Patient-Level Physician Billing Repository
Privacy Impact Assessment, January 2015
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
The Canadian Institute for Health Information (CIHI) is pleased to publish the following privacy impact assessment in accordance with its *Privacy Impact Assessment Policy*:

- Patient-level Physician Billing Repository Privacy Impact Assessment, January 2015

Approved by:

Brent Diverty  
Vice President, Programs

Anne-Mari Phillips  
Chief Privacy Officer & General Counsel

Ottawa – January 2015
Table of Contents

Quick Facts About the Patient-Level Physician Billing Repository ............................................... 6

1 Introduction .................................................................................................................................... 7

2 The Patient-Level Physician Billing Repository at CIHI ........................................................... 7
   2.1 Background .......................................................................................................................... 7
   2.2 Data Flow ............................................................................................................................ 8

3 Privacy Analysis ......................................................................................................................... 9
   3.1 Authorities Governing CIHI and the Patient-Level Physician Billing Repository ............. 9
   3.2 Principle 1: Accountability for Personal Health Information ........................................... 10
   3.3 Principle 2: Identifying Purposes for Personal Health Information ................................ 11
   3.4 Principle 3: Consent for the Collection, Use or Disclosure of Personal Health Information .......................................................... 12
   3.5 Principle 4: Limiting Collection of Personal Health Information ...................................... 12
   3.6 Principle 5: Limiting Use, Disclosure and Retention of Personal Health Information .... 14
   3.7 Principle 6: Accuracy of Personal Health Information ................................................... 15
   3.8 Principle 7: Safeguards for Personal Health Information ................................................ 16
   3.9 Principle 8: Openness About the Management of Personal Health Information ........... 16
   3.10 Principle 9: Individual Access to, and Amendment of, Personal Health Information .... 17
   3.11 Principle 10: Complaints About CIHI’s Handling of Personal Health Information ....... 17

4 Privacy Assessment Summary and Conclusion ....................................................................... 17

Appendix ........................................................................................................................................ 18

Reference ....................................................................................................................................... 19
Quick Facts About the Patient-Level Physician Billing Repository

1. The Patient-Level Physician Billing (PLPB) Repository was established to
   - Support patient-focused analysis—age–sex- and morbidity-adjusted health care use by different populations—that currently cannot be conducted easily through other data sources, such as those related to primary care and community mental health;
   - Support CIHI’s development of more comprehensive inpatient cost estimates that include the physician cost and other methodologies and tools to support health services analysis; and
   - Enhance the quality of historical National Physician Database (NPDB) data and indicators (e.g., full-time equivalents, cost per service).

2. The PLPB Repository will collect patient-level provider\(^i\) claims data for services insured under the provincial and territorial medical care plans. The data holding will comprise similar claims data already collected through CIHI’s existing NPDB submission specifications, in addition to personal health information, in the form of health card numbers, as well as diagnosis identifiers and certain service location identifiers where available.

3. Saskatchewan Health (spring 2011) and Alberta Health (spring 2013) initially provided CIHI with 3 years of data to conduct a pilot to demonstrate CIHI’s capacity to use PLPB data to answer a broad range of research questions.

4. The positive results of the pilot work have led to increased support and interest from a number of jurisdictions, leading CIHI to continue to develop a PLPB data collection standard, as well as to seek data from other jurisdictions. Saskatchewan and Alberta subsequently submitted 3 additional years of more current PLPB data. Furthermore, Ontario and British Columbia submitted the same 6 years of data as the other 2 provinces, but it was intended for the exclusive purpose to build a methodology for a population risk adjustment grouping (PRAG), a composite measure of the burden of illness or future use of health services by populations. A privacy impact assessment (PIA) specific to the PRAG project and the various data sources it relies on, including PLPB data, is available separately at www.cihi.ca.

\(^i\) The vast majority (approximately 90%) of the remunerations captured in the PLPB and NPDB relate to services provided by physicians. However, despite the physician-centric label for these systems, information about other service providers (e.g., nurse practitioners) insured under the provincial and territorial medical care plans is also collected in the PLPB Repository and the NPDB. The nomenclature is retained in this PIA in order to align with existing PLPB published documentation and avoid confusion.
1 Introduction

The Canadian Institute for Health Information (CIHI) collects and analyzes information on health and health care in Canada. Its mandate is 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. CIHI obtains data directly from hospitals and other health facilities, long-term care homes, regional health authorities, medical practitioners and governments. This data includes health information about services provided to patients, residents and clients; registration and practice information about health professionals; and health expenditure information.

The purpose of this privacy impact assessment (PIA) is to examine the privacy, confidentiality and security risks associated with the Patient-Level Physician Billing (PLPB) Repository.

The assessment 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 they apply to the development of the database and methods for submitting data to the PLPB Repository.

The primary driver for this PIA is compliance with CIHI’s *Privacy Impact Assessment Policy*.

2 The Patient-Level Physician Billing Repository at CIHI

2.1 Background

The National Physician Database (NPDB) is 1 of 2 pan-Canadian databases specific to physicians at CIHI. The NPDB contains physician-level information on the demographic characteristics of physicians, their remuneration and activity levels. The data is used to report on services provided by physicians and payments made to them by provincial and territorial medical insurance plans.

Historically, in Canada, physicians were paid mostly on a fee-for-service (FFS) basis. Over time, there has been a migration to various non-FFS (alternative) payment plans that are designed to better meet the specific needs of jurisdictions and regional areas. There is considerable detail about a physician’s interactions with patients that is captured in the FFS data but that is not yet available in the non-FFS or alternative payment program (APP) information submitted by the jurisdictions to CIHI. Currently, about 70% of total physician payments are FFS, but this proportion varies considerably by physician specialty and by province and territory. Under the current model of submission, when the FFS data is submitted to CIHI by the provincial and territorial ministries of health, it is aggregated to the physician level. This means that for any fee code in a province or territory’s schedule of fees, payments are aggregated to each physician according to the total payments and number of associated services provided to their male and female patients. The APP data is also typically submitted to CIHI at an aggregate level by most jurisdictions.
A feasibility study on the collection of PLPB data was completed in 2009. The findings of this study confirmed that all provinces and territories collect and maintain PLPB data and use the information to inform policy development and decision-making. In addition, the study confirmed that CIHI’s collection of PLPB data had the potential to significantly improve the data, information and understanding in several areas of stakeholder interest, such as primary health care and the cost of physician services, among others.

Although the data and analysis from the NPDB have served CIHI’s stakeholders well in the past, there has been an ever-growing need for more detailed patient-level physician billing data rather than data rolled-up/aggregated to the physician level. Patient-level information, including a patient’s health card number, would permit linkage of PLPB data to other CIHI databases and open up entirely new areas of analysis focused on patient interactions and their various health care providers across treatment paths and their outcomes.

Saskatchewan Health (spring 2011) and Alberta Health (spring 2013) provided CIHI with 3 years of data to conduct a pilot to demonstrate CIHI’s capacity to use PLPB data to answer a broad range of research questions. This pilot project clearly showed the potential for PLPB data to improve CIHI’s understanding of the information submitted to the NPDB, providing a better understanding of physicians as providers of care, their practices, their levels of compensation including benefits and other practice costs, and practice intensities. The final pilot project reports1, 2 based on Saskatchewan and Alberta data describe the experience and the results of analyses completed using the PLPB data and recommended proceeding with ongoing data submissions from both provinces.

Positive pilot results and increased support and interest from a number of jurisdictions have led to CIHI’s decision to continue development of the PLPB Repository.

### 2.2 Data Flow

Figure 1 illustrates the high-level data flow for the PLPB Repository. Provincial and territorial ministries of health generate provider claims data on the payments they have made to physicians for the insured services that physicians have provided to their patients. For example, physicians submit claims to provincial and territorial medical care plans in order to receive payment for the health services they delivered to patients. The data generated through the primary process of paying physicians is subsequently submitted to CIHI.

CIHI is a secondary data collector of health information. Data will flow directly to CIHI from existing provincial and territorial ministries of health data sources, and CIHI will rely on the submission of data collected by these sources.

CIHI has identified a minimum set of the data elements to be submitted to the PLPB Repository, referred to as the minimum data set (MDS). However, the collection of PLPB data will not be based on CIHI-issued mandatory file submission specifications. Instead, each data provider extracts a jurisdiction-specific data set from its existing data sources that conforms, to the degree possible, with the CIHI MDS.
PLPB data will be submitted to CIHI using CIHI’s secure web-based data submission service. Once received by CIHI, PLPB data files are immediately processed and the jurisdiction-issued health card number in each file is encrypted. Once the health card numbers are encrypted, each jurisdiction-specific PLPB data file is accessed by a limited number of authorized staff for additional processing before the files are transferred to CIHI’s SAS analytical environment.

Authorized CIHI analytical staff access PLPB data via CIHI’s SAS analytical environment. All requests for access to the SAS analytical environment are processed through CIHI’s centralized SAS Data Access process. The process ensures that all requests for access to PLPB data are traceable and authorized. The SAS Data Access process is subject to an annual audit to ensure that staff are accessing data on a need-to-know basis.

3 Privacy Analysis

3.1 Authorities Governing CIHI and the Patient-Level Physician Billing Repository

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. This 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. Newfoundland and Labrador, Nova Scotia, New Brunswick, Ontario, Manitoba, Saskatchewan and Alberta also have health information–specific privacy legislation with express lawful authority to use and disclose personal health information, without individual consent, for purposes of managing the health system, including statistical analysis and reporting.

For example, CIHI is recognized as a prescribed entity under the Personal Health Information Protection 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 in Section 2.2, data will flow directly to CIHI from ministries of health responsible for provider remuneration for services insured under the provincial and territorial medical care plans. Data flow will be governed by CIHI’s Privacy Policy, 2010, existing 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. Where required, existing data-sharing agreements will be updated to include the provision of PLPB data to CIHI, prior to the submission of data 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 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 the PLPB Repository in terms of privacy and security risk management:

<table>
<thead>
<tr>
<th>Position/Group</th>
<th>Roles/Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vice President, Programs</td>
<td>Responsible for the overall operations and strategic direction of the PLPB Repository</td>
</tr>
<tr>
<td>Director, Pharmaceuticals and Health Workforce Information Services</td>
<td>Responsible for strategic and operational decisions about the PLPB Repository</td>
</tr>
<tr>
<td>Manager, Physicians Information</td>
<td>Responsible for ongoing management and uptake of the PLPB Repository; makes day-to-day operational decisions about the PLPB Repository</td>
</tr>
<tr>
<td>Chief Information Security Officer</td>
<td>Responsible for the strategic direction and overall implementation of CIHI’s Information Security program</td>
</tr>
<tr>
<td>Chief Privacy Officer</td>
<td>Responsible for the strategic direction and overall implementation of CIHI’s Privacy program</td>
</tr>
<tr>
<td>Manager, ITS Health Information Applications</td>
<td>Responsible for ensuring that technical requirements for ongoing operations and enhancements for the PLPB Repository are met</td>
</tr>
</tbody>
</table>

3.3 Principle 2: Identifying Purposes for Personal Health Information

The PLPB Repository was established to

- Support patient-focused analysis—age–sex- and morbidity-adjusted health care use by different populations—that currently cannot be studied easily through other data sources, such as those related to primary care and community mental health;
- Support CIHI’s development of more comprehensive inpatient cost estimates that include the physician cost and other methodologies and tools to support health services analysis; and
- Enhance the quality of historical National Physician Database (NPDB) data and indicators (e.g., full-time equivalents, cost per service).

The PLPB Repository will collect personal health information, including patient identifiers in the form of the jurisdiction-assigned health card numbers, in order to facilitate linkage of person-level data across data holdings and time. Collection of patient identifiers, for example, enables CIHI to add (i.e., link) PLPB information to information that it already holds about a patient’s contact with the health care system (e.g., hospital stay data collected in the Discharge Abstract Database and National Ambulatory Care Reporting System).
3.4 Principle 3: Consent for the Collection, Use or Disclosure of Personal Health Information

Ministries of health will disclose PLPB data to CIHI for purposes of planning and managing the health system, including statistical analysis and reporting, under specific legislative authority or by legal agreements governing the flow of data. CIHI is a secondary collector of data and will not have direct contact with the physicians supplying PLPB data to ministries of health across Canada. CIHI relies on the 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.

3.5 Principle 4: Limiting Collection of Personal Health Information

CIHI is committed to the principle of data minimization. Per 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.

CIHI limits its collection of personal health information to that which is necessary to support authorized data quality and analytical activities. CIHI continues to develop the PLPB Repository in collaboration with ministries of health across Canada. The PLPB Repository at CIHI is in a developmental phase and, as such, identifying the information that will be collected from each province and territory will be done on a jurisdiction by jurisdiction basis and will evolve over time.

Examples of the types of information to be collected by the PLPB Repository are found in Table 1. Information collected from some data elements could present an increased risk of direct or indirect identification. (See the appendix for the collection rationale for these data elements.) Other data elements that are collected may be considered sensitive from a patient perspective, such as Service Date (the date on which a specific physician service was delivered), Fee Code (the code for a specific physician service that has been claimed) and Diagnostic Code (codes identifying the underlying morbidities of each patient).

<table>
<thead>
<tr>
<th>Data Elements Required for Submission</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patient</td>
</tr>
<tr>
<td>Health Card Number</td>
</tr>
<tr>
<td>Patient’s Postal Code</td>
</tr>
<tr>
<td>Date of Birth</td>
</tr>
<tr>
<td>Sex</td>
</tr>
<tr>
<td>Physician</td>
</tr>
<tr>
<td>Physician Identity Number</td>
</tr>
<tr>
<td>Specialty Code</td>
</tr>
<tr>
<td>Place of Specialty</td>
</tr>
</tbody>
</table>

(continued on next page)
As noted in Section 2.2, collection of PLPB data will not be based on CIHI-issued mandatory file submission specifications, which normally set out strict and prescribed file layout constraints and variable specifications for data submissions. As such, there is a risk that a PLPB data provider may inadvertently submit more data than is required. CIHI will mitigate this risk in several ways.

First, CIHI has identified the minimum list of data elements required (i.e., the MDS) and will negotiate with each potential data provider to ensure that only the data necessary for purposes of the PLPB Repository is submitted. Second, CIHI is currently developing a business case looking at the future of PLPB data, examining possible scenarios for its evolution in the future. It is expected that the business requirements of a technical solution (beyond the current PLPB Repository) will include automated file submission validation processes, which will greatly reduce or eliminate the risk of submission of data beyond what is requested and required for purposes of PLPB Repository. In the interim, until such time as a new technical solution is operational, CIHI staff will continue with the current procedure of manual review for unwanted data elements. This review takes place during secondary processing (see Section 2.2) of each PLPB data file, prior to transfer of the file to the SAS analytical environment. If data elements not requested by CIHI are included in a submission, they will be deleted from the file at the secondary processing stage, and the respective jurisdiction will be notified to adjust future submission specifications.

<table>
<thead>
<tr>
<th>Data Elements Required for Submission</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physician (cont'd)</td>
</tr>
<tr>
<td>Foreign-Certified Physician Indicator</td>
</tr>
<tr>
<td>Physician Age</td>
</tr>
<tr>
<td>Physician Gender</td>
</tr>
<tr>
<td>Graduation Year</td>
</tr>
<tr>
<td>Referring Physician Identity Number</td>
</tr>
<tr>
<td>Service Location</td>
</tr>
<tr>
<td>Facility Identifier</td>
</tr>
<tr>
<td>Postal Code/Area Code</td>
</tr>
<tr>
<td>Facility Type</td>
</tr>
<tr>
<td>Functional Centre</td>
</tr>
<tr>
<td>Service</td>
</tr>
<tr>
<td>Service Date</td>
</tr>
<tr>
<td>Diagnostic Code</td>
</tr>
<tr>
<td>Service Location Indicator</td>
</tr>
<tr>
<td>Remuneration Mode</td>
</tr>
<tr>
<td>Source of Payment/Program Type</td>
</tr>
<tr>
<td>Claim Number</td>
</tr>
<tr>
<td>Fee Code</td>
</tr>
<tr>
<td>Number of Services</td>
</tr>
<tr>
<td>Number of Units</td>
</tr>
<tr>
<td>Fee Paid</td>
</tr>
<tr>
<td>Fee Paid Date</td>
</tr>
</tbody>
</table>

Table 1: Detailed List of Proposed Data Elements Required for the Patient-Level Physician Billing Repository (cont’d)
3.6 Principle 5: Limiting Use, Disclosure and Retention of Personal Health Information

Limiting Use

CIHI will limit the use of PLPB data to authorized purposes, as described in Section 3.3. These include comparative analyses within and among jurisdictions; trend analyses to assess/monitor the impact of differences in policy, practices and service delivery; as well as statistics to support planning, management and quality improvement. CIHI staff will be 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.

Since 2009, data sets used for internal CIHI analysis purposes do not contain identifiers, such as unencrypted health card numbers. Health card numbers in an unencrypted form are available to CIHI staff on an exceptional, need-to-know basis only, subject to internal approval processes, as set out in CIHI’s Privacy Policy and Procedures, 2010.

Data Linkage

Data linkages are performed between the PLPB data and other CIHI data sources. While this potentially creates greater risk of identification of an individual, CIHI will undertake the following mitigating steps to reduce the risk.

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 encrypted health card 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 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
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.

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 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 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 both to data linkages for CIHI’s own purposes and to third-party data requests.

Return of Own Data

Section 34 of CIHI’s Privacy Policy, 2010 establishes that the return of data to the ministry of health that originally provided it to CIHI is not considered a disclosure; rather, it is considered a use. CIHI may return PLPB data via its web-based eServices or other approved CIHI method of dissemination.

Limiting Disclosure

Public Release of PLPB Data

As part of its mandate, CIHI releases aggregate data only, and in a manner designed to minimize any risk of identification and residual disclosure. Aggregate statistics and analyses are made available in publications and on CIHI’s website. This generally requires a minimum of 5 observations per cell.

Limiting Retention

The PLPB repository 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.

3.7 Principle 6: Accuracy of Personal Health Information

In compliance with CIHI’s Data Quality Framework Assessment Policy, once PLPB data collection has matured, the PLPB Repository will be subject to data quality assessment on a regular basis, based on CIHI’s Data Quality Framework. The process of completing the framework includes numerous activities to assess the various dimensions of quality, including the accuracy of the PLPB data.
3.8 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 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 PLPB data, which will eventually be developed, are highlighted below.

System Security

CIHI recognizes that information is secure only if it is secure throughout its entire lifecycle: creation and collection, access, retention and storage, use, disclosure and disposition. Accordingly, CIHI has a comprehensive suite of policies that specifies 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 card number has been removed or encrypted. In exceptional instances, staff will require access to original health card numbers. Section 10 of CIHI’s 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 personal health information as follows:

- Access to health card 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 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.

3.9 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. Specifically, CIHI’s Privacy and Security Framework, 2010 and Privacy Policy, 2010 are available to the public on its corporate 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, who may direct an inquiry or complaint to the privacy commissioner of the jurisdiction of the person making the inquiry or complaint.

4 Privacy Assessment Summary and Conclusion

There are no recommendations at this time and privacy risks identified during this assessment have been mitigated. This PIA will be updated or renewed in compliance with CIHI’s Privacy Impact Assessment Policy.
Appendix

The following table describes the jurisdiction-specific data elements that could present an increased risk of direct or indirect identification of an individual, including the jurisdiction-specific data element definitions and a rationale for its collection.

<table>
<thead>
<tr>
<th>Alberta</th>
<th>Alberta Data Element(s) and Definition(s)</th>
<th>Reason for Collection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health Card Number</td>
<td>Patient’s Identifier: Patient health card number</td>
<td>Used to link to data in other CIHI databases to provide a comprehensive picture of each patient’s clinical profile</td>
</tr>
<tr>
<td>Patient's Postal Code</td>
<td>Patient’s Postal Code: Patient full postal code of residence</td>
<td>Used for geographical analysis, for example, of service location compared with patient location of residence, and to append spatial measures from census or other sources to PLPB information</td>
</tr>
<tr>
<td>Date of Birth</td>
<td>Patient’s Date of Birth: Date of birth for patient</td>
<td>Used for calculation of age of patient between the date of service and the date of birth. The age itself will be used for patient age breakdown analysis.</td>
</tr>
<tr>
<td>Sex</td>
<td>Patient Gender: Sex of patient</td>
<td>Used when looking at gender breakdown in any analysis</td>
</tr>
<tr>
<td>Service Location Indicator</td>
<td>Service Event Location Postal Code: Full postal code populated only if service event location is the patient’s home</td>
<td>Used for geographical analysis of service location compared with patient location of residence</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Saskatchewan</th>
<th>Saskatchewan Data Element(s) and Definition(s)</th>
<th>Reason for Collection/Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health Card Number</td>
<td>Patient’s Identifier: Patient health card number</td>
<td>Used to link to data in other CIHI databases to provide a comprehensive picture of each patient’s clinical profile</td>
</tr>
<tr>
<td>Patient’s Postal Code</td>
<td>Patient Location: Beneficiary Residence Code at date of claim processing</td>
<td>Used for geographical analysis, for example, of service location compared with patient location of residence, and to append spatial measures from census or other sources to PLPB information</td>
</tr>
<tr>
<td>Sex</td>
<td>Patient Sex: Patient sex</td>
<td>Used when looking at gender breakdown in any analysis</td>
</tr>
</tbody>
</table>
References

