Hospital Mental Health Database
Privacy Impact Assessment
July 2016
The Canadian Institute for Health Information (CIHI) is pleased to publish the following privacy impact assessment in accordance with its Privacy Impact Assessment Policy:

- Hospital Mental Health Database, June 2016

Approved by:

Brent Diverty
Vice President, Programs
Ottawa – June 2016

Anne-Mari Phillips
Chief Privacy Officer & General Counsel
About the Hospital Mental Health Database

1. The Hospital Mental Health Database (HMHDB) is a pan-Canadian database containing information regarding hospital inpatient care provided for mental illness and addictions.

2. Unlike most CIHI databases, the HMHDB does not collect data directly from data providers. Instead, psychiatric and general hospitals submit data to CIHI databases that are intended to capture hospital information. Hospital data that concerns mental illness and addictions is extracted from these databases and exported to the HMHDB.

3. By extracting data from its source databases, the HMHDB contains data representing more than 800 facilities.

4. Once extracted to the HMHDB, the data is used to produce accurate, timely and comparable statistical information concerning hospital treatment for mental illnesses and addictions, such as the types of conditions treated, length of hospitalization, rehospitalization rates and demographic characteristics.

5. This statistical information helps facilities, ministries of health, regional health authorities, researchers and the public identify year-over-year trends, assess the impact of policies and practices, and compare outcomes across jurisdictions.
1. Introduction

The Canadian Institute for Health Information (CIHI) collects and analyzes information on health and health care in Canada. Its mandate is to deliver comparable and actionable information to accelerate improvements in health care, health system performance and population health across the continuum of care. CIHI obtains data from hospitals and other health care facilities, long-term care homes, regional health authorities, medical practitioners and governments. This data includes information about health services provided to individuals, the health professionals who provide those services and the cost of the health services.

The purpose of this privacy impact assessment (PIA) is to examine the privacy, confidentiality and security risks associated with the Hospital Mental Health Database (HMHDB). 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 the HMHDB. The primary driver for this PIA is compliance with CIHI’s Privacy Impact Assessment Policy.

2. Background

2.1 Introduction to the HMHDB

The HMHDB is a pan-Canadian database containing information regarding hospital inpatient care provided for mental illness and addictions. Unlike most CIHI databases, the HMHDB does not collect data directly from data providers. Instead, psychiatric and general hospitals submit data to CIHI databases that are intended to capture hospital information. Hospital data that concerns mental illness and addictions is extracted from these databases and exported to the HMHDB. Once extracted to the HMHDB, the data is used to produce accurate, timely and comparable statistical information about

- The types of mental illnesses and addictions for which Canadians are hospitalized;
- The length of hospitalization for various mental illnesses and addictions;
- Rehospitalization rates for various mental illnesses and addictions; and
- Demographic characteristics of individuals hospitalized for various mental illnesses and addictions.
This statistical information helps facilities, ministries of health, regional health authorities, researchers and the public identify year-over-year trends, assess the impact of policies and practices, and compare outcomes across jurisdictions.

The HMHDB does not currently include information regarding mental health care that hospitals provide on an outpatient basis, some of which is available in the National Ambulatory Care Reporting System (NACRS) and the Discharge Abstract Database/Hospital Morbidity Database (DAD/HMDB). The HMHDB also does not currently include information regarding mental health care provided outside of hospitals.

There is 1 exception to the above statement that HMHDB does not collect data directly from data providers. A fraction of 1% of records found in the HMHDB are collected directly from hospitals, which submit de-identified data directly to the HMHDB.

### 2.2 History of the HMHDB

Prior to 1994, Statistics Canada’s Mental Health Statistics program was responsible for collecting data about hospital inpatient care provided for mental illness and addictions, via the Hospital Mental Health Survey (HMHS). While Statistics Canada still maintains historical data for 1930 to 1994, CIHI assumed responsibility for collecting, compiling, analyzing and disseminating data regarding mental health hospitalizations as of the 1994–1995 fiscal year. Since that time, almost all HMHS facilities have migrated to reporting through the DAD/HMDB or the Ontario Mental Health Reporting System (OMHRS). As reporting migrated from HMHS to DAD/HMDB and OMHRS, additional data elements became available (e.g., health care number)\(^i\) and these have been incorporated into the HMHDB to improve analytical capabilities. (For more information, see Section 3.7.)

### 2.3 Where HMHDB data comes from

Unlike most CIHI databases, the HMHDB does not collect data directly from data providers; it extracts data from other CIHI databases.

Psychiatric and general hospitals (and in some cases chronic and rehabilitation facilities) submit data to CIHI databases that are intended to capture hospital information, specifically, the DAD/HMDB and OMHRS.

---

i. Most data providers submit unencrypted health care numbers to CIHI. Analysis at CIHI, however, is generally conducted with the use of de-identified record-level data, where the health care number has been removed or encrypted. For more information, see Section 3.8, under the heading “System security.”
The DAD/HMDB receives data from acute care facilities or from their respective regional health authority or ministry of health. Facilities in all provinces and territories except Quebec are required to report to the DAD/HMDB. Data from Quebec is submitted to CIHI via the ministère de la Santé et des Services sociaux du Québec. This data is appended to the DAD to create the HMDB component.

Since 2006, Ontario facilities with designated adult mental health beds have been mandated by the Ontario Ministry of Health and Long-Term Care to report psychiatric data to CIHI via OMHRS. Facilities in other provinces participate in OMHRS on a voluntary basis. Data has been extracted from OMHRS and exported to the HMHDB since the 2006–2007 fiscal year.

Inpatient mental health care that is provided by an Ontario hospital but not through a designated mental health bed is submitted to CIHI via the DAD/HMDB.

The hospital data found in the above-mentioned hospital databases (DAD/HMDB and OMHRS) is extracted and exported to the HMHDB if the data concerns mental illness and addictions. (See Section 3.6, under the headings “Extracting only certain records” and “Extracting only certain data elements,” for more information about this extraction process.) By extracting data from its source databases, HMHDB contains data representing over 800 facilities.

Figure 1 illustrates how data flows to the HMHDB via the DAD/HMDB and OMHRS.
Figure 1  HMHDB data flow
3. Privacy analysis

As indicated in Section 2.3, rather than collecting data directly from data providers, the HMHDB extracts data from other CIHI databases. Data collection takes place when HMHDB’s source databases collect data from facilities. For a discussion of how those databases limit collection, see CIHI’s Clinical Administrative Databases PIA (which addresses DAD/HMDB) and OMHRS PIA.

When the HMHDB extracts data from other CIHI databases for use in the HMHDB, this constitutes a “use” of data. Therefore, this PIA discusses how the 10 privacy principles apply to CIHI’s use of data in the context of the HMHDB.

3.1 Authorities governing HMHDB data

General

HMHDB data is governed by CIHI’s Privacy Policy, 2010 (which is discussed throughout this PIA), as well as legislation in the jurisdictions and data-sharing agreements with the provinces and territories (which are discussed in this section).

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: Alberta, Saskatchewan, Manitoba, Ontario, New Brunswick, Nova Scotia, Newfoundland and Labrador and the Northwest Territories (Yukon and Prince Edward Island are also in the process of implementing such legislation). 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 Ontario’s Personal Health Information Protection Act, 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

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.

3.2 Principle 1: Accountability for Personal Health Information

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

Organization and governance

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

<table>
<thead>
<tr>
<th>Position/group</th>
<th>Roles/responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vice president, Programs</td>
<td>Responsible for providing overall leadership and oversight regarding the acquisition, management and reporting of HMHDB data</td>
</tr>
<tr>
<td>Director, Methodologies and Specialized Care</td>
<td>Responsible for operational and strategic decisions regarding HMHDB data</td>
</tr>
<tr>
<td>Manager, Rehabilitation and Mental Health</td>
<td>Responsible for ongoing management of HMHDB data, including data quality and reporting</td>
</tr>
<tr>
<td>Chief information security officer</td>
<td>Responsible for the strategic direction and overall implementation of CIHI’s Information Security Program</td>
</tr>
<tr>
<td>Chief privacy officer</td>
<td>Responsible for the strategic direction and overall implementation of CIHI’s Privacy Program</td>
</tr>
<tr>
<td>Manager, ITS Health Information Applications</td>
<td>Responsible for ensuring availability of technical resources and solutions for ongoing operations and enhancements of HMHDB data</td>
</tr>
</tbody>
</table>
3.3 Principle 2: Identifying Purposes for Personal Health Information

HMHDB data is used to produce accurate, timely and comparable statistical information about inpatient mental health care provided by Canadian hospitals. The statistical information addresses

- The types of mental illnesses and addictions for which Canadians are hospitalized;
- The length of hospitalization for various mental illnesses and addictions;
- Rehospitalization rates for various mental illnesses and addictions; and
- Demographic characteristics of individuals hospitalized for various mental illnesses and addictions.

This statistical information helps facilities, ministries of health, regional health authorities, researchers and the public identify year-over-year trends, assess the impact of policies and practices, and compare outcomes across jurisdictions.

The types of data in the HMHDB and the reasons they are required are discussed in Section 3.6.

3.4 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.

3.5 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 and monitoring of the health care systems.
3.6 Principle 5: Limiting Use, Disclosure and Retention of Personal Health Information

Limiting use

CIHI limits the use of data in the HMHDB to the authorized purposes described in Section 3.3. 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.

Extracting only certain records

As indicated in Section 2.3, rather than collecting data directly from data providers, the HMHDB extracts data from other CIHI databases. The HMHDB extracts only the records required for its purposes.

The large majority of records in the HMHDB are extracted from the DAD/HMDB. The HMHDB extracts all DAD/HMDB records originating from psychiatric hospitals, as all records from psychiatric hospitals are relevant for the HMHDB’s purposes.

For DAD/HMDB records originating from general hospitals, the HMHDB’s extraction of records is guided by the HMHDB’s Grouping Table — a list of mental illness and addictions diagnoses (described by ICD and DSM codes)\(^\text{ii}\) that are within the scope of the HMHDB. The HMHDB extracts only the records from general hospitals that contain a most responsible diagnosis that corresponds to a mental illness or addiction identified in the Grouping Table.

In addition to extracting records from the DAD/HMDB, the HMHDB also extracts all records from OMHRS. When using OMHRS records to conduct analyses, however, HMHDB analysts usually use only the OMHRS records that contain a most responsible diagnosis that corresponds to a mental illness or addiction included in the HMHDB’s Grouping Table.

Extracting only certain data elements

Whether a record is extracted from the DAD/HMDB (psychiatric or general hospitals) or OMHRS, the HMHDB extracts only the data elements necessary for the HMHDB’s purposes. These data elements are determined by CIHI each year, but typically remain the same; some data elements are added or deleted from time to time as necessary. Table 2 describes the types of data elements extracted to the HMHDB and why they are necessary.

\(^{\text{ii. ICD: International Classification of Diseases; DSM: Diagnostic and Statistical Manual of Mental Disorders.}}\)
Table 2  Types of HMHDB data elements

<table>
<thead>
<tr>
<th>Description</th>
<th>Example</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identifying information</td>
<td>Encrypted health care number</td>
<td>To determine which services are provided to which individuals</td>
</tr>
<tr>
<td>Clinical data</td>
<td>Most responsible diagnosis</td>
<td>To permit analyses regarding which conditions are being treated</td>
</tr>
<tr>
<td>Demographic data</td>
<td>Homeless status</td>
<td>To permit analyses regarding which populations are being treated</td>
</tr>
<tr>
<td>Administrative data</td>
<td>Facility identification number</td>
<td>To permit analysis of health systems</td>
</tr>
</tbody>
</table>

Need for record identifiers

Each HMHDB record reflects a separation from a hospital, meaning that an individual is either discharged from hospital or dies. Therefore, where an individual is admitted and discharged 3 times in a given fiscal year, 3 HMHDB records result. Earlier in the HMHDB's development, the database had no mechanism by which to identify the fact that all 3 discharges pertained to the same individual. This limited the types of analyses that the HMHDB could facilitate.

To address this issue, encrypted health care numbers from source databases (i.e., the DAD/HMDB, OMHRS) were made available in the HMHDB for data years 2006–2007 and onward.iii This permitted HMHDB analysts to identify the services provided to the same individual, which significantly expanded the scope of analyses that could be performed (e.g., rehospitalization of the same individual for the same condition). To improve the accuracy of data linkages, a data element indicating which province/territory issued the individual's health care number was added to HMHDB records for data years 2006–2007 and onward. For more information, see the “Client linkage standard” discussion in this section.

Data linkage

Data linkages are performed between HMHDB data and other CIHI data sources. The linked data remains subject to the use and disclosure provisions in the Privacy Policy, 2010.

While data linkage potentially causes greater risk of identification of an individual, the Privacy Policy, 2010 imposes the following mitigating measures to reduce that risk.

---

iii. Most data providers submit unencrypted health care number to CIHI. Analysis at CIHI, however, is generally conducted with the use of de-identified record-level data, where the health care number has been removed or encrypted. For more information, see Section 3.8 under the heading “System security.”
Sections 14 to 31 of CIHI's *Privacy Policy, 2010* govern the 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.

Criteria for approval of data linkages are set out in Section 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.

**Client linkage standard** (with limited exceptions)

Under this standard, records are linked by using a combination of encrypted health care number and the province/territory that issued the individual’s health care number.

**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 both data linkages for CIHI’s own purposes and for third-party data requests.

Return of own data

Section 34 of CIHI’s Privacy Policy, 2010 establishes that the return of data to the facility that originally provided it to CIHI is not considered a disclosure; rather, it is considered a use. Section 34 also discusses the return of own data to the relevant ministry of health.

Because the HMHDB does not collect data directly from facilities, it does not return data to facilities (or to ministries). For a discussion of return of own data from HMHDB’s source databases, see CIHI’s Clinical Administrative Databases PIA (which addresses the DAD/HMDB) and OMHRS PIA.

Limiting disclosure

Public release of HMHDB data

As part of its mandate, CIHI publicly releases aggregate data only, in a manner designed to minimize any risk of identification and residual disclosure. Aggregate statistics and analyses are made available in publications and on CIHI’s website. This generally requires a minimum of 5 observations per cell.

In compliance with these principles, beginning with the 2003–2004 data year, aggregate data from the HMHDB is available via CIHI’s Quick Stats web tool. Historic reports regarding hospital mental health services can be found on CIHI’s website as well.

Third-party data requests

Customized de-identified record-level and/or aggregate data from the HMHDB may be requested by a variety of users, such as various levels of government, health care decision-makers and researchers.

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 aggregate 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.
Both the HMHDB and its source databases are used to respond to data requests from third parties. To ensure that consistent processes are used for the de-identification of data, CIHI’s third-party data request program has developed a series of forms and checklists that are available to staff who process third-party record-level data requests.

In 2009, CIHI adopted a complete life cycle approach to data management. As part of that life cycle, Privacy and Legal Services (PLS) has developed and is responsible for the ongoing compliance monitoring process whereby all data sets that are disclosed to third-party data recipients are tracked and monitored for secure destruction at the end of their life cycle. Prior to disclosing data, third-party recipients sign a data protection agreement and agree to comply with the conditions and restrictions imposed by CIHI relating to the collection, purpose, use, security, disclosure and return or disposal of data.

Data requestors are required to submit a written request. 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 of the publication of cell sizes less than 5; and
- The use of strong encryption technology that meets or exceeds CIHI’s standards where mobile computing devices are used.

As of January 2011, 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 are continuing to comply with their obligations as set out in the data request form and data protection agreement signed with CIHI.

**Limiting retention**

The HMHDB 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.

Even though HMHDB records are based on data extracted from other CIHI databases, where each source database codes the information in a different fashion, the HMHDB converts the data into HMHDB’s standardized format. Also, HMHDB records contain certain data which the HMHDB derives based on data in the source records. The data in HMHDB records associated with these processes is unique and will be retained as part of this data holding.
3.7 Principle 6: Accuracy of Personal Health Information

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

Similar to other CIHI data holdings, the HMHDB is subject to a data quality assessment on a regular basis, based on CIHI’s Data Quality Framework. The HMHDB data quality assessment is informed by data quality assessments performed for HMHDB’s source databases, and includes numerous activities to assess the various dimensions of quality, including the accuracy of HMHDB data.

3.8 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 the HMHDB data are highlighted below.

System security

CIHI recognizes that information is secure only if it is secure throughout its entire lifecycle: creation and collection, access, retention and storage, use, disclosure and disposition. 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. In exceptional instances, staff will require access to original health
care numbers. Section 10 of CIHI’s *Privacy Policy, 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 communication about CIHI’s privacy and security policies and procedures. 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. 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.
3.9  **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 on [www.cihi.ca](http://www.cihi.ca).

3.10  **Principle 9: Individual Access to, and Amendment of, Personal Health Information**

As indicated in Section 2.3, rather than collecting data directly, the HMHDB extracts data from other CIHI databases. An individual may request access to their personal health information found in those source databases, as indicated in CIHI’s Clinical Administrative Databases PIA (which addresses the DAD/HMDB) and OMHRS PIA.

3.11  **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 the HMHDB did not identify any privacy risks.