anadian In
for H fo
t canadien
d'information sur la té

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.
. Ottawa, ON: CIHI; 2024.

Cette publication est aussi disponible en français sous le titre

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

•

Approved by

Brent Diverty
Vice President, Data Strategies and Statistics

Rhonda Wing
Executive Director, Chief Privacy O f cer and General Counsel, O f ce of the Chief Privacy O f cer 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 . Finally, CIHI releases certain aggregate data to the public, available on cihi.ca.

2.2 Data collection

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.

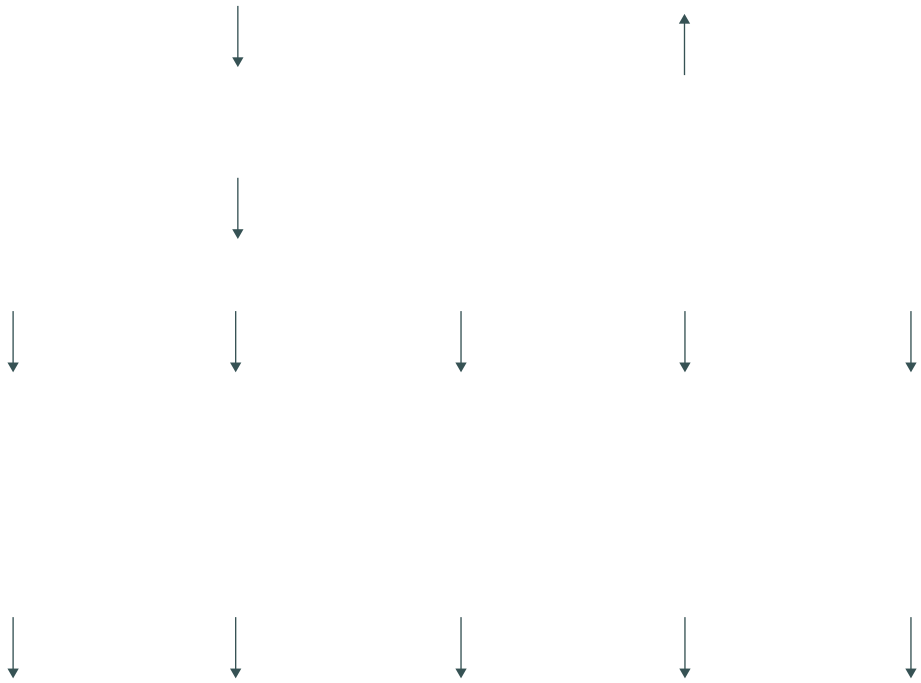
Once authenticated through CIHI's AMS, NPDUIS data providers submit record-level data from facilities that is electronically captured using specialized software, through CIHI's secure web-based electronic Data Submission Services (eDSS) or server-to-server application (Secure File Transfer Protocol).

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 .
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 and the associated . 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

3.2 Authorities governing NPDUIS data

General

CIHI adheres to its 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 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 , 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 o f cer is accountable for ensuring compliance with CIHI's . CIHI has a chief privacy o f cer and general counsel, a corporate Privacy, Con fdentiality and Security Committee, and a Governance and Privacy Committee of its Board of Directors.

Organization and governance

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 , 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 di f erences in policies, practices and service delivery; managemhin aqActity imta pnagem.use

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 . Access to CIHI's secure analytical environment is subject to an annual audit to ensure that staf 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 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 .

Criteria for approving data linkages are set out in sections 23 and 24 of CIHI's , 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 benefts of the linkage signifcantly ofset 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 specifc 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

as well as to terms specifc 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-identifed 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 .

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-identifed 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 , 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

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

.

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

. Aggregated statistics and analyses are made available in publications and on cihi.ca through tools such as Your Health System (e.g., report, report, Potentially Inappropriate Medication Prescribed to Seniors indicator).

Limiting retention

NPDUIS forms part of CIHI's data holdings and, con/Tcn

3.9 Principle 7: Safeguards for personal health information

CIHI's Privacy and Security Framework

CIHI's provides a compreh11eh11eh11eh11eh11eh11eh11eh11eh11e

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

and

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 a f ecting individuals. Requests from individuals seeking access to their personal health information will be processed in accordance with sections 60 to 63 of CIHI's

.

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

As set out in sections 64 and 65 of CIHI's , questions, concerns or complaints about CIHI's handling of information are investigated by the chief privacy o f cer 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

.

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