicators with registered users (that is, organizations that submit data to the CPCD and their respective provincial or territorial ministries of health). These reports will include aggregated or de-identified information on the patient demographics, clinical outcomes, service utilization, and quality and performance indicators. They will also include organization-specific reports and reports comparing information across organizations but do not contain any person-identifying information. The reports will be accessed through a secure web-based business intelligence tool that allows users, who will be under an eServices agreement with CIHI, to view and customize reports to suit their business needs. It is important to note that users of the planned CPCD eServices will not have access to health card numbers, dates of birth or full postal codes of recipients of health care services.

Subsets of de-identified data from the CPCD may also be included in CIHI Portal, an analytical web-based tool for health care data, designed by CIHI to provide users, such as hospitals, regional health authorities or ministries of health, with online access to pan-Canadian health care data in a secure environment that safeguards privacy and confidentiality. Clients using CIHI Portal are also required to sign CIHI's eServices agreement that sets out the purpose, use, disclosure and retention of confidential information, including de-identified data and facility-identifiable information, obtained through CIHI Portal.

Public Release of CPCD Data

As part of its mandate, CIHI publishes aggregated data only in a manner designed to minimize any risk of identifiability and residual disclosure. Aggregate statistics and analyses are made available on CIHI's website. This generally requires a minimum of five observations per cell.

Third-Party Data Requests

CIHI administers a third-party data request program, which contains and ensures tight privacy and security controls within the recipient organization. Furthermore, as set out in sections 45 to 47 of CIHI's *Privacy Policy, 2010*, CIHI's data disclosures are made at the highest degree of anonymity possible while still meeting the research and/or analytical purposes of the requester. This means that, whenever possible, data is aggregated. Where aggregate data is not sufficiently detailed for the intended purpose, data that has been de-identified may be disclosed to the recipient on a case-by-case basis, and where 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.

In 2009, CIHI adopted a complete lifecycle approach to data management. As part of that lifecycle, Privacy and Legal Services (PLS) 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 lifecycle. 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.

As of January 2011, in addition to the compliance-monitoring process, which leverages data captured to monitor compliance with data destruction requirements, PLS contacts third-party data recipients on an annual basis to certify that they continue to comply with their obligations as set out in the Third-Party Data Request Form and Data Protection Agreement signed with CIHI.

Data requestors are required to submit a written request. They must also sign an agreement wherein they agree to use the data only for the research 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 five; and
- The use of strong encryption technology.

In rare and exceptional circumstances, CIHI may enter into a data-sharing agreement (DSA) with a third-party for the disclosure of personal health information or de-identified data in situations where CIHI data is requested for a program of work rather than specific research projects, as set out in sections 41.1 and 46.1 of CIHI's *Privacy Policy Procedures, 2010*.

3.6.3 Limiting Retention

Patient cost data, including linked files, forms part of CIHI's information holdings. Consistent with sections 28 and 29 of CIHI's *Privacy Policy, 2010* ("Destruction of Data" and "Including Linked Data"), the linked files created and used by the CPCD for its ongoing program of work will occur when the data is no longer required to meet the identified purposes, in a manner consistent with CIHI's *Information Destruction Standard*.

3.7 Principle 6: Accuracy of Personal Health Information

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

Similar to other CIHI data holdings, the CPCD is subject to a data quality assessment, based on CIHI's Data Quality Framework. This framework provides an objective approach to applying consistent data-flow processes that focus on data quality priorities, assessing the data quality of a data holding, and producing standard data-holding documentation, with the ultimate goal of continuous improvement in data quality for CIHI's data holdings. It considers data quality from a user's perspective, whereby "quality" is defined as "fitness for use." Data quality is assessed based on 19 characteristics rolled up into five dimensions, namely timeliness, usability, relevance, accuracy and comparability. The process to complete the framework contains numerous activities to assess the accuracy of the data.

All patient cost data submitted to the CPCD is validated against established edit rules based on standards set out in documents, such as MIS Standards for data collection and the MIS Patient Costing Methodology. Data providers are notified where records fail validation (for example, invalid field values, duplicate records) through CDDS reports. Data corrections may be submitted. After passing the data quality checks, the data is incorporated into CIHI's production environment.

3.8 Principle 7: Safeguards for Personal Health Information

CIHI Privacy and Security Framework

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

Personnel Security

CIHI fosters and maintains a strong information privacy and data security culture. On initial employment, and, annually thereafter, all CIHI staff must sign confidentiality agreements and complete mandatory privacy and security training.

Physical Security

CIHI's offices provide a secure physical site for information assets and staff through, for example, the use of controlled access to its premises, secured access elevators and restricted access to individual floors requiring multi-factor authentication. Further restrictions are imposed within CIHI's premises to its server rooms/data centres where access is provided only to those employees who require such access for their employment, contractual or other responsibilities.

Data Communications Security

Participating data providers submit the CPCD data to CIHI through use of CIHI's eDSS. The eDSS application uses a secure, encrypted SSL (Secure Sockets Layer) session between CIHI and data providers for the purpose of data transfer. The level of encryption used is considered industry standard and is used for most internet banking and e-commerce applications. The encrypted file transmission from eDSS is maintained in encrypted form and is moved promptly into the protected area, where it is decrypted. The protected area has additional firewalls and is not linked to external-facing servers.

Similarly, CPCD data-providing facilities access online error reports through CIHI's secure, web-based CDDS using an encrypted SSL session. Only authorized users who have signed agreements with CIHI may access the online reports through use of password-protected accounts.

Information Processing Security

The CPCD files reside and are processed on secure servers that are maintained by CIHI's Information Technology and Services Division. Once the data is at CIHI's premises, it is stored in a database on a secure network that is not accessible outside the premises. CIHI's electronic networks, systems and computing devices are restricted to authorized personnel on a need-to-know/access basis. Staff desktop computers are subject to session time-outs that automatically logout a user after a preset period of inactivity, and to technical and procedural barriers preventing unauthorized software from being installed by users. All corporate laptops employ disk encryption, and CIHI's policy on the use of *mobile computing equipment* restricts work that can be completed on mobile equipment.

Audits and Assessments

CIHI is committed to safeguarding its information technology environment, to securing its data holdings and to 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 and are intended to ensure that best practices are being followed and used to assess compliance with all information security policies, procedures and practices implemented by CIHI. Audits are used to assess, among other things, 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 risk register and actioned accordingly.

3.9 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 on its corporate website. As well, this PIA is accessible on CIHI's website (www.cihi.ca).

3.10 Principle 9: Individual Access to, and Amendment of, Personal Health Information

Personal health information held by CIHI is not used by CIHI to make any administrative or personal health decisions affecting the individual. 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*.

3.11 Principle 10: Complaints About CIHI's Handling of Personal Health Information

As set out in sections 64 and 65 of CIHI's *Privacy Policy, 2010*, complaints about CIHI's handling of personal health information are investigated by the Chief Privacy Officer. The Chief Privacy Officer 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 implication associated with the CIHI CPCD Upgrade Project. No privacy risks were identified in this assessment.

Canadian Institute for Health Information
495 Richmond Road, Suite 600
Ottawa, Ontario K2A 4H6

Phone: 613-241-7860
Fax: 613-241-8120
www.cihi.ca
copyright@cihi.ca

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, août 2012*.

Talk to Us

CIHI Ottawa
495 Richmond Road, Suite 600
Ottawa, Ontario K2A 4H6
Phone: 613-241-7860

CIHI Toronto
4110 Yonge Street, Suite 300
Toronto, Ontario M2P 2B7
Phone: 416-481-2002

CIHI Victoria
880 Douglas Street, Suite 600
Victoria, British Columbia V8W 2B7
Phone: 250-220-4100

CIHI Montréal
1010 Sherbrooke Street West, Suite 300
Montréal, Quebec H3A 2R7
Phone: 514-842-2226

CIHI St. John's
140 Water Street, Suite 701
St. John's, Newfoundland and Labrador A1C 6H6
Phone: 709-576-7006

www.cihi.ca
At the heart of data

Canadian Institute
for Health Information

Institut canadien
d'information sur la santé