



# National Prescription Drug Utilization Information System

## Privacy Impact Assessment

January 2018



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.

All rights reserved.

The contents of this publication may be reproduced unaltered, in whole or in part and by any means, solely for non-commercial purposes, provided that the Canadian Institute for Health Information is properly and fully acknowledged as the copyright owner. Any reproduction or use of this publication or its contents for any commercial purpose requires the prior written authorization of the Canadian Institute for Health Information. Reproduction or use that suggests endorsement by, or affiliation with, the Canadian Institute for Health Information is prohibited.

For permission or information, please contact CIHI:

Canadian Institute for Health Information

495 Richmond Road, Suite 600

Ottawa, Ontario K2A 4H6

Phone: 613-241-7860

Fax: 613-241-8120

[www.cihi.ca](http://www.cihi.ca)

[copyright@cihi.ca](mailto:copyright@cihi.ca)

© 2018 Canadian Institute for Health Information

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, janvier 2018*.



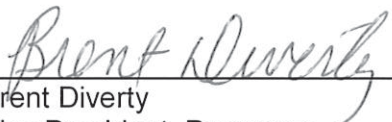
Canadian Institute  
for Health Information

Institut canadien  
d'information sur la santé

## National Prescription Drug Utilization Information System

### PRIVACY IMPACT ASSESSMENT

Approved by:

  
\_\_\_\_\_  
Brent Diverty  
Vice President, Programs

  
\_\_\_\_\_  
Anne-Mari Phillips  
Chief Privacy Officer & General Counsel

Ottawa – January 2018

# Table of contents

Quick Facts about CIHI and the National Prescription Drug Utilization Information System. . .	5
1 Introduction . . . . .	6
2 Background . . . . .	6
Information collected by NPDUIS . . . . .	7
Data providers . . . . .	7
How records are transferred . . . . .	7
Supporting information collected by NPDUIS . . . . .	9
3 Privacy analysis. . . . .	9
3.1 Privacy and Security Risk Management Program . . . . .	9
3.2 Authorities governing NPDUIS records . . . . .	10
General . . . . .	10
Legislation . . . . .	10
Agreements . . . . .	10
3.3 Principle 1: Accountability for personal health information. . . . .	11
Organization and governance . . . . .	11
3.4 Principle 2: Identifying purposes for personal health information. . . . .	12
3.5 Principle 3: Consent for the collection, use or disclosure of personal health information . . . . .	12
3.6 Principle 4: Limiting collection of personal health information . . . . .	13
3.7 Principle 5: Limiting use, disclosure and retention of personal health information . . . . .	13
Limiting use . . . . .	13
Data linkage . . . . .	14
Return of own data . . . . .	15
Limiting disclosure. . . . .	15
Limiting retention. . . . .	18
3.8 Principle 6: Accuracy of personal health information . . . . .	18
3.9 Principle 7: Safeguards for personal health information . . . . .	18
CIHI's Privacy and Security Framework . . . . .	18
System security. . . . .	18
3.10 Principle 8: Openness about the management of personal health information . . . . .	20
3.11 Principle 9: Individual access to, and amendment of, personal health information . . . . .	20
3.12 Principle 10: Complaints about CIHI's handling of personal health information . . . . .	20
4 Conclusion . . . . .	20
Appendix: Text alternative for figure. . . . .	21

# Quick Facts about CIHI and the National Prescription Drug Utilization Information System

The National Prescription Drug Utilization Information System (NPDUIS) is a pan-Canadian database at the Canadian Institute for Health Information (CIHI) that collects data regarding claims submitted to public drug programs for payment or that were processed for documentation under a drug information system. CIHI is working toward collecting data on all drugs dispensed from community pharmacies, including both publicly and privately funded drug claims, from all jurisdictions.

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 collects 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.

Data captured by NPDUIS is used to develop accurate, timely and comparable information, which in turn is used to make decisions 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.

The information developed using NPDUIS data is available in several ways. NPDUIS eReports provide participating ministries of health with access to aggregate NPDUIS data, and provide PMPRB with access to aggregate and de-identified (record-level) NPDUIS data. Third-party data requestors may request aggregate or de-identified data, subject to the rules set out in CIHI's [Privacy Policy, 2010](#). Finally, CIHI releases certain aggregate data to the public.

# 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 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 2011 version, includes a review of the 10 privacy principles set out in the Canadian Standards Association's *Model Code for the Protection of Personal Information*, as the principles apply to NPDUIS, and of 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

NPDUIS was developed in the early 2000s by CIHI in consultation with the Patented Medicine Prices Review Board (PMPRB). It was designed to meet the needs of federal, provincial and territorial public drug programs, the data providers for the database.

NPDUIS contains pan-Canadian prescription drug claims–level data. Focusing primarily on publicly financed drug benefit programs, NPDUIS collects a range of data in order to develop accurate, timely and comparable information used to

- Manage and make decisions 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.

## Information collected by NPDUIS

NPDUIS collects records regarding claims that were submitted to public drug programs for payment or that were processed for documentation under a drug information system. The records include information about the

- Drug prescribed (e.g., Drug Identification Number);
- Patient to whom the drug was prescribed (e.g., health care number, postal code, patient sex, date of birth);
- Prescriber of the drug (e.g., prescriber identifier, postal code);
- Provider of the drug (e.g., pharmacy identifier, postal code);
- Applicable drug program (e.g., the drug program that paid for the drug); and
- 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 the drug costs were not submitted to a drug program and were not processed for documentation under a drug information system; and
- Patients' diagnoses or the conditions for which drugs were dispensed.

A data dictionary containing detailed information about the records collected by NPDUIS is available at [cihi.ca](http://cihi.ca).

## Data providers

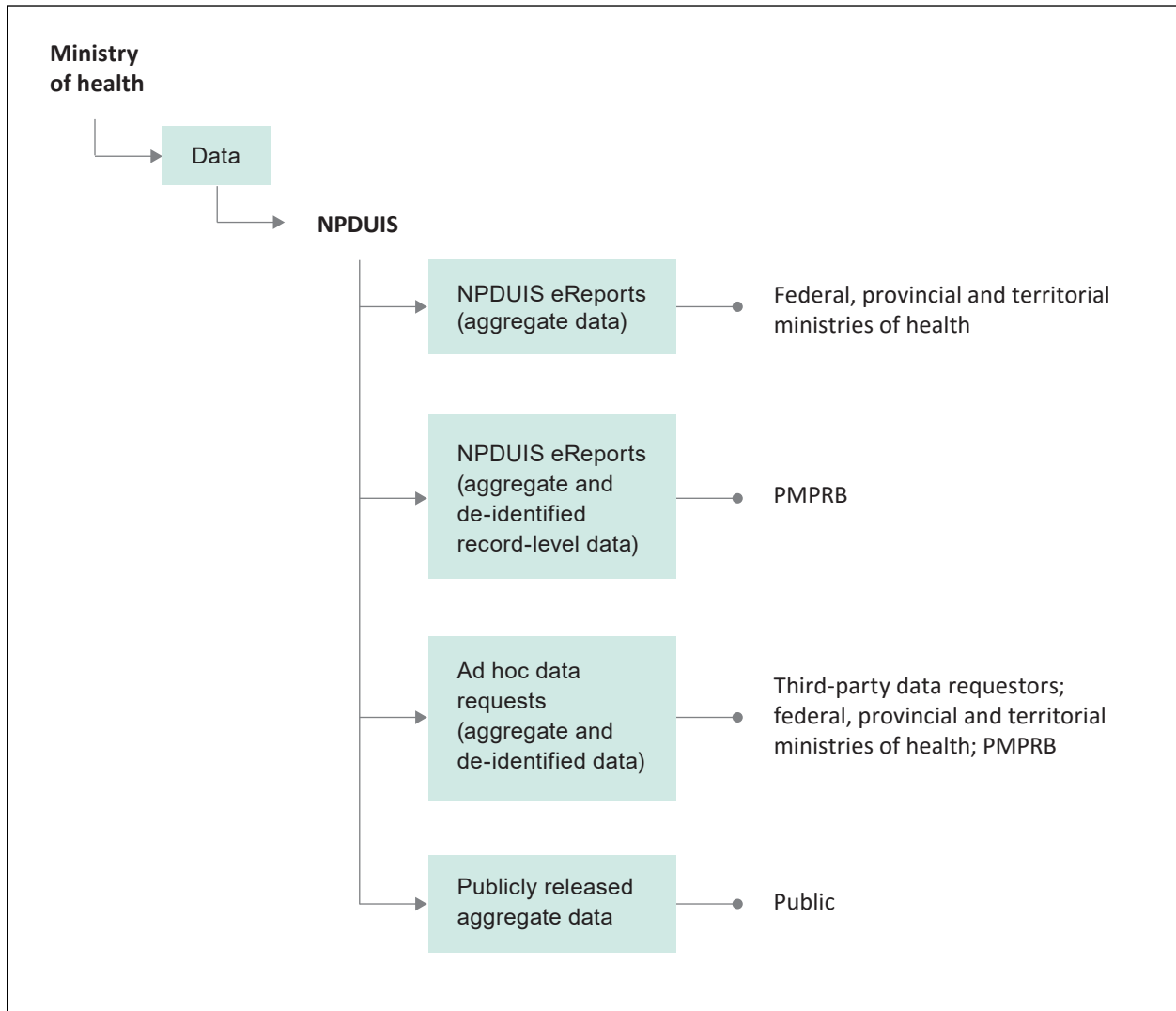
NPDUIS collects drug claims–level records from federal, provincial and territorial ministries of health. Some ministries provide CIHI with records regarding publicly funded drug claims only. Other ministries provide CIHI with records regarding all drugs dispensed from community pharmacies, including both publicly and privately funded drug claims. CIHI is working toward collecting both public and private data from all jurisdictions.

## How records are transferred

Ministries submit the records to CIHI via CIHI's web-based applications or server-to-server application.

The following figure illustrates NPDUIS data flows, which are discussed in greater detail throughout this PIA.

**Figure** NPDUIS data flows





# Supporting information collected by NPDUIS

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.

## 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, and monitoring and reviewing privacy and security risks.

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

- **High:** High probability of risk occurring and/or controls and strategies are not reliable or effective
- **Medium:** Medium probability of risk occurring and/or controls and strategies are somewhat reliable or effective
- **Low:** Low probability of risk occurring and/or reliable, effective controls and strategies exist

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

## 3.2 Authorities governing NPDUIS records

### 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 health systems, including statistical analysis and reporting. Data providers are responsible for meeting the statutory requirements in their respective jurisdictions, where applicable, at the time the data is collected.

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

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

### Agreements

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

### 3.3 Principle 1: Accountability for personal health information

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

#### Organization and governance

The following table identifies key positions with responsibilities for NPDUIS in terms of privacy and security risk management:

**Table** Key positions and responsibilities

<b>Position/group</b>	<b>Responsibilities</b>
<b>Vice president, Programs</b>	Strategic direction of NPDUIS
<b>Director, Pharmaceuticals and Health Workforce Information Services</b>	Strategic and operational development of NPDUIS
<b>Manager, Pharmaceuticals</b>	Development and operation of NPDUIS
<b>NPDUIS Database Advisory Group</b>	Provides advice on database enhancement, data quality, development of reports, and analytical topics and methods
<b>Chief information security officer</b>	Strategic direction and implementation of CIHI's Information Security Program
<b>Chief privacy officer</b>	Strategic direction and implementation of CIHI's Privacy Program
<b>Manager, ITS Health Information Applications</b>	Ensures availability of technical resources and solutions for ongoing operations and enhancements of NPDUIS
<b>Manager, Central Client Services</b>	Manages access to the web-based applications used to exchange NPDUIS data

## 3.4 Principle 2: Identifying purposes for personal health information

NPDUIS records pertain to individuals and indicate the drugs prescribed to them; NPDUIS records are therefore deemed to be personal health information.

NPDUIS records also identify members of the health workforce (e.g., physicians who prescribe drugs). CIHI's [Health Workforce Privacy Policy](#) establishes that whenever CIHI's activities involve personal health information, CIHI's [Privacy Policy, 2010](#) applies to the activities rather than CIHI's Health Workforce Policy. Because NPDUIS records are personal health information, the records are treated and protected as personal health information in accordance with CIHI's Privacy Policy, 2010.

NPDUIS collects personal health information because it is required for the purposes of the database, such as developing accurate, timely and comparable drug information, as described in Section 2.

The information developed using NPDUIS data is available in various forms to a range of stakeholders, as discussed in Section 3.7: Limiting disclosure.

## 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. 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 health care systems. NPDUIS collects only the data elements CIHI and its stakeholders (e.g., NPDUIS Database Advisory Group) determine to be necessary for the purposes of the database.

While NPDUIS records do not include the patient's name and address, they include other patient identifiers such as health care number, sex and date of birth. With respect to this information, each ministry of health determines whether it will submit

- Encrypted health care number or unencrypted health care number;
- Patient's year of birth or full date of birth; and
- Patient's postal code.

Ministries of health determine the information drug records contain to identify prescribers and providers of drugs, and submit an identifier and postal code for each respective prescriber and pharmacy, as described in Section 2.

CIHI treats all NPDUIS records as personal health information, regardless of which data elements the records contain.

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

### Limiting use

CIHI limits the use of NPDUIS records to authorized purposes, such as developing accurate, timely and comparable information as described in Section 2. 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.

Data sets used for internal CIHI analysis purposes do not contain direct identifiers, such as unencrypted health care numbers, birth dates and postal codes. They are removed from records before being moved to NPDUI's analytical environment (age is included, rather than birth date). Health care numbers in an unencrypted form are 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.

## Data linkage

To answer many questions about pharmaceutical use, data linkages are performed between NPDUI records and other CIHI data sources. While this potentially causes 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 consistently encrypted health card numbers. The linked data remain 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:

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.

## **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 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 to data linkages for both CIHI's own purposes and third-party data requests.

## **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, the province/territory that issued the health care number and year of birth. For the linkage of records that do not satisfy these criteria, the linkage mechanism is determined on a case-by-case basis.

## **Return of own data**

While ministries typically do not request the return of records they submit to the NPDUIS, such a return of own data is permitted under Section 34 of CIHI's [Privacy Policy, 2010](#).

## **Limiting disclosure**

### **NPDUIS eReports**

NPDUIS eReports is a secure, web-based, analytical reporting tool that provides access to aggregated information regarding drug claims. Users can produce reports about drug utilization, costs, and coverage of drugs by drug plans. NPDUIS eReports permit users to select certain inputs and outputs in order to customize reports.

CIHI provides participating ministries of health with access to aggregate NPDUIS data through NPDUIS eReports. CIHI provides the PMPRB with access to aggregate and de-identified (record-level) NPDUIS data through a separate eReporting environment.

Each time a user accesses NPDUIS eReports, the user must agree to a set of terms establishing rules for use of the data. In addition to the use of terms, a policy called NPDUIS Operating Principles governs ministries' access to the reports. The operating principles establish rules such as the following:

- With the exception of its own information, a ministry cannot publicly release information obtained from NPDUIS eReports.
- The ministry may not attempt to link information obtained from NPDUIS eReports to information from other sources.

### **PMPRB access**

PMPRB receives access to de-identified (record-level) data in order to perform the complex linkages and analyses that PMPRB undertakes in its role set out by the federal minister of industry under the *Patent Act*.

Like other users of NPDUIS eReports, PMPRB users must agree to a set of terms before using the service each time. PMPRB has also entered an agreement with CIHI that governs PMPRB's access to NPDUIS eReports and establishes rules such as these:

- PMPRB must not disclose information obtained from NPDUIS eReports to third parties, except when legally obligated to do so.
- PMPRB must take all reasonable steps, including suppressing cell sizes less than 5, to ensure that its publications do not contain information that could be used to identify an individual.

### **Risks and mitigation measures**

The 2011 NPDUIS PIA recommended that the terms discussed above be updated to reflect CIHI's current privacy and security practices. This work was completed.

The 2011 PIA also recommended that CIHI provide training materials to better educate users about their privacy and security responsibilities in using NPDUIS eReports. This recommendation is no longer relevant because CIHI will be replacing the specialized access management processes associated with NPDUIS eReports with CIHI's standardized access management processes. As part of this transition, the specialized documentation associated with NPDUIS eReports (including documentation regarding privacy and security responsibilities) will be replaced by CIHI's (existing) standardized documentation.



## Third-party data requests

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

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

CIHI has adopted a complete life cycle approach for record-level third-party data requests. As part of that life cycle, Privacy and Legal Services (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 receiving data, third-party recipients sign a data protection agreement and agree to comply with the conditions and restrictions imposed by CIHI relating to the collection, purpose, use, security, disclosure and return or disposal of data.

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

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

In addition to the compliance monitoring process, which leverages data captured to monitor compliance with data destruction requirements, PLS contacts third-party data recipients on an annual basis to certify that they continue to comply with their obligations as set out in the data request form and data protection agreement signed with CIHI.

## 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 a 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 NPDUIS records.

## 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 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 NPDUIS records 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 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 care number has been removed or encrypted upon first receipt. In the case of NPDUIS, direct identifiers such as unencrypted health care numbers, birth dates and postal codes are removed from analytical files. In exceptional instances, staff will require access to original health care numbers. CIHI's internal Privacy Policy and Procedures, 2010 sets out strict controls to ensure that access is approved at the appropriate level and in the appropriate circumstances, and that the principle of data minimization is adhered to at all times. CIHI logs access to data as follows:

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

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

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

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

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

CIHI makes information available about its privacy policies, data practices and programs relating to the management of personal health information. Specifically, CIHI's [Privacy and Security Framework](#) and [Privacy Policy, 2010](#) are available to the public on its corporate website ([cihi.ca](http://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](#), 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 NPDUIS did not identify any privacy risks.

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

# Appendix: Text alternative for figure

## **Figure: NPDUIS data flows**

This figure shows the flow of data in to and out of NPDUIS.

Regarding inflow of data, ministries of health submit data to NPDUIS. Specifically, ministries submit records regarding claims that were submitted to public drug programs for payment or that were processed for documentation under a drug information system.

Regarding outflow of data, this takes place in several ways:

1. NPDUIS makes reports containing aggregate data available to federal, provincial and territorial ministries of health.
2. NPDUIS makes reports containing both aggregate data and de-identified record-level data available to the Patented Medicine Prices Review Board.
3. NPDUIS discloses aggregate and de-identified record-level data to third-party data requestors generally; to the federal, provincial and territorial ministries of health; and to the Patented Medicine Prices Review Board.
4. NPDUIS releases aggregate data to the public.

**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

17136-0318

