Insured Persons Repository

Privacy Impact Assessment

April 2022

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.

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

How to cite this document:
Canadian Institute for Health Information. *Insured Persons Repository Privacy Impact Assessment, April 2022*. Ottawa, ON: CIHI; 2022.

Cette publication est aussi disponible en français sous le titre *Évaluation des incidences sur la vie privée du répertoire des personnes assurées, avril 2022*.

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

- *Insured Persons Repository Privacy Impact Assessment, April 2022*

Approved by

Brent Diverty
Vice President, Data Strategies and Statistics

Rhonda Wing
Executive Director, Chief Privacy Officer and General Counsel, Office of the Chief Privacy Officer and Legal Services

Ottawa, April 2022

Table of contents

Quick facts about the Insured Persons Repository

1. The Insured Persons Repository (IPR) was established to
   - Support the development and evolution of the population grouping methodology (POP Grouper) by the Canadian Institute for Health Information (CIHI). The POP Grouper is a methodology for a population risk-adjustment grouping, a composite measure of the burden of illness or future use of health services by populations, both health system users and non-users. A privacy impact assessment (PIA) specific to the POP Grouper and the various data sources it relies on, including IPR data, is available separately at cihi.ca.
   - 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.
2. The IPR collects personal health information on all clients and their eligibility for insured health care, regardless of whether they have accessed the health care system.
3. In 2013, 3 provinces provided CIHI with an ad hoc extract of their insured persons data for specific use in the initial development of CIHI's POP Grouper.
4. As of 2021, Nova Scotia, Ontario and Saskatchewan supply data to CIHI's IPR. Alberta has also supplied data to the IPR, but use is currently limited to enhancement of CIHI's POP Grouper. CIHI continues to work with other jurisdictions to obtain national coverage.

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 Insured Persons Repository (IPR). This PIA includes a review of the 10 privacy principles set out in the Canadian Standards Association's *Model Code for the Protection of Personal Information* and how the principles apply to the IPR, as well as a look at the application of CIHI's *Privacy and Security Risk Management Framework*.

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

2 Background

2.1 Introduction to the Insured Persons Repository

In 2013, CIHI was in the early-stage development of the population grouping methodology (POP Grouper). The POP Grouper project was established to develop a methodology and grouping software for population grouping, developed using CIHI data and expertise. The methodology is clinically driven and groups the entire population. Its foundation is a set of groups, or cells, that describe a person's clinical conditions and the severity of those conditions. The clinical groups and related predictive models make use of patient-level data from multiple data sources.

One data source that did not exist at CIHI in 2013, and was crucial in the development of the methodology, was the IPR. The unique aspect of the IPR data is that it covers the complete insured population, regardless of whether an individual accessed the health care system. Ensuring the entire population is covered, including those who did not access the health care system, is important when constructing a predictive model due to the fact that all the individuals are potential users.

3 provinces (Ontario, Alberta and British Columbia) provided CIHI with an ad hoc extract of their IPR data for use in the initial development of CIHI's POP Grouper. To support the inclusion of additional provinces and the evolution of the methodology, CIHI began to work with provinces to establish routine collection of IPR data. As of 2022, Nova Scotia, Ontario and Saskatchewan supply IPR data to CIHI on an ongoing basis. CIHI's use of Alberta data supplied to the IPR is currently limited to enhancement of CIHI's POP Grouper.

2.2 Data collection

Provincial and territorial ministries of health maintain a list of health care numbers, including the characteristics of the individuals associated with those numbers and their eligibility for jurisdiction-specific health insurance coverage. The data generated for this primary purpose is subsequently submitted to CIHI. Each record submitted to the IPR reflects the jurisdiction-specific data set that conforms, to the degree possible, with the minimum data set requested by CIHI and includes

- Health care number
- Patient postal code
- Patient date of birth
- Patient sex

2.3 Access management, data submission and flow for the IPR

Each data provider (i.e., jurisdictional ministries of health) extracts a jurisdiction-specific data set from its existing data sources that conforms, to the degree possible, with the minimum data set requested by CIHI.

Access to CIHI's secure applications is subject to CIHI's role-based access management process, which is managed by CIHI's Product Management and Client Experience (PMCE) department. PMCE manages access to CIHI's secure applications using established access management system (AMS) processes for granting and revoking access.

Once authenticated through CIHI's AMS, IPR data providers submit to CIHI record-level data through CIHI's secure web-based electronic Data Submission Services (eDSS) or other direct server-to-server option.

Once received by CIHI, IPR data files immediately undergo automated checks for file inconsistencies against jurisdiction-specific specifications, and the jurisdiction-issued health care number in each file is encrypted. Once the health care numbers have been encrypted, each jurisdiction-specific IPR 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. This secondary processing may include correcting errors in consultation with data providers (as an alternative to resubmitting files) and deleting data elements not required for routine analytical use within CIHI's SAS analytical environment.

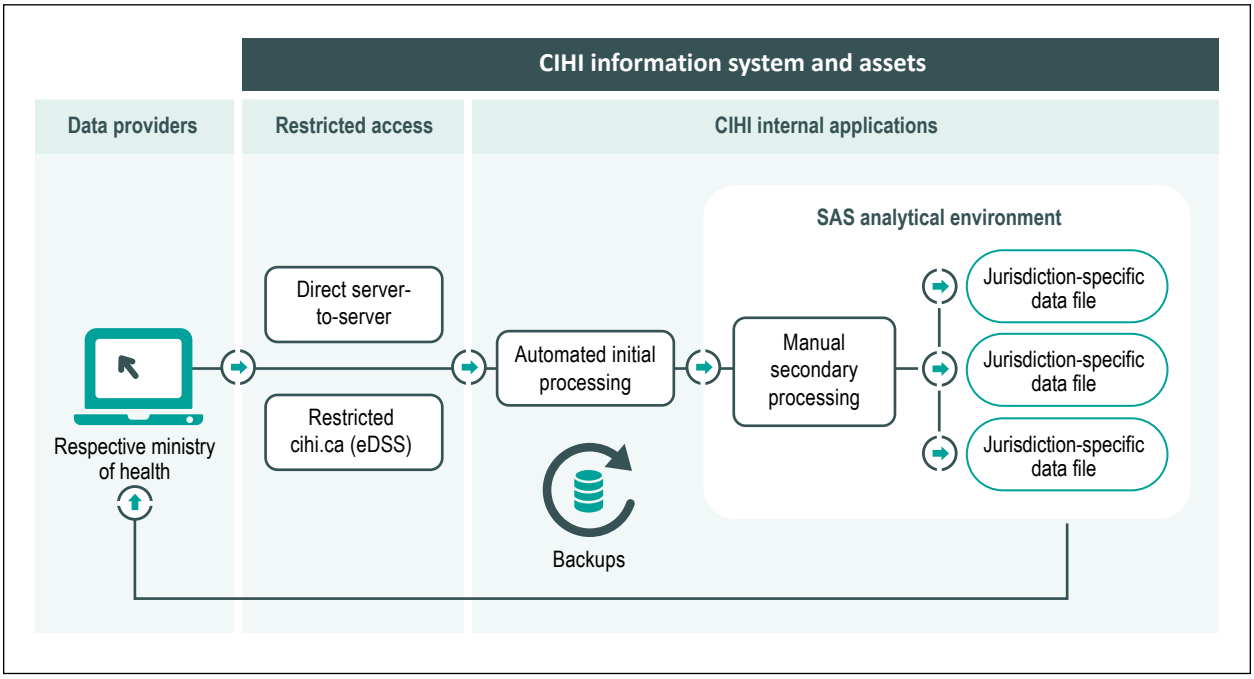
Once data has been successfully submitted, processed and stored within the IPR, a copy of the IPR data set is then uploaded to CIHI's SAS analytical environment where it is made available to approved CIHI staff for CIHI purposes. Staff are able to access IPR data through CIHI's SAS analytical environment, which is managed through a centralized SAS data access process in alignment with CIHI's policies for data access.

CIHI returns IPR data to the data provider that originally supplied the data, in this case the respective ministry of health.

Copies of CIHI data and applications are retained on backup systems.

All the IPR data flows are highlighted in the figure.

Figure Overview of the data flows for the Insured Persons Repository



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; or
- **Low:** Low probability of risk occurring, and/or reliable, effective controls and strategies exist.

The likelihood and impact of the identified risk are used to create a risk score. The risk assessment score of low, medium or high defines the seriousness of a risk. A higher risk ranking indicates a more serious threat and a greater imperative for treatment. Once an initial risk treatment is applied, the residual risk (the new calculation of the likelihood and impact of the risk, given the treatment) is assessed and compared against CIHI's privacy and security risk tolerance statement, which indicates that CIHI's privacy and security risk tolerance is low. If the risk score for the residual risk is still greater than low, additional risk treatment is necessary until the risk is low or the untreated/residual risk is accepted by CIHI's Executive Committee on behalf of the corporation.

There were no privacy and security risks identified as a result of this PIA.

3.2 Authorities governing Insured Persons Repository data

General

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

Privacy legislation

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

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

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

Agreements

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

3.3 Principle 1: Accountability for personal health information

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

Organization and governance

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

Table Key positions and responsibilities

Position/group	Roles/responsibilities
Vice president, Data Strategies and Statistics	Responsible for the overall operations and strategic direction of the IPR
Director, Pharmaceuticals and Health Workforce Information Services	Responsible for strategic and operational decisions about the IPR
Manager, Physician Information	Responsible for ongoing management and uptake of the IPR; makes day-to-day operational decisions about the IPR
Chief information security officer	Responsible for the strategic direction and overall implementation of CIHI's Information Security Program
Executive director, chief privacy officer and general counsel	Responsible for the strategic direction and overall implementation of CIHI's Privacy Program
Manager, Infrastructure Business Operations	Responsible for ensuring that technical requirements for web-based submission and initial processing are met, including encryption of original jurisdiction-issued health care numbers prior to transfer of IPR data files into CIHI's SAS analytical environment

3.4 Principle 2: Identifying purposes for personal health information

CIHI's mandate is to deliver comparable and actionable information to accelerate improvements in health care, health care system performance and population health across the continuum of care. This includes the following:

- Support the development and evolution of CIHI's population grouping methodology (POP Grouper); and
- 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.

In order to fulfill these goals, CIHI collects the following types of IPR data for the purposes indicated.

Personal identifiers/demographic information

Examples include health care number, date of birth, postal code and sex. CIHI uses this information to develop a complete picture of the care provided to the individual by linking together records describing the different types of care provided to the individual, at different times, by different facilities. In order to link together the individual's records, CIHI needs to know which records pertain to the individual. Accordingly, all records must include some identifying information — especially the individual's health care number. CIHI uses age calculated using date of birth, geographic information derived from postal code, and sex for demographic analysis of health care services and outcomes.

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

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

3.6 Principle 4: Limiting collection of personal health information

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

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 IPR in collaboration with ministries of health across Canada. Identifying the information that will be collected from each province and territory will continue to be done on a jurisdiction-by-jurisdiction basis and will evolve over time.

As noted in Section 2.3, collection of IPR data is not 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 an IPR 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 this is used to negotiate with each potential data provider to ensure that only the data necessary for purposes of the IPR is submitted.

Second, CIHI has a corporate de-identification process for encrypting health care numbers. During this process, if the structure of the file submitted to CIHI has changed in any way from what is expected (i.e., inclusion of additional information), then the corporate de-identification process will fail. Following this, Infrastructure Business Operations will notify the program area that something is wrong with the file and the program area will follow up with the provider to verify what was transmitted.

Third, CIHI staff have implemented additional procedures for manual review for unwanted data elements. This review takes place during secondary processing (see Section 2.3) of each IPR data file, prior to transferring 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. Data elements required for purposes of the IPR but not necessary for routine analytical activities in CIHI's SAS analytical environment are accessible only on an exceptional basis, subject to approval in compliance with CIHI's internal *Privacy Policy and Procedures, 2010*.

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

Limiting use

Clients

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

CIHI staff

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.

Staff access to the SAS analytical environment is provided through CIHI's centralized SAS data access process managed through CIHI's Service Desk. This environment is a separate, secure space for the storage of analytical data files, where staff can conduct and store the outputs from their analytical work.

The process ensures that all requests for access, including access to IPR data, are traceable and authorized, in compliance with Section 10 of CIHI's *Privacy Policy, 2010*. The SAS data access process is subject to an annual audit to ensure that staff are accessing data on a need-to-know basis. Section 3.9 includes additional information about how the various procedural and technical measures are deployed to prevent unauthorized access to and otherwise secure the IPR data.

Data linkage

Data linkages are performed between the IPR data and other CIHI data sources. While this potentially causes greater risk of identification of an individual, CIHI undertakes mitigating steps to reduce the risks.

Sections 14 to 31 of CIHI's *Privacy Policy, 2010* govern linkage of records of personal health information. Pursuant to this policy, CIHI permits the linkage of personal health information under certain circumstances. Data linkage within a single data holding for CIHI's own purposes is generally permitted. Data linkage across data holdings for CIHI's own purposes and all third-party requests for data linkage are subject to an internal review and approval process.

When carrying out data linkages, CIHI will generally do so using consistently encrypted health care numbers. The linked data remains subject to the use and disclosure provisions in the *Privacy Policy, 2010*.

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

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

Section 24 All of the following criteria are met:

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

Client linkage standard

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

Destruction of linked data

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

Section 29 of CIHI's *Privacy Policy, 2010* further requires that for time-limited specific projects, the secure destruction of linked data will occur within 1 year after publication of the resulting analysis, or 3 years after the linkage, whichever is sooner, in a manner consistent with CIHI's *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 *Destruction Standard*. These requirements apply to data linkages both for CIHI's own purposes and for third-party data requests.

Return of own data

Upon request, CIHI will provide an organization with a copy of any data the organization submitted to the IPR as a return of own data. In addition to returning data to submitting organizations, Section 34 of CIHI's *Privacy Policy, 2010* establishes that CIHI may return records to the relevant ministry for data quality purposes and for purposes consistent with its mandate (e.g., for health services and population health management, including planning, evaluation and resource allocation). The return of own data is considered a use and not a disclosure.

Limiting disclosure

Third-party data requests

IPR data is not accessible through CIHI's third-party data request program.

Public release

CIHI does not publicly release aggregate data from the IPR.

Limiting retention

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

3.8 Principle 6: Accuracy of personal health information

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

Similar to other CIHI data holdings, the IPR 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 IPR 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 IPR data are highlighted below.

System security

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

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

- Access to health care numbers and patient names (rarely collected) within CIHI's operational production databases;
- Access to data files containing personal health information extracted from CIHI's operational production databases and made available to the internal analytical community on an exceptional basis; and
- Changes to permissions in access to operational production databases.

CIHI's employees are made aware of the importance of maintaining the confidentiality of personal health information and other sensitive information through the mandatory Privacy and Security Training Program and through ongoing communications about CIHI's privacy and security policies and procedures. Employees attempting to access a CIHI information system must confirm, prior to each logon attempt, their understanding that they may not access or use the computer system without CIHI's express prior authority or in excess of that authority.

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

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

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

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

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

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

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

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

4 Conclusion

CIHI's assessment of the IPR did not identify any privacy or security risks.

This PIA will be updated or renewed in compliance with CIHI's *Privacy Impact Assessment Policy*.

Appendix

Text alternative for image

Data collection by CIHI: Once authenticated through CIHI's access management system processes for granting and revoking access, IPR data providers submit record-level data to CIHI through CIHI's secure web-based electronic Data Submission Services or other direct server-to-server options.

Internal data processing following collection by CIHI: IPR data undergoes automated checks for file inconsistencies against jurisdiction-specific specifications, and the jurisdiction-issued health care number in each file is encrypted. Authorized internal staff perform additional processing before the files are transferred to CIHI's SAS analytical environment.

Backups: Copies of IPR data are retained on backup systems.

CIHI return, disclosure and use of data: CIHI staff access data within the SAS analytical environment on a need-to-know basis, to return data to the original data provider. IPR data is not accessible through CIHI's third-party data request process, and CIHI does not publicly release aggregate IPR data.

help@cihi.ca

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

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

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

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

cihi.ca

13861-0522