National Prescription Drug Utilization Information System

Privacy Impact Assessment

April 2024

Canadian Institute for Health Information
Institut canadien d'information sur la santé

Production of this document is made possible by financial contributions from Health Canada and provincial and territorial governments. The views expressed herein do not necessarily represent the views of Health Canada or any provincial or territorial government.

Unless otherwise indicated, this product uses data provided by Canada's provinces and territories.

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

How to cite this document:
Canadian Institute for Health Information. *National Prescription Drug Utilization Information System Privacy Impact Assessment, April 2024*. Ottawa, ON: CIHI; 2024.

Cette publication est aussi disponible en français sous le titre *Système national d'information sur l'utilisation des médicaments prescrits : évaluation des incidences sur la vie privée, avril 2024*.

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

- *National Prescription Drug Utilization Information System Privacy Impact Assessment, April 2024*

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 2024

Table of contents

Quick facts about the National Prescription Drug Utilization Information System

1. The National Prescription Drug Utilization Information System (NPDUIS) is a pan-Canadian database at the Canadian Institute for Health Information (CIHI) that primarily contains data regarding claims submitted to public drug programs for payment or that were processed for documentation under a drug information system.
2. CIHI is working toward expanding NPDUIS to include data on all drugs dispensed from community pharmacies (including privately funded drug claims), drugs dispensed in hospitals and drugs dispensed through cancer agencies from all jurisdictions.
3. NPDUIS was developed in the early 2000s by CIHI in consultation with the Patented Medicine Prices Review Board (PMPRB). It is designed to meet the needs of the federal, provincial and territorial public drug programs, which are its data providers. NPDUIS has expanded with changing jurisdictional information needs. For example, in 2019, NPDUIS collection expanded to include Ontario's Narcotics Monitoring System claims-level data.
4. NPDUIS contains information about the drug prescribed; the patient to whom the drug was prescribed; the prescriber of the drug; the provider of the drug; the applicable drug program; and drug costs. Some supporting information is also collected, such as which drugs are covered by public drug programs.
5. Data captured by NPDUIS is used to develop comparable and actionable information to support decision-making about public drug programs; to compare drug spending and use over time; to measure the impact of drug policy changes on drug trends; to identify changes in prescribing; and to support monitoring and surveillance work associated with problematic prescription drug use. NPDUIS collects only the information necessary for these purposes.
6. The information developed using NPDUIS data is available in several ways. NPDUIS eReports provide participating ministries of health, PMPRB and Canada's Drug Agency with access to aggregate and de-identified (record-level) NPDUIS data. Third-party organizations may request aggregate de-identified data, subject to the terms set out in CIHI's *Privacy Policy, 2010*. Finally, CIHI releases certain aggregate data to the public, available on cihi.ca.

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 National Prescription Drug Utilization Information System (NPDUIS). This PIA, which replaces the January 2018 version, includes both a review of the 10 privacy principles set out in the Canadian Standards Association's *Model Code for the Protection of Personal Information* and how the principles apply to NPDUIS, 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*.

All policies referenced in this PIA are available on cihi.ca.

2 Background

2.1 Introduction to NPDUIS

NPDUIS was developed in the early 2000s by CIHI in consultation with the Patented Medicine Prices Review Board (PMPRB). It is designed to meet the needs of the federal, provincial and territorial public drug programs, which are its data providers. NPDUIS contains pan-Canadian prescription drug claims–level data, focusing primarily on data regarding claims submitted to public drug programs for payment or that were processed for documentation under a drug information system.

NPDUIS has expanded with changing jurisdictional information needs. For example, in 2019, NPDUIS collection expanded to include Ontario's Narcotics Monitoring System claims-level data. Also, NPDUIS now contains data on all drugs dispensed from community pharmacies in Manitoba, Saskatchewan and British Columbia, including those paid by public programs, private insurance or individuals paying out of pocket.

2.2 Data collection

NPDUIS primarily contains records regarding claims that were submitted to public drug programs for payment or that were processed for documentation under a drug information system. NPDUIS collects drug claims–level records from federal, provincial and territorial ministries of health. Some ministries of health provide CIHI with records regarding publicly funded drug claims only. Other ministries of health provide CIHI with records regarding all drugs dispensed from community pharmacies, including both publicly and privately funded drug claims. Where there are gaps in the drug data CIHI collects, CIHI works to fill them.

Each record submitted to NPDUIS reflects the minimum data set and includes information about

- The drug prescribed (e.g., drug identification number);
- The patient to whom the drug was prescribed (e.g., health care number, postal code, patient sex, date of birth);
- The prescriber of the drug (e.g., prescriber identifier, postal code);
- The provider of the drug (e.g., pharmacy identifier, postal code);
- The applicable drug program (e.g., the drug program that paid for the drug); and
- The drug costs (e.g., ingredient cost, professional fees, costs paid by the drug program, cost sharing).

NPDUIS does not collect information about

- Drugs that were prescribed but never dispensed to the patient;
- Drugs that were dispensed but for which the drug costs were not submitted to a drug program and were not processed for documentation under a drug information system; or
- Patients' diagnoses or the conditions for which drugs were dispensed.

In addition to drug claim records, NPDUIS also collects supporting information to provide context for the drug claim records, such as

- Information collected from ministries of health about which drugs are covered under public drug programs (formulary information); and
- Drug product information collected from Health Canada.

Additional information about the information collected in the NPDUIS can be found on CIHI's NPDUIS metadata web page.

2.3 Access management and flow for NPDUIS

Access to CIHI's secure applications is managed by CIHI's Client Access and Engagement (CAE) department. CAE manages access to CIHI's secure applications using established access management system (AMS) processes for granting and revoking access.

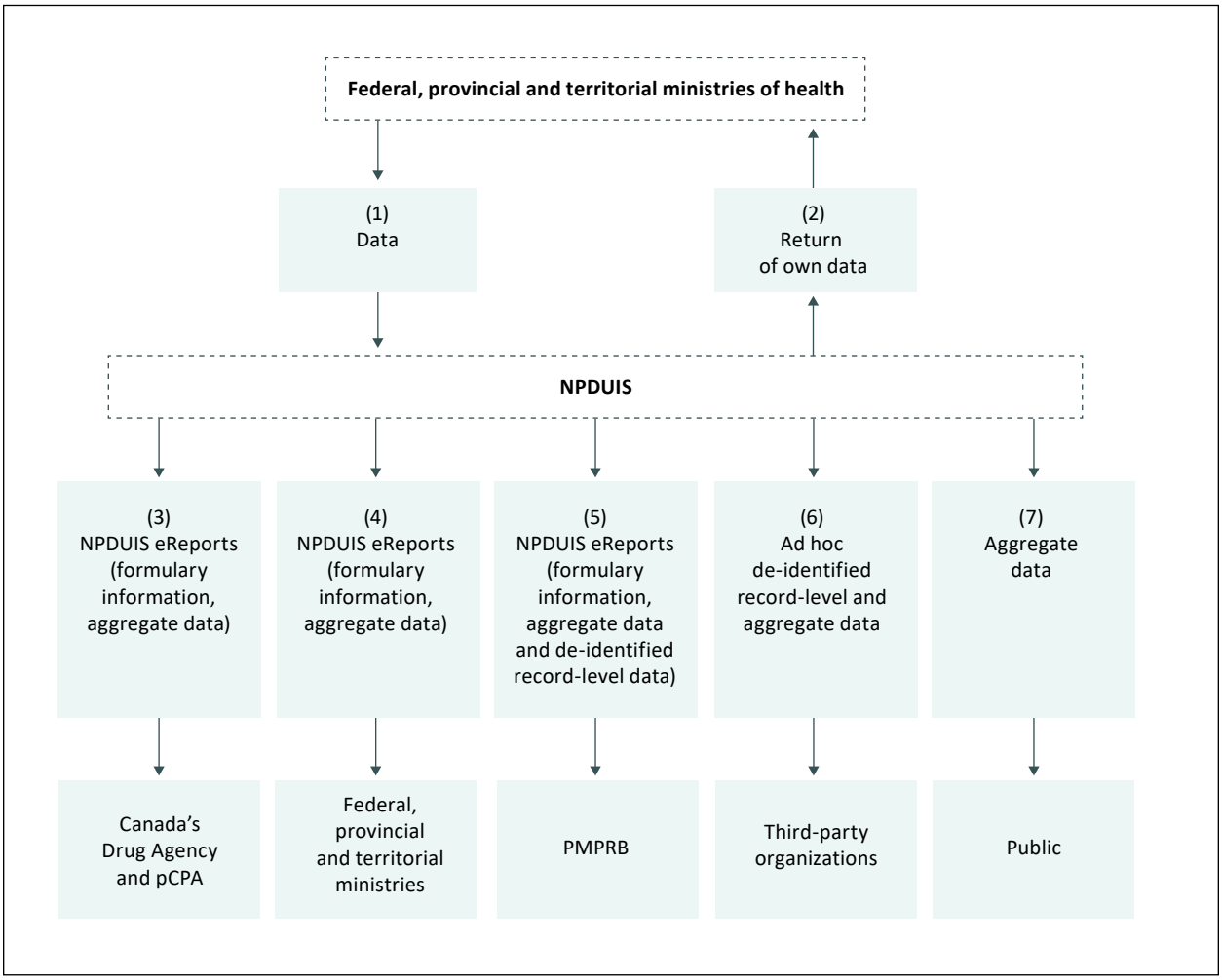
Once authenticated through CIHI's AMS, NPDUIS data providers submit record-level data from facilities that is electronically captured using specialized software, through CIHI's secure web-based electronic Data Submission Services (eDSS) or server-to-server application (Secure File Transfer Protocol).

The NPDUIS data flow of drug claim records is as follows:

1. Federal, provincial and territorial ministries of health submit data to NPDUIS. Specifically, ministries of health submit records regarding claims that were submitted to public drug programs for payment or that were processed for documentation under a drug information system.
2. A copy of the records as accepted by NPDUIS, as well as certain reports that include personal health information, are available to the respective ministry of health that submitted the data to CIHI.
3. Via NPDUIS eReports, CIHI provides access to formulary information and aggregate data to Canada's Drug Agency and the pan-Canadian Pharmaceutical Alliance (pCPA).
4. Via NPDUIS eReports, CIHI provides access to formulary information and aggregate data to ministries of health that submit data to NPDUIS.
5. Via NPDUIS eReports, CIHI provides access to formulary information and de-identified record-level and aggregate data to the Patented Medicine Prices Review Board (PMPRB).
6. NPDUIS discloses de-identified record-level and aggregate data to third-party organizations, in accordance with CIHI's *Privacy Policy*.
7. NPDUIS releases aggregate data to the public.

The following figure illustrates the NPDUIS data flow.

Figure NPDUIS data flow



3 Privacy analysis

3.1 Privacy and Security Risk Management Program

Privacy and security risk management is a formal, repeatable process for identifying, assessing, treating and monitoring risks in order to minimize the probability of such risks materializing and/or their impact should they occur. CIHI has implemented its *Privacy and Security Risk Management Framework* and the associated *Policy on Privacy and Security Risk Management*. CIHI's chief privacy officer and general counsel, and chief information security officer, in collaboration with senior managers, are responsible for identifying, assessing, treating, monitoring and reviewing privacy and security risks that impact the privacy principles described in sections 3.3 to 3.12.

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 assessment score indicates a more serious threat and a greater imperative for treatment. Once an initial risk treatment has been 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 assessment 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.

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

3.2 Authorities governing NPDUIS 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 Canada's 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, the 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, NPDUIS 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, 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, and a Governance and Privacy Committee of its Board of Directors.

Organization and governance

The following table identifies key internal senior positions with responsibilities for NPDUIS 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 strategic direction of NPDUIS.
Director, Pharmaceuticals	Responsible for the overall operations and strategic business decisions of NPDUIS.
Chief information security officer	Responsible for the strategic direction and overall implementation of CIHI's Information Security Program.
Chief privacy officer and general counsel	Responsible for the strategic direction and overall implementation of CIHI's Privacy Program.

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 system performance and population health across the continuum of care. This includes producing information to

- Support decision-making about drug programs;
- Compare drug spending and use over time;
- Measure the impact of drug policy changes on drug trends;
- Identify changes in prescribing; and
- Support monitoring and surveillance work associated with problematic prescription drug use.

To fulfill these goals, CIHI collects the following types of NPDUIS data for the purposes indicated.

Patient personal identifiers

Examples include health care number or jurisdiction encrypted health care number. CIHI uses this information to develop a complete picture of the care provided to an individual by linking records describing the different types of care provided to the individual at different times by different facilities. In order to perform these linkages, CIHI needs to know which records pertain to the individual. Accordingly, all records must include identifying information.

Patient demographic information

Examples include birthdate, postal code, sex and Indigenous identifiers. CIHI uses age calculated using date of birth, geographic information derived from postal code, sex and Indigenous identifiers for demographic analysis of healthcare services and outcomes.

Health facility identifiers

Examples include the number assigned to the pharmacy that provided the drug and the postal code of the pharmacy. CIHI uses this information to compare facilities and groups of facilities.

Health service provider identifiers

An example is the number assigned to the prescriber of the drug and the postal code of the prescriber's physical address of practice. CIHI uses this information to determine the types of human resources involved in the individual's care.

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

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

3.6 Principle 4: Limiting collection of personal health information

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

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

Limiting use

Clients

CIHI limits the use of NPDUIS 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 policies, 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 CIHI's secure analytical environment is provided through CIHI's centralized data access process. This environment is a separate, secure space for analytical data files, where staff are required to conduct and store the outputs from their analytical work.

NPDUIS data sets used for internal CIHI analysis do not contain direct identifiers such as unencrypted health care numbers, birthdates and full postal codes. Instead, NPDUIS data sets used for internal CIHI analysis contain age, encrypted health care number and province/territory. Information containing direct identifiers is available to CIHI staff on an exceptional, need-to-know basis only, subject to approval processes as set out in CIHI's internal Privacy Policy and Procedures, 2010.

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

Data linkage

Data linkages are performed between NPDUIS data and other CIHI data sources. While this potentially causes greater risk of identifying 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 approving 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

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

Destruction of linked data

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

Section 29 of CIHI's *Privacy Policy, 2010* further requires that for time-limited specific projects, the secure destruction of linked data will occur within 1 year after publication of the resulting analysis or 3 years after the linkage, whichever is sooner, in a manner consistent with CIHI's Secure Destruction Standard. For linked data resulting from an ongoing program of work, secure destruction will occur when the linked data is no longer required to meet the identified purposes, in a manner consistent with CIHI's Secure Destruction Standard. These requirements apply to data linkages both for CIHI's own purposes and for third-party data requests.

Return of own data

While ministries of health typically do not request the return of records they submit to NPDUIS, Section 34 of CIHI's *Privacy Policy, 2010* establishes that CIHI may return records to the data provider (i.e., the ministry of health) or as directed in the data-sharing agreement or other legal instrument. The return of own data is considered a use and not a disclosure.

Limiting disclosure

NPDUIS eReports

NPDUIS eReports is a secure web-based analytical reporting tool that, depending on the access level granted by CIHI, provides access to

- Formulary information (i.e., comparable contextual information associated with the administration policies of the federal, provincial and territorial public drug benefit plans and programs);
- Aggregated NPDUIS data; and/or
- Record-level de-identified NPDUIS data.

Users can produce reports about drug utilization, costs and coverage of drugs by drug plans. NPDUIS eReports permits users to select certain inputs and outputs in order to customize reports.

Before being provided with access to NPDUIS eReports, organizations must sign CIHI's Electronic Reporting Services Agreement that, among other things

- Restricts use of the data to non-commercial purposes limited to the client's internal management, data quality, planning, research, analysis or evidence-based decision-support activities;
- Prohibits disclosure of the data to any third party, except in the case of the client's own data;
- Permits publication only where all reasonable measures are employed to prevent the identification of individuals, and where the data does not contain cell sizes with fewer than 5 observations; and
- Prohibits the release of health facility/organization–identifiable information unless the client has notified CIHI prior to the disclosure, in order to permit CIHI to notify the applicable ministry of health.

Under the Electronic Reporting Services Agreement, each organization designates a contact from their organization who is responsible for authorizing designated users from their organization, who then are permitted to access NPDUIS eReports in accordance with the services agreement.

NPDUIS eReports is available as one of CIHI's restricted services and applications. In order to access CIHI's restricted services and applications, at the initiation of each use, each user must agree to CIHI's Client Services System and Applications Terms and Conditions of Access and Use. Users must agree to general terms (e.g., username and password security),

as well as to terms specific to the use of CIHI's electronic reporting applications, including NPDUIS eReports (e.g., you will access and use the service[s] in a manner consistent with the provisions of the Services Agreement).

Participating data provider access

CIHI provides participating federal, provincial and territorial ministries of health with access to formulary information and aggregate NPDUIS data through NPDUIS eReports.

CIHI's Client Services System and Applications Terms and Conditions of Access and Use and the Electronic Reporting Services Agreement, described above, govern each ministry of health's access to NPDUIS eReports.

Canada's Drug Agency and pCPA access

CIHI provides Canada's Drug Agency and pCPA with access to formulary information and aggregate NPDUIS data through NPDUIS eReports.

CIHI's Client Services System and Applications Terms and Conditions of Access and Use and the Electronic Reporting Services Agreement, described above, govern each organization's access to NPDUIS eReports.

PMPRB access

CIHI provides PMPRB with access to formulary information aggregate NPDUIS data, as well as to de-identified record-level NPDUIS data via NPDUIS eReports, in order to perform the complex analyses that PMPRB undertakes in its role set out by the federal minister of industry under the *Patent Act*.

CIHI's Client Services System and Applications Terms and Conditions of Access and Use govern PMPRB's access to NPDUIS eReports. An Electronic Reporting Services Agreement also governs PMPRB's access. This agreement includes the standard terms described above, as well as additional terms to protect the de-identified record-level data PMPRB accesses.

Third-party data requests

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

CIHI administers its Third-Party Data Request Program, which establishes privacy and security controls that must be met by the recipient organization. Furthermore, as set out in sections 37 to 57 of CIHI's *Privacy Policy, 2010*, CIHI discloses health information in a manner consistent with its mandate and core functions, and data disclosures are made at the highest degree of anonymity possible while still meeting the research and/or analytical purposes of

the requester. This means that, whenever possible, data is aggregated. When aggregated data is not sufficiently detailed for the intended purpose, record-level de-identified data or personal health information (in limited circumstances, for example, with individual consent) may be disclosed to the recipient on a case-by-case basis, when the recipient has entered into a data protection agreement or other legally binding instrument with CIHI. Only those data elements necessary to meet the intended purpose may be disclosed.

CIHI uses a secure access environment (SAE) as the preferred means of providing record-level data access available to third-party data requestors (the SAE is separate from CIHI's secure analytical environment that CIHI staff access, as described in Section 3.7). CIHI's SAE is an encrypted, secure environment hosted in CIHI's data centre. Consistent with CIHI's existing policies and procedures, approved researchers — who are subject to stringent agreement terms — access data extracts that have been prepared and vetted by CIHI staff for an approved research project. Record-level data cannot be copied or removed from the SAE; only aggregate results can be extracted from the SAE. Further information about CIHI's SAE is available on cihi.ca on the Make a data request web page and in the *SAE Privacy Impact Assessment*.

CIHI has adopted a complete life cycle approach to record-level data that it has extracted into files and sent to researchers and other approved users. As part of that life cycle, Privacy and Legal Services (PLS) has developed and is responsible for the ongoing compliance monitoring process whereby all data sets that are disclosed to third-party data recipients are tracked and monitored for secure destruction at the end of their life cycle. Prior to disclosing data, third-party recipients sign a data protection agreement and agree to comply with the conditions and restrictions imposed by CIHI relating to the collection, purpose, use, security, disclosure and return or disposal of data.

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

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

In addition to the ongoing compliance monitoring process, whereby all data sets that are disclosed to third-party data recipients are tracked and monitored for secure destruction at the end of their life cycle, PLS contacts third-party data recipients annually to certify that they continue to comply with their obligations as set out in the data request form and data protection agreement signed with CIHI.

As noted in Section 3.4, NPDUIS collects Indigenous identifiers. The disclosure of this information is governed by CIHI's Policy on the Release and Disclosure of Indigenous Identifiable Data, which requires that any request for Indigenous-identifiable data at CIHI be accompanied by approvals from appropriate Indigenous authorities. For more information, see *A Path Forward: Toward Respectful Governance of First Nations, Inuit and Métis Data Housed at CIHI*.

Public release

As part of its mandate, CIHI publicly releases aggregated data only in a manner designed to minimize any risk of re-identification and residual disclosure. This generally requires a minimum of 5 observations per cell in accordance with Section 33 of CIHI's *Privacy Policy, 2010*. Aggregated statistics and analyses are made available in publications and on cihi.ca through tools such as Your Health System (e.g., *Prescribed drug spending in Canada* report, *Drug use among seniors in Canada* report, Potentially Inappropriate Medication Prescribed to Seniors indicator).

Limiting retention

NPDUIS 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, NPDUIS is subject to an information 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 NPDUIS data.

3.9 Principle 7: Safeguards for personal health information

CIHI's Privacy and Security Framework

CIHI's *Privacy and Security Framework* provides 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 NPDUIS 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 risk-reduced record-level data, where the health care number has been 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 attempt to log in, 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 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 and general counsel, who may direct an inquiry or complaint to the Information and Privacy Commissioner of the jurisdiction of the person making the inquiry or complaint.

4 Review and update process

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

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 511
Montréal, Que.
H3A 2R7
514-842-2226

cihi.ca

51238-0724