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

- Ontario Mental Health Reporting System Privacy Impact Assessment, November 2016

Approved by:

Brent Diverty
Vice President, Programs

Anne-Mari Phillips
Chief Privacy Officer & General Counsel

Ottawa – November 2016
# Table of contents

Quick facts about the Ontario Mental Health Reporting System ................................................. 4

1 Introduction .............................................................................................................................. 5

2 Background ............................................................................................................................ 5
   2.1 Introduction to mental health data and OMHRS .......................................................... 5
   2.2 Data providers .............................................................................................................. 6
   2.3 Data collected .............................................................................................................. 7
   2.4 Data flow and access management ............................................................................ 11

3 Privacy analysis ..................................................................................................................... 13
   3.1 Privacy and Security Risk Management Program ...................................................... 13
   3.2 Authorities governing OMHRS data ......................................................................... 14
   3.3 Principle 1: Accountability for personal health information ..................................... 15
   3.4 Principle 2: Identifying purposes for personal health information ............................ 16
   3.5 Principle 3: Consent for the collection, use or disclosure of personal health information ................................................................. 17
   3.6 Principle 4: Limiting collection of personal health information ................................. 17
   3.7 Principle 5: Limiting use, disclosure and retention of personal health information ........ 18
   3.8 Principle 6: Accuracy of personal health information ................................................ 24
   3.9 Principle 7: Safeguards for personal health information ............................................ 24
   3.10 Principle 8: Openness about the management of personal health information ........... 26
   3.11 Principle 9: Individual access to, and amendment of, personal health information .......... 26
   3.12 Principle 10: Complaints about CIHI’s handling of personal health information ......... 26

4 Conclusion .............................................................................................................................. 26

Appendix ................................................................................................................................... 27
Quick facts about the Ontario Mental Health Reporting System

1. The Ontario Ministry of Health and Long-Term Care mandated the implementation of the Ontario Mental Health Reporting System (OMHRS), with data collection that commenced on October 1, 2005.

2. OMHRS is a longitudinal reporting system that captures data on hospital mental health inpatients at multiple points throughout their episodes of care.

3. It is designed to capture standardized, patient-specific clinical, demographic, administrative and resource utilization information within a single reporting framework.

4. OMHRS is designed to accept data on all patients who have been admitted to hospitals with designated adult mental health beds for inpatient mental health services.

5. It excludes mental health data from outpatient or community-based services, residential care facilities, centres for the care of individuals with intellectual disabilities, group homes or private practitioners.

6. OMHRS is used to report services provided in more than 5,000 mental health beds. Each fiscal year, on average, OMHRS reflects approximately
   - 43,000 individual patients (i.e., unique people);
   - 53,000 hospitalization episodes; and
   - 99,000 assessments (i.e., each episode includes one or more assessments).

7. OMHRS data is used to produce a variety of outputs to support
   - Provincial accountability, through reporting of comparable health indicators of access, outcomes and service utilization;
   - Inpatient adult mental health programs, facility and system-level strategic and operational management, benchmarking and quality improvement; and
   - Clinical and policy research and analyses.

8. A picture of the patients, their clinical and demographic characteristics, their use of resources, and their outcomes can be developed over time. This enables accurate and timely cross-sectional analysis of patients even prior to their discharge from the designated mental health bed.

9. Information is also collected on hospital characteristics — type, size and location — to provide contextual information for analysis of quality and utilization data.
10. Recent analyses produced by CIHI using data from OMHRS include the characteristics of senior inpatient mental health clients (age 65 and older) in Ontario, care for children and youth with mental disorders, self-harm and assault among children and youth, eating disorders among young women, as well as the relationship between concurrent mental illness and addictions and subsequent inpatient readmission and length of hospital stay.

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 healthcare 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 Ontario Mental Health Reporting System (OMHRS). 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 OMHRS. The primary driver for this PIA is compliance with CIHI’s Privacy Impact Assessment Policy.

2 Background

2.1 Introduction to mental health data and OMHRS

Prior to 1994, Statistics Canada’s Mental Health Statistics program was responsible for collecting data regarding 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 1994–1995. Since that time, almost all HMHS facilities have migrated to reporting through the Discharge Abstract Database
(DAD)/Hospital Morbidity Database (HMDB) or OMHRS. As reporting migrated from the HMHS to these databases, additional data elements became available (e.g., Health Care Number)i which have been incorporated into OMHRS to improve analytical capabilities.

The Ontario Ministry of Health and Long-Term Care (the Ontario ministry) mandated the implementation of OMHRS with data collection that commenced on October 1, 2005. OMHRS is designed to capture standardized, patient-specific, clinical, demographic, administrative and resource utilization information within a single reporting framework.

It is a longitudinal reporting system that captures data on hospital mental health inpatients at multiple points throughout their episodes of care. A key component of OMHRS is that data is collected through the Resident Assessment Instrument–Mental Health (RAI-MH)©, developed by the Ontario ministry and the Ontario Hospital Association in collaboration with interRAI, an international consortium of health researchers.

An agreement between the Ontario ministry, the Ontario Hospital Association and CIHI set in motion the development and implementation of OMHRS. This provided the opportunity to use the RAI-MH for collecting data about adult inpatients admitted to designated mental health beds across the province of Ontario, with the potential of moving toward pan-Canadian use. The Ontario ministry is the primary provincial stakeholder and sponsor of OMHRS, while CIHI has operational responsibilities for the construction and management of the database along with related processing, reporting and educational activities.

### 2.2 Data providers

Since October 1, 2005, Ontario facilities with designated adult mental health beds have been mandated by the Ontario ministry to report psychiatric data to CIHI via OMHRS. Facilities in other provinces participate in OMHRS on a voluntary basis.

The Ontario ministry has mandated all hospitals with designated adult inpatient mental health beds to submit mental health data collected using the RAI-MH instrument to CIHI. These designated mental health beds are located in general hospitals and in specialty psychiatric hospitals. All hospitals with designated adult inpatient mental health beds have an “MH” Master Number for use with those beds. This Master Number is used to identify the mental health unit(s) within a hospital for various reporting activities, including data submission to OMHRS. There are approximately 70 OMHRS-participating facilities with an MH Master Number. Due to various mergers and closures of various inpatient mental health units and facilities, this number fluctuates slightly on an annual basis.

---

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. See Section 3.9, “System security,” for more information.
Since 2008, the OMHRS database has also included data from Newfoundland and Labrador and Manitoba. In the coming years, CIHI will work with other hospitals and jurisdictions that are interested in implementing the RAI-MH instrument and submitting data to the OMHRS database at CIHI.

2.3 Data collected

The data submitted to OMHRS is required by the hospitals themselves in order to provide care and to plan, conduct and manage the delivery of inpatient mental health services.

The process for performing the RAI-MH assessment requires that information about patients be gathered from multiple sources, including the patient, the patient’s family or other health care team members through observation, interviews, reviewing lab results, and so forth. Interdisciplinary team members may be nurses, social workers, occupational therapists and physicians.

Prior to the commencement of the Ontario ministry mandate in 2005, CIHI led the development of a technical solution to support OMHRS functions and provided technical specifications to software vendors for the development of data capture and submission software products. Participating hospitals use these vendor products to collect OMHRS data and to submit it directly to CIHI.

OMHRS is designed to accept data on all adult patients who have been admitted for inpatient mental health services. OMHRS includes clinical, administrative and resource information to support inpatient mental health services planning. OMHRS data is limited to adult inpatient mental hospital events and excludes mental health data from outpatient or community-based services, residential care facilities, centres for the care of individuals with intellectual disabilities, group homes and private practitioners. However, if patients younger than 18 are in a designated adult bed in a hospital, or in a designated children’s mental health bed that uses the RAI-MH instrument (which is rare), for example, data for those inpatient episodes is also included. The majority of data relating to services provided in designated children’s mental health beds is not submitted to OMHRS but, rather, continues to be submitted to the DAD.

OMHRS is used to report services provided in more than 5,000 mental health beds. Each fiscal year, on average, OMHRS reflects approximately

- 43,000 individual patients (i.e., unique people);
- 53,000 hospitalization episodes; and
- 99,000 assessments (i.e., each episode includes one or more assessments).
Data collected through RAI-MH assessments accounts for most of the information submitted to OMHRS. Additional administrative and clinical data elements beyond the RAI-MH instrument are listed later in this section.

RAI-MH assessments are composed of approximately 300 data elements relating to health conditions, cognitive and behavioural data, physical functioning, medication use, nutritional status, special treatments and procedures, demographic information and other administrative information, such as admission and discharge information.

RAI-MH assessment information is typically captured using data collection software at participating OMHRS facilities. Such software is typically limited to data required for submission to CIHI for OMHRS. Data required for the OMHRS assessments can also be extracted from a more comprehensive clinical documentation system in use at the facility (i.e., an electronic health record).

Given the nature of OMHRS requirements, most episodes of care will be associated with multiple RAI-MH assessments. A RAI-MH full assessment is completed on each patient within 72 hours of admission. It is repeated on a quarterly basis at least every 92 days for longer-term patients, and/or after a significant change in clinical status. For lengths of stay less than 3 days, a short stay record is required, which includes a subset of RAI-MH and other administrative and clinical data elements, with all other data elements being optional. A RAI-MH discharge assessment is also required at the end of the inpatient episode, with a shorter discharge record being mandatory for sudden or unexpected discharges.

In instances when a patient is discharged from a designated mental health bed in one OMHRS facility in order to be admitted to a mental health bed in another OMHRS facility, it is necessary for a discharge assessment to be completed upon discharge from the first facility; the assessment process must be restarted in the second facility with an admission assessment.

In order to meet its standards for data collection across health care settings and populations and also to meet particular requests of the Ontario ministry, CIHI has included in OMHRS additional data elements over and above the RAI-MH instrument. These additional data elements are denoted with the prefix “X” in the column labelled “ID” in the appendix. All data elements collected for OMHRS, whether from or in addition to the RAI-MH instrument, are required for established purposes.

The rationale for the collection of data elements with an increased risk of direct or indirect identification of an individual is also provided in the appendix.

Examples of the types of information collected by the RAI-MH instrument appear below. A full list of data elements included in OMHRS can be found on CIHI’s website.
The OMHRS data elements in the Minimum Data Set–Mental Health (MDS-MH) are organized into the following sections:

- **Patient identifiers**: These are data elements used to identify individual records. Patient names are never collected for OMHRS.

- **Personal items**: These items capture basic demographic information about the person, such as sex, birthdate, marital status, language, education, sources of income and Aboriginal origin.

- **Referral items**: This section identifies circumstances surrounding the initial referral, such as admission date, reasons for admission, where the person was admitted from and who he or she lived with at the time of admission.

- **Mental health service history**: This section provides information about service utilization patterns — such as number of psychiatric admissions, contact with community mental health services and age at first hospitalization — that could be helpful for care planning and program planning.

- **Assessment information**: The information collected in this section relates to the medical/legal aspects of the person’s care, via data elements such as inpatient status, forensic status and police intervention.

- **Mental status**: Mental state indicators and insight into mental health are collected for assessing the outcomes of clinical interventions.

- **Substance use and excessive behaviours**: This section captures data on alcohol, drug and tobacco use, gambling behaviours and withdrawal symptoms that can be used for early detection of and intervention with addictions.

- **Harm to self and others**: This section tracks safety and security information, including self-injury and violence, which is vital to the initial and subsequent care plans for the person.

- **Behaviour disturbance**: The assessment elements in this section capture information on behaviours that pose a potential risk to self or others and/or that tend to be socially inappropriate.

- **Cognition**: This section assesses the person’s abilities to think coherently and to remember and organize thoughts into actions. This information can significantly contribute to the development of a care plan, including the discharge plan.

- **Self-care**: Data is collected on activities/instrumental activities of daily living and stamina that may relate to some mental illnesses or cognitive deficits, as well as side effects of medications and other treatments that contribute to needless loss of self-sufficiency.

- **Communication/vision patterns**: This section identifies communication impairments — such as hearing, vision and making self understood during a person’s psychiatric stay — that will facilitate the development of necessary adaptions during the person’s stay in hospital.
• **Health conditions and possible medication side effects:** Physical health issues and diagnoses (e.g., skin and/or foot problems, pain, bladder/bowel continence) are captured in this section. Close attention to physical health concerns is warranted to ensure the person is assessed holistically and to find and treat physical issues that may be contributing to the person’s mental health deterioration.

• **Stressors:** This section captures events in a person’s life (e.g., parental abuse of alcohol or drugs) that have potentially life-altering characteristics which play a large role in patterns of psychological and social development and coping.

• **Medications:** The person’s medication history is provided in this section to facilitate appropriate plans of care.

• **Service utilization/treatments:** This section collects information on the professional health care and interventions (e.g., nursing interventions, electroconvulsive therapy) received in the period before the assessment.

• **Control procedures/observation:** The procedures such as physical restraint by staff and confinement, as well as levels of observation that have been utilized for the management of safety and security concerns, are captured in this section.

• **Nutrition:** This section collects information on the person’s nutritional status (e.g., height and weight, nutritional problems, eating disorders), which is an important consideration in care planning.

• **Role functioning and social relations:** This section captures information about the life of the person that defines him or her socially, such as family roles and social relationships.

• **Resources for discharge:** This section assesses resources currently available to the person upon discharge. This includes the informal support system (e.g., family and friends) potentially available to the person, discharge readiness and living arrangements.

• **Psychiatric diagnostic information:** The person’s applicable mental health diagnoses, as determined by the attending psychiatrist, are recorded in this section.

• **Service history:** The items in this section report details related to the person’s stay in hospital (e.g., whether the person was admitted through the emergency department, the discharge date, time spent away from the mental health bed, time spent in an alternate level of care).

Since the OMHRS database is structured to reflect the different service events that patients experience over time, various assessment records are submitted for individual patients related to each episode of care. A picture of the patients, their clinical and demographic characteristics, their use of resources and their outcomes can be developed over time. This enables accurate and timely cross-sectional analysis of patients even prior to their discharge from the designated mental health bed. Capturing similar information at multiple points in time also enables measurement of change, which is the basis for analysis of outcomes and many indicators of quality. CIHI uses such data for statistical reporting purposes only.
Information is also collected on hospital characteristics — type, size and location — to provide contextual information for analysis of quality and utilization data.

While there have been no major or substantial changes to OMHRS since the last PIA was conducted in 2011, the data set has been modified to capture the following information:

- Replaced the DSM-IV-TR classification system with DSM-5;
- Added new data elements to capture admission via emergency department in response to requests from the Ontario ministry;
- Modified a number of data elements to further align with the interRAI MH instrument, which is a subsequent version of the RAI-MH;
- Removed data elements for service interruption start and end dates;
- Added a new data element to capture service interruption in the previous fiscal year; and
- Added a new data element to indicate the patient’s forensic status.

### 2.4 Data flow and access management

Mandated hospitals in Ontario and participating facilities from Newfoundland and Labrador and Manitoba submit data to OMHRS through CIHI’s secure web-based electronic Data Submission Services (eDSS).

External access to CIHI’s secure applications such as eDSS, as well as applications CIHI uses to deliver reports and data to external clients, is subject to CIHI’s role-based access management process managed by CIHI’s Central Client Services. CIHI’s Central Client Services manages access to CIHI’s secure applications, using established Access Management System processes for granting and revoking access. Once authenticated, users can log in to CIHI’s secure website with access applications and services provided by CIHI.

Once received by CIHI via eDSS, OMHRS data files are immediately processed and the jurisdiction-issued health care number in each file is encrypted before files are transferred to CIHI’s SAS analytical environment.

For CIHI use, and to prepare data for purposes of return of own data or disclosure, authorized CIHI analytical staff access OMHRS data via CIHI’s SAS analytical environment. Staff access to the SAS analytical environment is provided through CIHI’s centralized SAS Data Access process. The process ensures that all requests for access to OMHRS data are traceable and authorized. The SAS Data Access system is subject to an annual audit to ensure that staff are accessing data on a need-to-know basis.
CIHI returns OMHRS data to the hospital that originally supplied the data, as well as to the respective ministry of health. CIHI also discloses facility-identifiable aggregate OMHRS data to the data provider community (in the form of comparative reports), aggregate and de-identified record-level data to third-party requestors, and aggregate data to the public.

Sections 3.5 and 3.6 include a more detailed discussion of how data flows into and out of OMHRS, as well as a description of the various procedural and technical measures deployed to prevent unauthorized access and otherwise secure the data. The following figure illustrates the data flows at a high level.

**Figure**  OMHRS data flow

**Input**

- Ontario facilities with designated adult mental health beds
- Facilities outside Ontario (inpatient mental health beds)

**Output**

- *Use by CIHI*
  - Data management, data quality, linkage and analysis.

- *Return of own data*
  - Submitting facility (source of data) and respective ministry of health
  - CIHI returns aggregate and record-level data, as well as reports focused on data submissions, data quality, health system management and comparative indicators.

- *Disclosures*
  - Data provider community
    - Comparative reports containing aggregate data, including facility-identifiable data.
  - University of Waterloo under agreement
    - Record-level de-identified data for all submitting facilities (annually).
  - Third-party data requests
    - CIHI responds to requests for record-level de-identified and aggregate data.
  - Public release of OMHRS data
    - Aggregate statistics and analyses are made available in publications and on CIHI’s website.
3 Privacy analysis

3.1 Privacy and Security Risk Management Program

Privacy and security risk management (PSRM) is a formal, repeatable process for identifying, assessing, treating and monitoring risks in order to minimize the probability of such risks materializing and/or their impact, should they occur. In 2015, CIHI approved its Privacy and Security Risk Management Framework and implemented the associated Policy on Privacy and Security Risk Management. CIHI’s chief privacy officer and chief information security officer, in collaboration with senior managers, are responsible for identifying, assessing, treating and monitoring and reviewing risk privacy and security risks.

Privacy and security risks may be identified from a variety of sources, including PIAs, for example. 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 ranking indicates a more serious threat and a greater imperative for treatment. Once an initial risk treatment is applied, the residual risk (the new calculation of the likelihood and impact of the risk, given the treatment) is assessed and compared against CIHI’s privacy and security risk tolerance statement, which indicates that CIHI’s privacy and security risk tolerance is low. If the risk score for the residual risk is still greater than low, additional risk treatment is necessary until the risk is low or the untreated/residual risk is accepted by CIHI’s Senior Management Committee on behalf of the corporation.
3.2 Authorities governing OMHRS data

General

OMHRS 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 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.

The following provinces and territories have enacted health information–specific privacy legislation: Alberta, Saskatchewan, Manitoba, Ontario, New Brunswick, Nova Scotia, Newfoundland and Labrador, the Northwest Territories and Yukon (Prince Edward Island is 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.
3.3 Principle 1: Accountability for personal health information

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

Organization and governance

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

<table>
<thead>
<tr>
<th>Table</th>
<th>Responsibility for OMHRS data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Position/group</td>
<td>Roles/responsibilities</td>
</tr>
<tr>
<td>Vice president, Programs</td>
<td>Responsible for providing overall leadership and oversight regarding the acquisition, management and reporting of OMHRS data</td>
</tr>
<tr>
<td>Director, Methodologies and Specialized Care</td>
<td>Responsible for operational and strategic decisions regarding OMHRS data</td>
</tr>
<tr>
<td>Manager, Rehabilitation and Mental Health</td>
<td>Responsible for ongoing management of OMHRS 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 OMHRS data</td>
</tr>
</tbody>
</table>
3.4 Principle 2: Identifying purposes for personal health information

OMHRS will collect personal health information, including patient identifiers in the form of the jurisdiction-assigned health care numbers, in order to facilitate linkage of person-level data across data holdings and time. Collection of patient identifiers, for example, enables CIHI to add (i.e., link) OMHRS information to information that it already holds about a patient’s contact with the health care system (e.g., hospital stay data collected in the DAD and National Ambulatory Care Reporting System [NACRS]).

The data in OMHRS is used to produce accurate, timely and comparable statistical information about inpatient mental health care provided by participating hospitals.

OMHRS data is used to produce a variety of outputs to support

- Provincial accountability, through reporting of comparable health indicators of access, outcomes and service utilization;
- Inpatient adult mental health programs, facility- and system-level strategic and operational management, benchmarking and quality improvement; and
- Clinical and policy research and analyses.

Moreover, OMHRS is designed to

- Provide management decision-makers and front-line service providers with accurate and timely information on the characteristics of their patient population, service utilization and outcomes;
- Create a repository of comparable clinical and administrative data, collected as a by-product of an improved, standardized process of care;
- Provide hospitals with the opportunity to participate in provincial reporting of comparable indicators for inpatient mental health services;
- Support quality of care analyses and research and benchmarking for best practices in inpatient mental health services;
- Provide technical infrastructure to support knowledge transfer initiatives for education and client support activities; and
- Foster communities of practice among OMHRS stakeholders to support utilization of data and promote best practices.
3.5 Principle 3: Consent for the collection, use or disclosure of personal health information

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

3.6 Principle 4: Limiting collection of personal health information

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

The Ontario ministry and the Ontario Hospital Association, in collaboration with interRAI, conducted pilot projects with selected hospitals to determine the data elements that should be included in the original version of the RAI-MH. As a result of this pilot work, the subsequent version of the RAI-MH that is included in OMHRS has fewer data elements than the original version. The RAI-MH data elements submitted to CIHI for OMHRS can be used for one of several purposes, including outcome scales, quality indicators, case-mix grouping methodologies or assessment protocols. All of these applications are considered part of a comprehensive RAI-MH implementation. Necessary changes are made in OMHRS over time to improve data quality, to align with revised interRAI instrument standards and to adhere to Ontario ministry and CIHI requirements and needs.

In most cases, an attempt is made to collect all required information about each patient. Some components of the data set are considered optional (e.g., medication record). A facility may choose not to submit optional components of the OMHRS data set, depending on the hospital’s practices or policies. In the case of short-stay admissions, staff members may not have access to all information required to complete some RAI-MH items prior to the patient’s discharge (e.g., the family may not be able to provide information on the patient’s customary routine). In these instances, as much information as can be reasonably obtained is collected and submitted to CIHI. OMHRS does not contain patients’ names or home addresses.
The data in OMHRS is also limited to inpatient hospital events. It does not include mental health data from outpatient or community-based services, residential care facilities, centres for the care of individuals with intellectual disabilities, group homes or private practitioners. Collection and submission of OMHRS data under the Ontario ministry mandate applies only to inpatient mental health services provided to patients in beds designated for that purpose by the Ontario ministry.

Data specifications and other associated documentation, such as file layouts, are available from CIHI. All OMHRS submissions to CIHI must conform to its submission and edit specifications.

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

Limiting use

CIHI limits the use of data in OMHRS to the authorized purposes described in Section 3.4. 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.

Since 2009, data sets used for the purpose of internal CIHI analysis do not contain direct identifiers, such as unencrypted health care numbers. Health care numbers in an unencrypted form are available to CIHI staff on an exceptional, need-to-know basis only, subject to approval processes as set out in CIHI’s internal Privacy Policy and Procedures, 2010.

Data linkage

Data linkages are performed between OMHRS 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.

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. When carrying out data linkages, CIHI will generally do so using consistently encrypted health care numbers. The linked data remains subject to the use and disclosure provisions in the Privacy Policy, 2010.
Criteria for approval of data linkages are set out in sections 23 and 24 of CIHI’s Privacy Policy, 2010, as follows:

1. The individuals whose personal health information is used for data linkage have consented to the data linkage; or

2. All of the following criteria are met:
   a. The purpose of the data linkage is consistent with CIHI’s mandate;
   b. The public benefits of the linkage significantly offset any risks to the privacy of individuals;
   c. The results of the data linkage will not be used for any purpose that would be detrimental to the individuals that the personal health information concerns;
   d. The data linkage is for a time-limited specific project and the linked data will be subsequently destroyed in a manner consistent with sections 28 and 29; or
   e. The data linkage is for purposes of an approved CIHI ongoing program of work where the linked data will be retained for as long as necessary to meet the identified purposes and, when no longer required, will be destroyed in a manner consistent with sections 28 and 29; and
   f. The data linkage has demonstrable savings over other alternatives or is the only practical alternative.

Client linkage standard

In 2015, CIHI implemented a corporate-wide client linkage standard to be used for the linkage of records created in 2010–2011 or later, where the records include the following data elements: encrypted health care number, the province/territory that issued the health care number, and year of birth. For the linkage of records that do not satisfy these criteria, the linkage mechanism is determined on a case-by-case basis.

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.

Through CIHI’s restricted web-based services, reports are accessible to authorized users from the submitting facility and the associated ministry of health. Access to restricted web-based services for return of own data is provided by CIHI’s Central Client Services using established Access Management System processes. The types of reports that are accessible include the following:

Submission Reports: Error and Verification reports are accessible. Verification reports allow users to determine whether their data submission was successfully accepted by CIHI, either for individual records or for a group of records within an assessment date range specified by the user. Error reports provide summary characteristics about the submission (e.g., how many records the facility has successfully submitted to OMHRS), and indicate which files or records were not submitted successfully and the reason why (e.g., the records were missing information). The reports permit the facility to correct errors in the records and resubmit them. In order to identify the rejected records, the reports refer to the Chart Number that the facility assigns to each patient, the Case Record Number, which is a registration number assigned to a person for each admission to the facility, and Record ID, which is a number assigned by the facility to identify a record uniquely across all submissions from the facility. Health care numbers are not used to identify records in reports.

System for Classification of In-Patient Psychiatry (SCIPP) Weighted Patient Day Reports: Using the SCIPP grouping methodology, a facility’s assessments are categorized into specific groups based on similar clinical and resource utilization characteristics, and reports provide an estimate, or sample, of the resources used by each group, which can be used for planning, resource allocation, data quality and funding purposes. These reports are currently available for facilities in Ontario only, for methodological reasons.

---

ii. Canadian Institute for Health Information. SCIPP Grouping and Weighting Methodology. September 2016.
Comparative Reports: Aggregate data (small cell sizes may be present) on resource utilization, patient characteristics, clinical outcomes, service utilization and quality indicators is presented for the submitting facility, along with comparative information at the peer group (information from similar facilities grouped together), region (i.e., local health integration network for Ontario facilities) and province/territory levels.

Data Quality Reports: These reports contain record-level and aggregate data (small cell sizes may be present) summarizing data quality issues with a facility’s data.

Upon request, CIHI will also provide a facility with a copy of any data the facility submitted to OMHRS, as a return of own data. In addition to returning data to submitting facilities, CIHI may return records to the relevant ministry of health for data quality purposes and for purposes consistent with its mandate (e.g., for health services and population health management, including planning, evaluation and resource allocation). Record-level data for all Ontario facilities submitting to OMHRS is returned to the Ontario ministry on a regularly scheduled basis.

Limiting disclosure

Disclosures to data provider community

Via restricted web-based services, CIHI makes comparative reports containing facility-identifiable aggregate OMHRS information available to the data provider community. Access to restricted web-based services used for disclosures to the data provider community is provided by CIHI’s Central Client Services using established Access Management System processes. Facilities that submit data to OMHRS, ministries of health and regional health authorities access comparative reports that include the following:

- Information on resource utilization, patient characteristics, clinical outcomes, service utilization and quality indicators compared across facilities; and
- Comparisons of selected RAI-MH indicators across OMHRS-participating facilities in Ontario. The indicators are designed to support patient care planning and outcome measurement, as well as planning, management and quality improvements.

Steps have been taken to ensure that identification of individuals in the facility-identifiable reports does not occur per CIHI standard practices for avoiding identifiability and residual disclosure (e.g., suppression of units of observation less than 5, other than when aggregate data presented constitutes a return of own data).

Depending on the information requirements of the specific user group, aggregate data may be reported at a facility, peer group (information from similar facilities grouped together), region (i.e., local health integration network for Ontario facilities) and/or province/territory level.
Note that reports to the Ontario ministry do not include data from the facilities in Manitoba and Newfoundland and Labrador currently reporting data to OMHRS. However, for comparative purposes, Ontario data aggregated to the province level is present in the comparative reports available to Manitoba and Newfoundland and Labrador.

Before being able to access comparative reports, organizations must sign a service agreement with CIHI. The service agreement is signed at a senior level of the organization to ensure that the organization is aware of both its responsibilities and those of its users. The service agreement sets out terms and conditions for use and subsequent disclosure of data.

Once a service agreement has been signed, a request for individual access to comparative reports is made to CIHI’s Central Client Services team, which

- Verifies that the user is affiliated with the organization;
- Verifies, through the organization contact, that the requestor is a designated user and the level of access associated with the designated user’s profile; and
- Grants the designated user the appropriate level of access.

Each time a designated user logs on to access comparative reports, the user must reconfirm acceptance of the terms of use imposed under the service agreement.

**Disclosure to interRAI University of Waterloo under agreement**

Upon specific direction of the Ontario ministry and related in part to the nature of the Non-Core Services Agreement between CIHI and the Ontario ministry, under separate agreement, CIHI provides to interRAI University of Waterloo, on an annual basis, de-identified record-level OMHRS data from all reporting facilities in Ontario, Manitoba and Newfoundland and Labrador. The separate agreement between CIHI and interRAI University of Waterloo includes provisions requiring interRAI University of Waterloo to secure and maintain the confidentiality of the data at all times and expressly prohibits any attempts to re-identify individuals.

**Third-party data requests**

Customized de-identified record-level and/or aggregate data from OMHRS 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.

OMHRS is used to respond to data requests from third parties. 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 order to ensure that consistent processes are used for the de-identification of data.

In 2009, CIHI adopted a complete life cycle approach to data management. As part of that lifecycle, 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.

**Public release of OMHRS 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.
Limiting retention

OMHRS forms part of CIHI’s data holdings and, consistent with its mandate and core functions, CIHI retains such information for as long as necessary to meet the identified purposes.

3.8 Principle 6: Accuracy of personal health information

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

Similar to other CIHI data holdings, OMHRS is subject to a data quality assessment on a regular basis, based on CIHI’s Data Quality Framework.

3.9 Principle 7: Safeguards for personal health information

CIHI’s Privacy and Security Framework

CIHI has developed a Privacy and Security Framework to provide a comprehensive approach to privacy and security management. Based on best practices from across the public, private and health sectors, the framework is designed to coordinate CIHI’s privacy and security policies and provide an integrated view of the organization’s information management practices. Key aspects of CIHI’s system security with respect to OMHRS data are highlighted below.

System security

CIHI recognizes that information is secure only if it is secure throughout its entire life cycle: creation and collection, access, retention and storage, use, disclosure and 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.
3.10 Principle 8: Openness about the management of personal health information

CIHI makes information available about its privacy policies, data practices and programs relating to the management of personal health information. Specifically, CIHI’s Privacy and Security Framework and Privacy Policy, 2010 are available on www.cihi.ca.

3.11 Principle 9: Individual access to, and amendment of, personal health information

Personal health information held by CIHI is not used by CIHI to make any administrative or personal decisions affecting individuals. Requests from individuals seeking access to their personal health information will be processed in accordance with sections 60 to 63 of CIHI’s Privacy Policy, 2010.

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

As set out in sections 64 and 65 of CIHI’s Privacy Policy, 2010, complaints about CIHI’s handling of information are investigated by the chief privacy officer, who may direct an inquiry or complaint to the privacy commissioner of the jurisdiction of the person making the inquiry or complaint.

4 Conclusion

CIHI’s assessment of OMHRS did not identify any privacy risks. This PIA will be updated or renewed in compliance with CIHI’s Privacy Impact Assessment Policy.
Appendix

The table below describes personal identifiers and other data elements that could present an increased risk of direct or indirect identification of an individual. It also gives the definition and rationale for collection of each data element, and specifies when collection of each data element takes place.

Note: Elements are from the Resident Assessment Instrument–Mental Health (RAI-MH), Government of Ontario, Ontario Hospital Association and interRAI. CIHI has included in OMHRS additional data elements over and above those in the RAI-MH instrument. These additional data elements are denoted with the prefix “X” in the ID column.

<table>
<thead>
<tr>
<th>ID</th>
<th>Data element</th>
<th>When collected</th>
<th>Purpose/rationale/comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>AA2</td>
<td>Health Card Number (HCN)</td>
<td>Mandatory: Admission</td>
<td>Since it allows identification of individuals, particularly across facilities, health care facilities use it as the principal identifier. However, not all patients have a valid provincial/territorial health card number, and these patients are coded as “-70” if unknown or “-90” if not applicable. If available, it can be used to link individuals’ episodes of care across multiple organizations and potentially across the continuum of care. CIHI never releases unencrypted HCNs except when • Data is being requested by the original provider or the ministry; • Consent has been obtained; or • An act requires (or an agreement permits) disclosure.</td>
</tr>
<tr>
<td></td>
<td>Number (HCN)</td>
<td>Record</td>
<td></td>
</tr>
<tr>
<td>X30</td>
<td>Chart Number (CN)</td>
<td>Mandatory: All Records</td>
<td>The Chart Number is a unique number assigned to a patient by the facility and is not the same as the individual’s provincial/territorial health card number. It is required to differentiate an individual within a given facility. The CN for a person remains unchanged with multiple admissions, readmissions and discharges within a given facility.</td>
</tr>
<tr>
<td>AA3</td>
<td>Case Record Number (CRN)</td>
<td>Mandatory: All Records</td>
<td>The Case Record Number is a unique admitting number assigned to patients by the facility upon admission. It cannot identify an individual on its own.</td>
</tr>
</tbody>
</table>

iii. The data element Health Card Number used in OMHRS documentation is referred to as “health care number” elsewhere in this PIA.
<table>
<thead>
<tr>
<th>ID</th>
<th>Data element</th>
<th>When collected</th>
<th>Purpose/rationale/comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>BB1</td>
<td>Sex</td>
<td>Mandatory: Admission and Short Stay Records</td>
<td>Coded Male, Female, or Other. It is used to produce key analyses of utilization, health status and outcomes by sex, and for age and sex standardization.</td>
</tr>
<tr>
<td>BB2</td>
<td>Birth Date</td>
<td>Mandatory: Admission and Short Stay Records</td>
<td>Birth Date is used to calculate age, which is required for analysis of indicators by both age and age and sex standardization. CIHI does not typically release full date of birth in response to an external data request. Either the date is truncated to include only the year of birth, or an exact age/age grouping is derived and released instead.</td>
</tr>
<tr>
<td>BB4</td>
<td>Primary Language</td>
<td>Optional: Short Stay Record (MDS-MH Assessment)</td>
<td>This data element can be used to identify patients potentially underserved due to inability to speak one of Canada's official languages or due to cultural differences. The list of possible languages that can be coded is large, which is likely to result in small numbers of clients being coded to less frequently spoken languages. For external data requests, all languages other than English and French are typically categorized as “Other.”</td>
</tr>
<tr>
<td>X50</td>
<td>Responsibility for Payment</td>
<td>Mandatory: Admission and Short Stay Records</td>
<td>The coding option &quot;First Nations and Inuit Health Branch (FNIHB)&quot; for this data element can potentially be used to identify patients’ Aboriginal status.</td>
</tr>
<tr>
<td>BB7</td>
<td>Aboriginal Origin</td>
<td>Mandatory: Admission and Short Stay Record (MDS-MH Assessment)</td>
<td>Required for aggregate analysis of health status outcomes for a vulnerable population. There is considerable research to indicate that Aboriginal populations are at risk for particular diseases, illnesses and injuries. Both Health Canada and Statistics Canada collect information on Aboriginal origin for a variety of purposes. The RAI-MH clinical assessment requires that the clinician ask the client or family whether the client identifies himself or herself as a member of an Aboriginal community (Inuit, Métis or North American Indian). This data element was aligned with a Health Canada definition in 2002 in collaboration with interRAI. The understanding of various populations is critical to providing appropriate access and service quality; it is particularly important in order to understand and meet the needs of vulnerable populations. It will allow for the analyses of health and functional status, access to services, and health outcomes across populations.</td>
</tr>
</tbody>
</table>
| ID  | Data element          | When collected                                      | Purpose/rationale/comments                                                                                                                                                                                                。
|-----|-----------------------|-----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
| BB7 (cont’d) | Aboriginal Origin    | Mandatory: Admission Record                          | that have unique health needs. It will be critical in the development of valid, comparable indicators, which support quality improvement initiatives.                                                                                                               |
|     |                       | Optional: Short Stay Record (MDS-MH Assessment)     |                                                                                               |
| X60 | Postal Code           | Mandatory: Admission and Short Stay Records          | The postal code of the patient’s prior primary residence is coded by all 6 characters, or by the first 3 characters if the full code is unknown, or “-70” if the postal code is entirely unknown, or “-90” if the element is not applicable (i.e., the patient is not a resident of Canada). The prior primary residence may be the patient’s home or another residential facility, such as a nursing home. In Ontario, the postal code is used to assign patients to health regions, otherwise known as local health integration networks (LHINs), in order to report LHIN-specific access, utilization and outcome indicators used for planning purposes and population health initiatives. Geographic boundaries of LHINs are not necessarily static but change with time and health system restructuring. CIHI needs the postal code as one constant, unique geographic variable to be able to validate that the health data belongs within a specific location. Postal Code can be linked to Standard Geographic Regions using Statistics Canada’s Postal Code Conversion File. These Standard Geographic Regions can then be linked to health regions using Statistics Canada’s Health Region to Census Geography correspondence files. Census geography does not recognize LHIN boundaries (and vice versa), and neither geographical system neatly falls into Canada Post’s assignment of postal codes to mailing addresses. Correspondence files provide the linkage between these geographic units and require all 6 characters of the postal codes for accurate mapping. Using Forward Sortation Area (FSA), or the first 3 digits of the postal code, to map to a LHIN does not always produce a 100% match. The FSA is too large a geographic unit to facilitate reliable and precise mapping to a LHIN. Therefore, data integrity depends upon the availability of the full 6-digit postal code. |

---

iv. Statistics Canada has established these “correspondence files” as a standard way to convert postal code information to an appropriate geographical region across Canada that suits the requirements of data users. It could be, for example, the geographical expanse of a regional health authority in British Columbia.
<table>
<thead>
<tr>
<th>ID</th>
<th>Data element</th>
<th>When collected</th>
<th>Purpose/rationale/comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>X60 (cont’d)</td>
<td>Postal Code</td>
<td>Mandatory: Admission and Short Stay Records</td>
<td>Although all 6 digits of the postal code are required for accurate mapping to LHINs, data released by CIHI in response to external data requests is limited to geographic identifiers smaller than FSAs or equivalent to them, such as large Census Subdivisions and LHINs, which are mapped from the postal codes.</td>
</tr>
<tr>
<td>AA4</td>
<td>Facility Number</td>
<td>Mandatory: All Records</td>
<td>Used to uniquely identify facilities for analysis and reporting purposes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Note:</strong> OMHRS psychiatric specialty hospitals on average have length of stays (LOS) that are longer than OMHRS general hospitals, and in some cases the LOS can exceed 10 years.</td>
</tr>
</tbody>
</table>