# National Prescription Drug Utilization Information System Database Privacy Impact Assessment

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

## Who We Are

Established in 1994, CIHI is an independent, not-for-profit corporation that provides essential information on Canada's health system and the health of Canadians. Funded by federal, provincial and territorial governments, we are guided by a Board of Directors made up of health leaders across the country.

## Our Vision

To help improve Canada's health system and the well-being of Canadians by being a leading source of unbiased, credible and comparable information that will enable health leaders to make better-informed decisions.

National Prescription Drug Utilization Information System (NPDUIS)
Database Privacy Impact Assessment (PIA)

Approved by:

Jean-Marie Berthelot
Vice President, Programs

Chief Privacy Officer

Ottawa – June 2011

# Table of Contents

# Ten Quick Facts About the NPDUIS Database

1. In September 2001, federal/provincial/territorial ministers of health announced plans to establish NPDUIS, based on a business case prepared by the Canadian Institute for Health Information (CIHI) and the Patented Medicine Prices Review Board (PMPRB).

2. In September 2006, CIHI launched the NPDUIS Database with drug claims data submitted from Manitoba and Saskatchewan.

3. As of May 2011, drug claims data are submitted to CIHI, using a secure electronic data submission service, for public drug programs in seven jurisdictions, namely Alberta, Saskatchewan, Manitoba, New Brunswick, Nova Scotia, Ontario and Prince Edward Island as well as preliminary data from the First Nations and Inuit Health Branch.

4. While not yet contributing drug claims data, British Columbia, Newfoundland and Labrador and the Yukon have committed to participating in the NPDUIS Database.

5. The NPDUIS Database is a pan-Canadian database, housing data related to public drug programs.

6. The NPDUIS Database was designed by CIHI to meet the needs of the participating federal/provincial/territorial public drug programs.

7. The NPDUIS Database provides data to inform discussion and decisions related to policy and the management of public drug programs in Canada.

8. The NPDUIS Database contains information, in both identified and de-identified form, on drug claimants collected from publicly financed drug benefit programs in Canada. In addition, the database contains formulary data, drug product information, and information regarding various public drug plan/program administrative policies. The NPDUIS Database contains 80 data elements.

9. Claims data identify a unique patient, prescriber and service provider (dispensing pharmacy) as well as cost and payment information in relation to prescribed drugs. This information is used to measure and analyze the pattern of drug use in Canada.

10. Some recently-released NPDUIS analytic reports include

    - *Drug Use Among Seniors on Public Drug Programs in Canada: 2002 to 2008*
    - *Proton Pump Inhibitor Use in Seniors: An Analysis Focusing on Drug Claims, 2001 to 2008*
    - *Antipsychotic Use in Seniors: An Analysis Focusing on Drug Claims 2001 to 2007*

# Executive Summary

The NPDUIS Database is a pan-Canadian database housing data related to public drug programs, including drug coverage or formulary information, drug claims, administrative policies, as well as population statistics. The NPDUIS Database was designed by the Canadian Institute for Health Information (CIHI) to meet the needs of the participating federal/provincial/territorial public drug programs, hereafter referred to as the "clients"—who are also the data providers—as well as the Patented Medicine Prices Review Board (PMPRB). CIHI provides the clients with access to aggregated data from the NPDUIS Database through web reports. As well, CIHI provides PMPRB with web access to de-identified record-level data through the NPDUIS analytical environment.

To use web reports, the clients must accept and agree to abide by operating principles set out by CIHI. The operating principles limit the users' rights to use and disclose confidential information, including aggregated data with small cell sizes obtained through the NPDUIS Database.

The privacy impact assessment (PIA) sets out the following recommendations:

**Recommendation 1:** Strengthen the terms of use of the current *Operating Principles for Use of NPDUIS Web Reports* and the associated pop-up notice to reflect CIHI's most up-to-date privacy and security practices to ensure that the clients and authorized users are aware of and understand their confidentiality and security restrictions and obligations.

**Recommendation 2:** As part of the education process for users, include in the training materials a clear and easily understood explanation of the obligations when accessing the web reports and the NPDUIS analytical environment.

# 1 Introduction

The Canadian Institute for Health Information (CIHI) collects and analyzes information on health and health care in Canada. Its goal is to provide timely, accurate and comparable information to inform health policies, support the effective delivery of health services and raise awareness among Canadians of the factors that contribute to good health. CIHI obtains data directly from hospitals, regional health authorities and ministries of health, including personal health information about recipients of health services, registration and practice information about health professionals and health facility information.

## 1.1 Privacy Impact Assessment Objectives and Scope

The purpose of this privacy impact assessment (PIA) is to examine the privacy, confidentiality and security risks associated with the NPDUIS Database. The PIA includes a review of the 10 privacy principles set out in Canadian Standards Association's *Model Code for the Protection of Personal Information* as they apply to the web reports and the NPDUIS analytical environment; it also includes a summary of potential privacy risks that have been identified, along with any measures that have been put in place to avoid or mitigate those risks.

This PIA is specific to the NPDUIS Database. It builds on two previous PIAs carried out in 2003 and 2006 that assessed and addressed key data protection issues throughout the development phases of the database.

# 2 NPDUIS Database Background and Context

## 2.1 Background

In September 2001, federal/provincial/territorial ministers of health announced the establishment of the NPDUIS Database, based on a business case prepared by CIHI and the Patented Medicine Prices Review Board (PMPRB). The stated objective of the NPDUIS Database was ". . . to provide critical analyses of price, utilization and cost trends so that Canada's health system has more comprehensive, accurate information on how prescription drugs are being used . . ."[i]

In February 2002, the federal budget allocated funding to CIHI to enable it to continue its efforts to provide improved information on health and health care throughout the country. As specified in the funding agreement between CIHI and the Government of Canada, the available funding enabled CIHI to develop and implement a prescription claims-level drug database.

i. Federal/Provincial/Territorial Health Ministers' Meeting, St. John's, Newfoundland and Labrador, September 26, 2001.

An NPDUIS Database steering committee was formed to provide advice to CIHI and PMPRB regarding the strategic and analytical direction and the overall development of the NPDUIS Database. The committee was comprised of individuals from the clients with expertise in drug program management, drug utilization research, policy development and standards development.

In March 2004, Health Canada awarded additional funding to CIHI to support the expansion of the NPDUIS Database project to include claims data funded by private payers.

An initial privacy impact assessment of the NPDUIS Database was completed in 2003. With the funding for the proposed expansion, the PIA was updated and revised to reflect the possibility of holding identifiable data, such as health card numbers and full birthdate for all drug claimants regardless of the source of payment (client organizations, private insurance or out-of-pocket).

In September 2006, CIHI launched the NPDUIS Database with drug claims data submitted from Manitoba and Saskatchewan. As of February 2011, drug claims data is submitted to CIHI, using a secure electronic data submission service, for public drug programs in seven jurisdictions: Alberta, Saskatchewan, Manitoba, New Brunswick, Nova Scotia, Ontario and Prince Edward Island. As of March 2011, CIHI has received preliminary data from the First Nations and Inuit Health Branch. While not yet contributing drug claims data, British Columbia, Newfoundland and Labrador and the Yukon are committed to participating in the NPDUIS Database.

In November 2007, CIHI formed a new NPDUIS Database advisory group to provide advice on operational issues such as data quality, database enhancements, report development and analysis.

The NPDUIS Database is designed to be flexible and scalable in order to address evolving information needs.

## 2.2 Description of the NPDUIS Database

The NPDUIS Database in its current form provides the clients with access to national, standardized, timely and accurate information on prescription drug utilization on public drug programs through comparative data and reports.

The NPDUIS Database contains health information, in both identified and de-identified form, on drug claimants collected from publicly financed drug benefit programs in Canada. In addition, the database contains information on drug claims data such as formulary data, drug product information and information regarding various public drug plan/program administrative policies.

An aggregated subset of the NPDUIS Database data is accessible by authorized users of the clients through pre-designed web reports. Small cell sizes in this controlled environment are not suppressed. The reports are flexible in a manner that permits users to select various inputs and outputs to allow some customization based on the users' business needs. Authorized users can carry out analysis and

planning on issues related to drug coverage, drug utilization, resourcing and cost efficiencies. In the future, the web reports may also permit authorized users to share reports, methodologies and findings with authorized users within and across participating client organizations.

A subset of the record-level NPDUIS Database data is accessible online via the NPDUIS analytical environment, but only by authorized users employed by the PMPRB. This environment is used to access de-identified record-level data, giving the PMPRB the ability to create customized queries to aggregate the data in the NPDUIS analytical environment. PMPRB is permitted to export only the aggregated data tables from the NPDUIS analytical environment for further analysis.

## 2.3 Description of Data Accessible Through the NPDUIS Database

The NPDUIS Database includes the following types of data:

- Claims data that identifies a unique patient, prescriber and service provider (dispensing pharmacy) as well as cost and payment information in relation to prescribed drugs:
  - Variables related to **claimants** of drug products (health card number [identified or de-identified depending on the jurisdiction], gender and date of birth);
  - Variables related to **providers** of drug products (pharmacy ID, postal code);
  - Variables related to the **prescribers** of the drug product (de-identified prescriber identifier, prescriber specialty code, postal code); and
  - Variables related to the **costs** of the drug product (ingredient, markup, professional fee).

  This information is used to measure and analyze the pattern of drug use in Canada.
- Formulary data that identify how drugs are covered on the various public drug programs.
- Standardized drug product data to identify the drugs being claimed or covered.
- Plan information, contextual data held external to the main system that outlines a variety of administrative policies of the public drug plans or programs that may explain differences in drug utilization patterns across the country.

With respect to information about claimants of drug products, it is important to note that names and addresses are not submitted to the NPDUIS Database and, therefore, are not found in the web reports or in the NPDUIS analytical environment.

The health card number (identified or de-identified), date of birth and postal code data is in the original data submitted to the NPDUIS Database and is removed from the analytical environment. These data elements are used only to support special studies that require linkage with other CIHI databases, to assign claimant age for age groupings and for special studies that involve sub-provincial analysis. These data elements are not included in the web reports or the NPDUIS analytical environment.

## 2.4 Organization and Governance

### 2.4.1 Organization

The NPDUIS Database was established as a program area in the Health Resources Information branch in February 2002. Responsibility for the NPDUIS Database was moved to the newly established Pharmaceuticals and Health Workforce Information Services branch in September 2009.

### 2.4.2 Governance

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

| Position/Group | Role/Responsibilities |
|---|---|
| **Vice President, Programs** | The Vice President, Programs, is responsible for the overall operations and strategic direction of the NPDUIS Database. |
| **Director, Pharmaceuticals and Health Workforce Information Services** | The Director is fully accountable for the NPDUIS Database. The Director is responsible for strategic and operational decisions and for ensuring its continued successful development. |
| **Manager, Pharmaceuticals** | The Manager is responsible for ongoing management, development and deployment of the NPDUIS Database. The Manager makes operational decisions, supports the NPDUIS Database advisory group and consults internally and externally as appropriate. |
| **NPDUIS Database Advisory Group** | Chaired by the Manager, Pharmaceuticals, and comprising representatives from the clients, this group provides advice on operational issues such as data quality, database enhancements, report development and analytical topics and methods. |
| **Vice President and Chief Technology Officer** | The Vice President and Chief Technology Officer is responsible for the strategic direction and overall operations/implementation of CIHI's technological and security solutions. |
| **Chief Privacy Officer** | The Chief Privacy Officer is responsible for the strategic direction and overall implementation of CIHI's privacy program. |
| **Senior Program Consultant, Security** | The Senior Program Consultant is responsible for providing guidance on maintaining and enhancing security for the web reports and the NPDUIS analytical environment and for assisting with documentation such as security impact assessments and threat and risk assessments. |

### 2.4.3 Authorities Governing the NPDUIS Database

CIHI adheres to its *Privacy Policy on the Collection, Use, Disclosure and Retention of Personal Health Information and De-Identified Data, 2010*, and to any applicable privacy legislation and/or agreements.

#### Legislation

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

All provinces and territories have public-sector privacy legislation in place. Canadian privacy legislation includes provisions that authorize public bodies covered by the acts to disclose person-identifiable data, without the consent of the individual, for statistical purposes. Alberta, Saskatchewan, Manitoba, Ontario and New Brunswick (legislation pending in Newfoundland and Labrador and Nova Scotia) also have health information–specific privacy legislation with express lawful authority to use and disclose personal health information, without individual consent, for purposes of management of the health system, including statistical analysis and reporting.

For example, CIHI is recognized as a prescribed entity under the *Personal Health Information Protection Act* of Ontario. Custodians in Ontario may disclose personal health information to CIHI without patient consent pursuant to Section 29 as permitted by Section 45(1) of the Act.

#### Agreements

CIHI has in place the following types of agreements:

- Bilateral and data sharing agreements between the provinces and territories and CIHI in support of data collection, and any subsequent data sharing with authorized users; and
- Data sharing and other types of agreements negotiated between other data providers and CIHI, which set out the purpose for collection, use, disclosure and retention requirements, as well as any subsequent data sharing that may be permitted.

### 2.4.4 NPDUIS Web Report Operating Principles and Data Access Agreement

A prerequisite to clients' use of the web reports is the acceptance and agreement to abide by the operating principles set out by CIHI (Appendix 3). If a jurisdiction chooses not to, or cannot, accept and agree to abide by the principles, then the service must not be used. The operating principles limit the users' rights to use data obtained through the NPDUIS Database for internal ministry purposes only and restricts the ministry and the users from allowing third parties to use the service in any manner.

The PMPRB's access to NPDUIS data is governed by the terms and conditions of the data access agreement between CIHI and the PMPRB. The data access agreement limits authorized users' rights to use and disclose confidential information, including de-identified record-level data, obtained through the NPDUIS analytical environment. Specifically, PMPRB authorized users are permitted to use such data solely for internal, non-commercial, local/regional, evidence-based decision-making, planning and analytical purposes. Confidential information cannot be further disclosed to any third party, except as expressly permitted in the data access agreement or as required by law. Publication or disclosure of reports or analyses outside of the PMPRB is permitted only where it is not reasonably foreseeable in the circumstances that the information could be used to identify individuals and where there are no cell sizes of fewer than five observations.

CIHI has ratified its terms and conditions of use whereby the clients and the PMPRB undertake to ensure that users of the web reports and the NPDUIS analytical environment in their organizations are aware of the terms and conditions of the applicable agreements.

In particular, PMPRB authorized users must be made aware of their strict obligation to

- Keep their username and password strictly confidential;
- Not export, download, print or in any way reproduce or store any de-identified record-level data obtained through the NPDUIS analytical environment;
- Keep any data, including any reports, strictly confidential and not disclose such data to persons or organizations outside their organization, except as expressly provided in the applicable agreements or as required by law;
- Use data obtained from the web reports or the NPDUIS analytical environment solely for non-commercial, internal purposes related to planning, research/analysis or decision-support activities, unless explicitly permitted by an agreement with CIHI;
- Not attempt to identify individuals when accessing and using data accessible through the web reports or the NPDUIS analytical environment, or attempt to link this data with personal health information originating from any other source; and

- Access the web reports and the NPDUIS analytical environment from their corporate network only.

The clients and the PMPRB agree to immediately notify CIHI of any unauthorized use of any users' means of access or any other breach of confidentiality or security of which they become aware.

In addition, both the operating principles and the data access agreement set out the following specific requirements and responsibilities with respect to usernames and passwords:

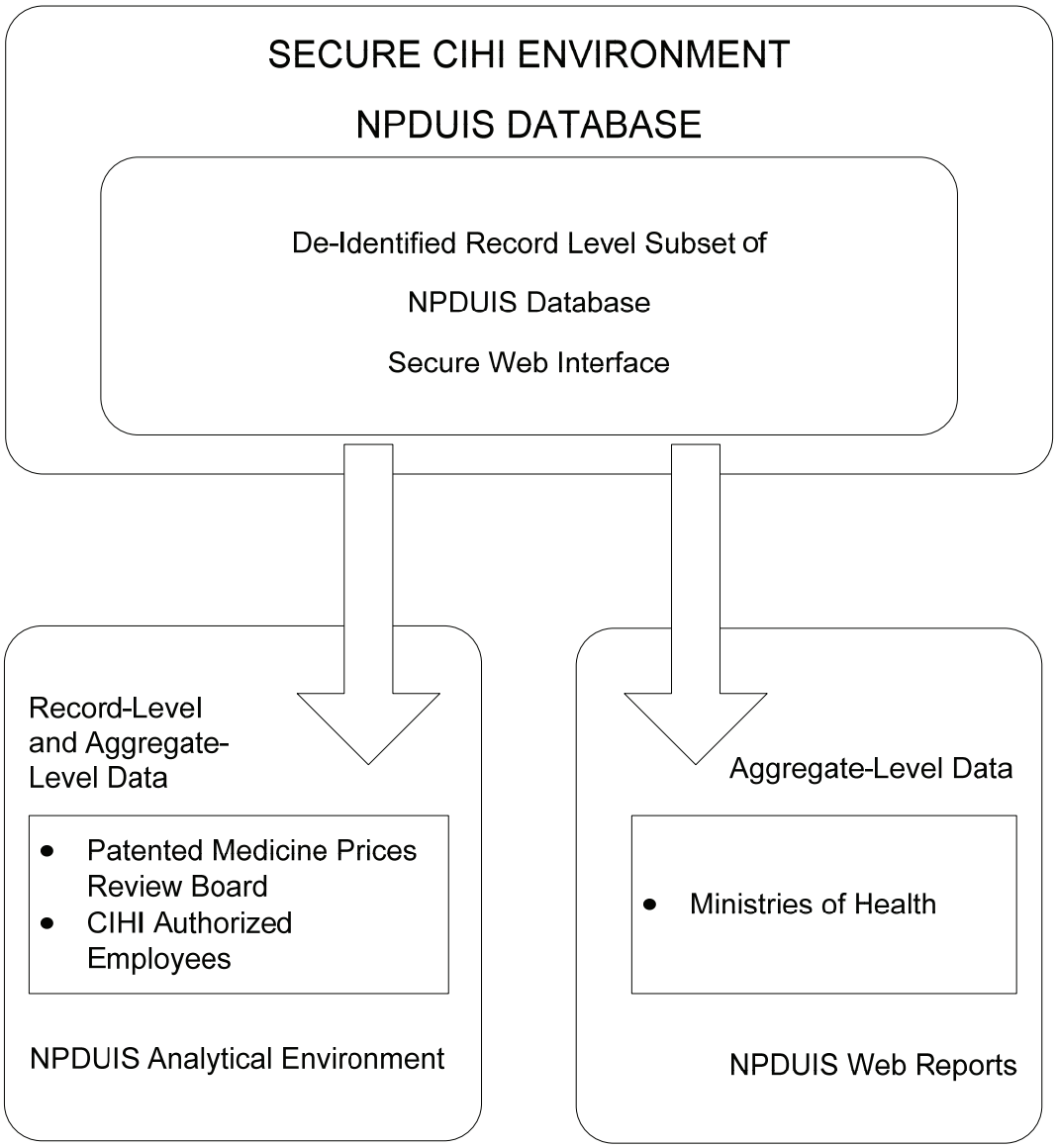
- Each user must create a user profile (name, title and email address), username and password on CIHI's website as instructed by CIHI;
- Users are responsible for maintaining the confidentiality of the means of access;
- Jurisdictions and the PMPRB and their users are fully responsible for all activities that occur under their means of access;
- Usernames and passwords cannot be shared and are non-transferable, nor can they be assigned to an unnamed individual or occupational position (for example, Director of Health Records);
- The clients, the PMPRB and their respective authorized users must not permit any third party or unauthorized user to access the web reports or the NPDUIS analytical environment; and
- Each authorized user will be issued a username and password that provides him or her with access to those areas of the web reports or the NPDUIS analytical environment that he or she is permitted to access.

As a reminder for the authorized users, a notice of use conditions is provided each time a user logs into the web reports or the NPDUIS analytical environment (see Appendix 4).

# 3 NPDUIS Database Conceptual Overview of Data Access

Authorized users access the NPDUIS web reports and the NPDUIS analytical environment through a secure web interface. Depending on their role, authorized users may be able to create custom queries or access reports created by CIHI and other NPDUIS Database users, both within and outside of their respective organizations. The aggregated data from these queries may be exported to other file formats (for example, MS Excel). The underlying de-identified record-level data is not to be exported.

Figure 1: NPDUIS Database Conceptual Overview of Data Access



# 4 Privacy Analysis

## 4.1 Principle 1: Accountability for Personal Health Information

CIHI's President and Chief Executive Officer is ultimately accountable for privacy and security at CIHI. The day-to-day responsibility has been delegated to CIHI's Chief Privacy Officer. Furthermore, CIHI has a corporate Privacy, Confidentiality and Security team mandated to review and, where appropriate, approve internal data linkages and external data requests that involve data linkages, disclosure outside of Canada and retention periods beyond three years. CIHI also has a Privacy and Data Protection Sub-Committee of its Board of Directors and an external Chief Privacy Advisor to advise the Chief Privacy Officer and the organization as a whole on any given privacy or security matter, as the need arises.

CIHI, the clients and the PMPRB are accountable for the application of the operating principles and data access agreements within their respective organizations. They are also subject to the requirements of data protection laws in their respective jurisdictions and the independent oversight of privacy commissioners or their equivalents.

## 4.2 Principle 2: Identifying Purposes for Personal Health Information

The NPDUIS Database provides data to inform discussion and decisions related to policy and the management of public drug programs in Canada.

## 4.3 Principle 3: Consent for the Collection, Use or Disclosure of Personal Health Information

The record-level data found in the NPDUIS Database, consisting of health information in both identified and de-identified form, is collected from the clients in its original form through the administration of the health care system. Data is typically disclosed to CIHI without individual consent for purposes of planning and management of the health system, including statistical analysis and reporting.

## 4.4 Principle 4: Limiting Collection of Personal Health Information

Data elements collected are limited to the minimum number required to meet the purposes of the collection. The data elements included in the NPDUIS Database were established based on consultations with federal/provincial/territorial drug plan representatives, as well as other key stakeholders.

No personal health information is accessed by external clients through the use of the web reports or the NPDUIS analytical environment. These are secure means of access to a selected subset of data already held at CIHI in the NPDUIS Database.

## 4.5 Principle 5: Limiting Use, Disclosure and Retention of Personal Health Information

### 4.5.1 Limiting Use

CIHI limits the use of web reports and the NPDUIS analytical environment for authorized purposes, and only authorized users have access. Specifically

- The operating principles limit the clients and their authorized users to access data for internal ministry use only; and
- The data access agreement limits the PMPRB's rights to use and disclose confidential information, including de-identified record-level data, accessed through the NPDUIS analytical environment. Specifically, the PMPRB and its authorized users are permitted to use such data solely in aggregate format for non-commercial, evidence-based decision-making, planning and analytical purposes.

**Privacy Risk—Inappropriate use and/or disclosure of web reports by authorized users**

Mitigation Measures Currently in Place

As described in Section 2.4.4, authorized users are required to agree with the operating principles and the data access agreement where applicable, which impose certain restrictions and obligations. Failure to respect the terms and conditions of the operating principles and the data access agreement would jeopardize their continued access to NPDUIS Database data. CIHI audits compliance through audits and periodic user verification, minimally on an annual basis, with the clients and the PMPRB. Authorized users are also subject to the requirements of data protection laws in their respective jurisdictions.

### 4.5.2 Limiting Disclosure

As part of its mandate, CIHI publishes aggregated data in a manner designed to minimize any risk of identification and residual disclosure. This generally requires that cells consist of a minimum of five observations.

CIHI recognizes, however, that the reports produced for the clients and the PMPRB through the web reports and the NPDUIS analytical environment are not reviewed for confidentiality in the same manner as are the analytical results that CIHI publishes and releases into the public domain.

Query results obtained through web reports may contain small cell sizes (defined as fewer than five occurrences) that are not suppressed in the reports produced and accessed by authorized users.

CIHI has implemented strict administrative controls stipulating that information obtained through the web reports and the NPDUIS analytical environment will not be published but will be used to inform internal decision-making in a specific health care environment.

Privacy Risk—Re-identification and residual disclosure (for example, the combination of data on age of patient, plus gender, province and drug use that could re-identify individuals and result in residual disclosure of personal health information)

### Mitigation Measures Currently in Place

The disclosure of reports produced by authorized users is limited to the clients who have agreed to the operating principles or the PMPRB through a signed data access agreement (see Appendix 4 for details), which imposes a variety of security restrictions and obligations on them.

The terms of the data access agreement prohibit the PMPRB from

- Attempting to identify individuals;
- Exporting, downloading, printing or in any way reproducing or storing any de-identified record-level data obtained through the NPDUIS analytical environment;
- Linking data using information gained from the NPDUIS Database; and
- Publishing findings that include cell sizes with fewer than five observations.

The data access agreement further stipulates that, in the case of demonstrated breaches, denial of further access to NPDUIS Database data may result.

In addition, specific protective measures implemented in the web reports and the NPDUIS analytical environment to control disclosures include the following:

- Only a select subset of variables from the NPDUIS Database have been included in the web reports and the NPDUIS analytical environment (approximately 60 data elements [see Appendix 2], not including calculated or descriptive data elements, for example, Number of Beneficiaries Paid or the Anatomical Therapeutic Chemical [ATC] Code broken down into levels 1 through 5);
- De-identification measures are applied to the data, for example, patients' date of birth, health card number and postal code, as well as prescriber and service providers are not included in the web reports or the NPDUIS analytical environment;

- The NPDUIS analytical environment allows direct access to de-identified individual records by authorized users, who
  - May create queries that return record-level data that must be aggregated prior to extraction; and
  - Must not extract the individual record-level data;
- The organizational contact for each jurisdiction and the PMPRB is responsible for naming authorized users and notifying CIHI;
- The undertaking of mandatory education (eLearning and instructor-led training) by users reinforces the appropriate use and disclosure of data from the NPDUIS Database; and
- Technical safeguards (for example, user ID and password, access audits and system performance monitoring) regulate the query environment and limit disclosure by minimizing risks of unauthorized access, including only providing access to named users (for further information, see Principle 7—Safeguards for Personal Health Information).

### Third-Party Data Requests

CIHI receives third-party data requests, primarily from researchers, for data to support research and analysis. Disclosures are made at the highest degree of anonymity possible to achieve the research purpose. Whenever possible, data is aggregated. Where aggregate data is not sufficiently detailed for the identified purpose, only the data elements required for the specified purpose are provided. Identifiers are removed and data elements that would lead to possible re-identification are truncated or rolled up to broader categories. For example, CIHI might release in a third-party record-level data request, with sufficient justification, the age in single years, age groups or age categories rather than providing the full date of birth.

Personal health information will not be disclosed unless

- Disclosure is required or authorized by law; or
- External data recipients have obtained the consent of the individuals concerned and have signed non-disclosure/confidentiality agreements.

Information on the proposed analyses and the data being requested must be submitted as part of third-party data requests. CIHI reviews the requests in accordance with its Privacy Policy, and, if approved, requestors must sign a data protection agreement that details the limits for the use of the data and binds the researcher to protect the information properly, to respect the sensitivity and confidentiality of the data, to not attempt to re-identify anyone in the data set and to destroy the data in a timely way in accordance with the agreement. It also provides CIHI with the right to audit compliance with the terms of the agreement.

## 4.5.3 Limiting Retention

NPDUIS Database data forms part of CIHI's information holdings and is retained as long as necessary for purposes of long-term analyses and reporting.

## 4.6 Principle 6: Accuracy of Personal Health Information

CIHI's Data Quality Framework is implemented annually on the NPDUIS Database. The Data Quality Framework is a CIHI-developed tool that is designed to provide a common, objective approach to assessing and documenting the data quality of its various data holdings along five general dimensions of quality: accuracy, comparability, timeliness, usability and relevance. Further information on CIHI's Data Quality Framework can be found on CIHI's website.

Any known data quality issues are addressed with the data provider or set out in data limitations documentation that is made available to all authorized users. The NPDUIS Database team verifies that the data available within the web reports and the NPDUIS analytical environment matches the data in the NPDUIS Database in terms of accuracy (that is, volume and completeness).

The NPDUIS Database team performs edit checks on the data submitted from the clients to identify duplicate records, missing and/or invalid data and inconsistencies in data transmissions. Feedback reports are provided to the clients for the purposes of taking action as required and/or supporting continuous improvements in data quality or enhancements to the data quality cycle. CIHI makes corrections to the data once the respective jurisdiction has communicated with CIHI. These are desirable practices from a data protection perspective because of the need to ensure accurate information in the database.

CIHI allows the clients to correct erroneous NPDUIS Database data during the entire submitting year and up to the closing date. This includes errors detected by CIHI or by the clients. Errors detected after the closing date are corrected when those errors affect a dollar amount greater than 10% of the total annual amount submitted by the respective jurisdiction. This latter point poses a risk to data quality, although a relatively minor one that is acceptable to CIHI.

## 4.7 Principle 7: Safeguards for Personal Health Information

CIHI has established physical, technical and administrative security practices to ensure the confidentiality and security of its data holdings.

In addition to the general safeguards already in place, the following technical and administrative safeguards have been implemented:

- Authorized users of the web reports and the NPDUIS analytical environment cannot turn off security features. Only the internal CIHI NPDUIS Database administrator has the ability to modify security filters, privileges and permissions.
- The encryption software incorporated uses a networking protocol called Secure Sockets Layer (SSL). SSL is a cryptographic protocol that provides secure communication on the internet for such things as web browsing, email, internet faxing, instant messaging and other data transfers.

- Usernames and passwords permit authentication and ensure that only authorized users can access the NPDUIS Database data.

**Privacy Risk—Unauthorized access to the web reports or the NPDUIS analytical environment**

Mitigation Measures Currently in Place

- User access
  - The system will lock out users after a pre-determined number of failed log-in attempts (because of the complexity of the passwords).
  - Sessions are disconnected after a set period of inactivity.
  - Users will be required to attain re-authorization from CIHI if they have not accessed the web reports or the NPDUIS analytical environment for a period of 90 days.
  - There is an annual verification audit and logs for access to the data, including validation by the clients and the PMPRB that authorized users remain current active employees with a continued business need for access.
- Ethical hacks
  - CIHI conducts an annual vulnerability assessment and penetration testing of select information systems (ethical hack). The intent of the assessment is to gather information on the selected systems and applications and then examine this information for weaknesses that could ultimately be used to compromise the underlying system and, hence, personal health information.
  - The latest ethical hack conducted in 2009 found that, in general, external facing systems (that is, via the internet) were well protected.
  - While the results of the 2009 ethical hack were generally positive, they were not specific to the NPDUIS Database**.**
- Web report operating principles and data access agreement
  - As described in Section 2.4.4, use of the web reports by authorized users in the client organizations is governed by the terms of the operating principles (see Appendix 3). Access to the web reports and the NPDUIS analytical environment by the PMPRB is governed by the terms and conditions of a data access agreement. The terms of the data access agreement, for example, state that authorized PMPRB users must use at least the same degree of care and oversight to maintain confidentiality as they would use to protect their own information but in no event less than a reasonable degree of care.

While the data access agreement with the PMPRB imposes specific confidentiality and security restrictions and obligations, the operating principles governing access to the NPDUIS web reports are not as comprehensive. There is no mention of the conditions of use and disclosure with respect to reports containing small cell sizes.

**Recommendation 1:** Strengthen the terms of use of the current *Operating Principles for Use of NPDUIS Web Reports* and the associated pop-up notice to reflect CIHI's most up-to-date privacy and security practices to ensure that the clients and authorized users are aware of and understand their confidentiality and security restrictions and obligations.

**Privacy Risk—Lack of control of usernames and passwords by NPDUIS Database authorized users, including active passwords that were assigned to users who are no longer employed by the clients or the PMPRB**

### Mitigation Measures Currently in Place

In order to be able to use the web reports or the NPDUIS analytical environment, each authorized user must agree to the NPDUIS Database notice of use conditions that set out specific requirements and responsibilities with respect to usernames and passwords each time he or she logs into the system. In addition to the requirement to keep their usernames and passwords strictly confidential, the clients and the PMPRB agree to immediately notify CIHI of any unauthorized use of any users' means of access or any other breach of confidentiality or security of which they become aware (see Section 2.4.4—NPDUIS Web Report Operating Principles and Data Access Agreement).

The operating principles for the web reports and the data access agreement for the NPDUIS analytical environment require that the clients and the PMPRB designate an organizational contact who is responsible for notifying CIHI of who, within the organization, will be named as users and to provide and maintain accurate, complete, true information about each user.

The NPDUIS Database team provides the organizational contact with annual reports outlining names of users, as well as usage, and asks for discrepancies to be reported.

**Recommendation 2:** As part of the education process for users, include in the training materials a clear and easily understood explanation of the obligations when accessing web reports and the NPDUIS analytical environment.

## 4.8 Principle 8: Openness About the Management of Personal Health Information

CIHI makes information available on its corporate website about its privacy policies, data practices and programs relating to the management of personal health information and de-identified data. As well, this PIA is accessible on CIHI's website (www.cihi.ca).

## 4.9 Principle 9: Individual Access to and Amendment of Personal Health Information

Personal health information held by CIHI is not used to make any administrative or personal health decisions affecting the individual. An individual seeking access to his or her personal health information will be processed in accordance with sections 60 to 63 of CIHI's *Privacy Policy on the Collection, Use, Disclosure and Retention of Personal Health Information and De-Identified Data, 2010*.

## 4.10 Principle 10: Complaints About CIHI's Handling of Personal Health Information

As set out in CIHI's *Privacy Policy on the Collection, Use, Disclosure and Retention of Personal Health Information and De-Identified Data, 2010*, complaints about CIHI's handling of personal health information are investigated by its Chief Privacy Officer. The Chief Privacy Officer may direct an inquiry or complaint to the Privacy Commissioner of the jurisdiction of the person making the inquiry or complaint.

# 5 Conclusion

This PIA summarizes CIHI's assessment of the privacy implications of the NPDUIS Database.

The few privacy risks that have been identified in this privacy impact assessment are deemed to be low and the mitigation measures currently in place reasonable, except as identified under Principle 7: Safeguards for Personal Health Information (Section 4.7). As such, two recommendations have been made to strengthen the conditions of use and disclosure of the data accessed through the NPDUIS web reports and NPDUIS analytical environment by the clients and authorized users.

# Appendix 1—Glossary of Terms

| Term | Definition |
|---|---|
| **NPDUIS analytical environment** | An analytical tool that provides authorized users with online access to de-identified record-level pan-Canadian drug utilization data in a secure environment that safeguards privacy and confidentiality. |
| **Authorized users** | Employees and contractors of CIHI, the clients and the PMPRB who have successfully completed required training and require access to the web reports or the NPDUIS analytical environment. |
| **Confidential information** | For purposes of the NPDUIS Database, confidential information includes personal health information. |
| **Data provider** | An organization, health care provider or other individual that discloses health information to CIHI; may include ministries of health, regional health authorities and similar bodies, hospitals, other health care facilities and professional colleges. |
| **De-identified information** | For purposes of the NPDUIS Database, record-level data that does not include patient name, date of birth, health card number or postal code. |
| **Ethical hack** | An assessment of the vulnerability and penetration testing of information systems. |
| **Health information** | A broad term including, but not limited to, financial information about health and health care, personal health information, de-identified data and aggregate data. |
| **Clients** | The federal/provincial/territorial public drug programs that have agreed to participate in activities related to the development and maintenance of the NPDUIS Database. |
| **Mitigation measures** | Means of reducing the possibility of privacy risks. |
| **National Prescription Drug Utilization Information System (NPDUIS) Database** | A national-level database that contains information regarding drug claims data as supplied by participating ministries of health in Canada. |
| **Personal health information** | Health information about an individual that<br>• Identifies the specific individual;<br>• May be used or manipulated by a reasonably foreseeable method to identify the individual; or<br>• May be linked by a reasonably foreseeable method to other information that identifies the individual.<br>Personal health information does not include health workforce information or health facility information as defined in CIHI's *Policy on Health Facility Identifiable Information*. |
| **Prescribed entity** | For purposes of the Ontario *Personal Health Information Protection Act*, an organization prescribed by the regulations made under this act to which personal health information may be disclosed for the purpose of analysis or compiling statistical information with respect to the management of, evaluation or monitoring of, the allocation of resources to or planning for all or part of the health system, including the delivery of services. |
| **Privacy impact assessment** | A tool used to assess the possible privacy-related consequences of systems and practices for the collection, use and disclosure of personal information, including personal health information. |
| **Privacy risk** | An undesirable event with the potential to compromise privacy or breach data confidentiality. |
| **Record-level data** | Data in which each record is related to a single individual or organization (also referred to as "micro data"). |

| Term | Definition |
|---|---|
| **Residual disclosure** | The combination of publicly released health information with other available information that reveals previously unknown information about an individual. |
| **Residual risk** | The remaining risk after the mitigation measures have been applied to the identified privacy risks. |
| **Secondary use** | For purposes of web reports or the NPDUIS analytical environment, the use of personal health information for purposes other than direct patient care (for example, statistical and analytical purposes). |
| **Web reports** | An analytical tool that provides authorized users with access to aggregate-level pan-Canadian drug utilization data in a secure environment that safeguards privacy and confidentiality. |

# Appendix 2—Examples of NPDUIS Analytical Environment Data

| Type of Information | Examples of Data and Variables |
|---|---|
| **Patient Demographic/ Geography** | • Unique de-identified CIHI patient identifier<br>• Province of residence or region of registration<br>• Age (actual, in years)<br>• Age group: younger than 65, 65 and older<br>• Gender |
| **Dispensing Organization Identification/Geography** | • De-identified CIHI service provider identifier<br>• Province<br>• Postal code |
| **Drug Claim Data** | • Utilization data (for example, ingredient cost submitted, costs paid, quantity of drug, days' supply) |
| **Drug Product Identification** | • Drug identification number (DIN) from Health Canada<br>• Pseudo-identification number (PDIN) from jurisdiction<br>• CIHI brand name<br>• CIHI strength and CIHI form |
| **Drug Classification System** | • Anatomical Therapeutic Chemical (ATC) Classification<br>• American Hospital Formulary System (AHFS) |
| **Prescriber Code and Type of Service** | • De-identified CIHI prescriber identifier<br>• Province<br>• Postal code |
| **Date and Time Periods** | • Actual service date—date dispensed<br>• Fiscal and calendar periods for analysis |
| **Derived Variables** | • NUM (for example, number of drug identification numbers, number of claims)<br>• SUM (for example, total cost accepted, total cost paid) |

# Appendix 3—Operating Principles for Use of NPDUIS Web Reports

The Canadian Institute for Health Information (CIHI) is pleased to offer the Ministry of Health access to CIHI's online National Prescription Drug Utilization Information System (NPDUIS) service. The service provides electronic access to aggregate data tables for use by a limited number of individual Ministry of Health users authorized by CIHI. The aggregate data to which the service provides access has been summarized and presented in a manner that does not permit identification of individuals.

If the ministry wishes to receive the service, CIHI will provide each user with a username and password ("means of access"). The ministry will be responsible for all activities undertaken or permitted by users provided with means of access. Further, the ministry will provide CIHI with the name of an organizational contact ("ministry contact") who holds a senior-level position and will notify CIHI of any change of the ministry contact. The ministry contact will represent the ministry in all communications and contact between the ministry and CIHI regarding the service. Michael Hunt, Manager, Pharmaceuticals, will represent CIHI in this area of responsibility.

The service is provided for internal ministry use only. Neither the ministry nor the users will allow third parties to use the service in any manner. The ministry will immediately notify CIHI of any unauthorized access to or use of the service. Means of access are non-transferable and may not be assigned to an unnamed individual, occupational position, department or organization. Due to operational requirements or other factors, constraints may be imposed from time to time by CIHI as to the number of users who may access the service. The ministry or CIHI may also direct that means of access associated with specific users be inactivated and eliminated. The service will be provided until either the ministry or CIHI notifies the other party in writing that the service is no longer desired or will no longer be provided, respectively.

Users must create a profile—containing their full name, department and full work mailing address—on CIHI's secure site in order to be provided with means of access. Users may access the service only from their place of work. Users will log off the service when not actively using it. Users will keep their means of access strictly confidential. The ministry will ensure that users are aware of their obligations regarding the service. CIHI will also make efforts to remind users of these obligations and will refer users to the ministry if they have any concerns or questions.

Although CIHI endeavours to ensure that the data is as current and accurate as possible, errors may occur. Therefore, CIHI cannot guarantee the accuracy of the data and users should, where possible, verify the data before acting on it. CIHI may make changes to the data and the service at any time and without notice. The ministry will not hold CIHI liable for any damages whatsoever arising from use of the service. Use of the service by the ministry and users is at the ministry's risk, and the ministry assumes all costs of such risk.

Use of the service is also governed by CIHI's privacy, confidentiality and security guidelines, found in the following document:
*Privacy and Confidentiality of Health Information at CIHI: Principles and Policies for the Protection of Personal Health Information and Policies for Institution-Identifiable Information*, 3rd edition, Ottawa: CIHI, 2002. It is available online at http://secure.cihi.ca/cihiweb/en/downloads/privacy_policy_priv2002_e.pdf

# Appendix 4—Online Service Agreements

## 1 NPDUIS Web Reports (Aggregate Data)

### Pop-Up Notice for Use of NPDUIS Database Service

The Canadian Institute for Health Information (CIHI) provides, as a service to the ministry, electronic access to NPDUIS Database aggregate data tables. As an authorized user of this service, you must be aware of and abide by CIHI's terms and conditions as conveyed to the ministry. These terms and conditions include, among other things, the following:

1. You will access the service from your place of work only.
2. Your username and password are
   - To be kept strictly confidential;
   - Not to be transferred to someone else; or
   - Not to be assigned to an unnamed individual, an occupational position, department or organization.
3. Your use of the service is for internal ministry purposes only.
4. You will not allow third parties to use the service in any manner.
5. You will log off the service when you are not actively using it.

Any questions or concerns about using this service should be directed to the appropriate official within the ministry.

Information about CIHI's privacy, confidentiality and security guidelines, which also govern this service, can be found in the following document: *Privacy and Confidentiality of Health Information at CIHI: Principles and Policies for the Protection of Personal Health Information and Policies for Institution-Identifiable Information*, 3rd edition, Ottawa: CIHI, 2002. It is available online at http://secure.cihi.ca/cihiweb/en/downloads/privacy_policy_priv2002_e.pdf

# 2 NPDUIS Analytical Environment (Users of Record-Level Data)

## Accessing NPDUIS Database Secure Analytical Environment

The Canadian Institute for Health Information (CIHI) provides through this site, as a service, electronic access to the NPDUIS Database claims records data, as well as aggregate data tables. As an authorized user of this service, you must be aware of and abide by the terms and conditions as agreed upon within the data access agreement that your organization has with CIHI. These terms and conditions include, among other things, the following:

1. The service will be accessed only through the provided web-based analytical tool from the physical offices agreed upon within the terms of the agreement.
2. Your username and password are
   - To be kept strictly confidential;
   - Not to be transferred to someone else; or
   - Not to be assigned to an unnamed individual, an occupational position, department or organization.
3. Your use of the service is for internal analytical purposes only.
4. You will not export or download record-level claims data for any purpose.
5. You will not allow third parties to use the service in any manner.
6. You will log off the service when you are not actively using it.

Any questions or concerns about using this service should be directed to the appropriate official within your organization.

Information about CIHI's privacy, confidentiality and security policy, which also govern this service, can be found in the following document: *Privacy and Confidentiality of Health Information at CIHI: Principles and Policies for the Protection of Personal Health Information and Policies for Institution-Identifiable Information*, 3rd edition, Ottawa: CIHI, 2002. It is available online at http://secure.cihi.ca/cihiweb/en/downloads/privacy_policy_priv2002_e.pdf

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
copyright@cihi.ca



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*.

# Talk to Us

CIHI Ottawa
495 Richmond Road, Suite 600
Ottawa, Ontario  K2A 4H6
Phone: 613-241-7860

CIHI Toronto
4110 Yonge Street, Suite 300
Toronto, Ontario  M2P 2B7
Phone: 416-481-2002

CIHI Victoria
880 Douglas Street, Suite 600
Victoria, British Columbia  V8W 2B7
Phone: 250-220-4100

CIHI Montréal
1010 Sherbrooke Street West, Suite 300
Montréal, Quebec  H3A 2R7
Phone: 514-842-2226

CIHI St. John's
140 Water Street, Suite 701
St. John's, Newfoundland and Labrador  A1C 6H6
Phone: 709-576-7006

July 2011

www.cihi.ca

Canadian Institute for Health Information

Institut canadien d'information sur la santé