Trauma Registries Privacy Impact Assessment, December 2012
Our Vision
Better data. Better decisions.
Healthier Canadians.

Our Mandate
To lead the development and maintenance of comprehensive and integrated health information that enables sound policy and effective health system management that improve health and health care.

Our Values
Respect, Integrity, Collaboration, Excellence, Innovation
CIHI is pleased to publish the following Privacy Impact Assessment pursuant to its Privacy Impact Assessment Policy:

Trauma Registries
Privacy Impact Assessment

Approved by:

Jean-Marie Berthelot
Vice President, Programs

Anne-Mari Phillips
Chief Privacy Officer & General Counsel

Ottawa – January 2013
Ten Quick Facts About the Trauma Registries

1. The Ontario Trauma Registry (OTR) was created in 1992 with funding from the Ontario Ministry of Health and Long-Term Care (MOHLTC).

2. The MOHLTC set up a contract with the Canadian Institute for Health Information (CIHI) to manage the OTR.

3. The multidisciplinary Trauma Registry Advisory Committee (TRAC) provides guidance to the MOHLTC about the OTR.

4. The National Trauma Registry (NTR) was established in 1997.

5. The National Trauma Registry Advisory Committee (NTRAC) plays a pivotal role in the development and maintenance of the NTR by providing advice on its goals and objectives, potential uses of the data, definitions, inclusion/exclusion criteria, data quality issues, report formats and development of promotional strategies.

6. The submission of data to the NTR Comprehensive Data Set (CDS) is a requirement for trauma centre accreditation with the Trauma Association of Canada.

7. The data collected for the trauma registries includes demographic information, administrative information (for example, pre-admission information, ambulance transfers and circumstances of injury), clinical information (for example, diagnoses and procedures) and patient outcomes information.

8. The trauma registries do not capture the names of patients or their addresses (that is, street number and street name) from any source.

9. The OTR CDS contains approximately 200 data elements. As of 2012–2013, the NTR CDS contains 87 data elements.

10. The OTR MDS and NTR CDS are sourced from an existing CIHI data holding: the Discharge Abstract Database–Hospital Morbidity Database.
1 Introduction

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

The purpose of this privacy impact assessment (PIA) is to examine the privacy, confidentiality and security risks associated with the National Trauma Registry (NTR) and the Ontario Trauma Registry (OTR), collectively referred to as the trauma registries. It 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 they apply to the registries.

This PIA updates the NTR PIA completed in 2005. The primary driver for this PIA is compliance with CIHI’s Privacy Impact Assessment Policy.

2 CIHI’s Trauma Registries

CIHI is mandated to coordinate the development and maintenance of a comprehensive and integrated health information system for Canada. Inherent in that mandate is a responsibility to provide and coordinate the provision of accurate and timely information necessary to establish sound health policies, manage the Canadian health system effectively and generate public awareness of factors affecting good health.

The trauma registries are managed by CIHI’s Primary Health Care Information and Clinical Registries branch, which maintains five separate trauma data holdings:

1. National Trauma Registry Comprehensive Data Set;
2. National Trauma Registry Minimum Data Set;
3. Ontario Trauma Registry Comprehensive Data Set;
4. Ontario Trauma Registry Death Data Set; and
5. Ontario Trauma Registry Minimum Data Set.

While similarities exist between the NTR and OTR, there are some differences. Each registry was examined as part of this PIA.
2.1 Background

The OTR was created in 1992 with funding from the Ontario Ministry of Health and Long-Term Care (MOHLTC). The NTR was created in 1997. The data contained in the trauma registries is used by trauma health care providers, researchers and injury prevention programs to quantify trauma, to educate Canadians about trauma and its consequences, and to provide a framework for trauma prevention. The submission of data to the NTR Comprehensive Data Set is a requirement for trauma centre accreditation with the Trauma Association of Canada.

The overall goals of the trauma registries are to

- Contribute to the reduction of injuries and related deaths;
- Facilitate provincial and international injury comparisons; and
- Increase awareness of injury as a public health challenge in Canada and support injury-related research.

Ontario Trauma Registry

The OTR contains data on patients hospitalized or killed due to major trauma in Ontario. It is made up of three distinct data sets: the Comprehensive Data Set (CDS), the Death Data Set (DDS) and the Minimum Data Set (MDS).

Ontario Trauma Registry Comprehensive Data Set

The OTR CDS contains information on severely injured patients who were hospitalized or who died in the emergency department in Ontario’s lead trauma hospitals.\(^1\) It contains approximately 200 data elements and includes information on medical exams (that is, vital signs, computed tomography scans and operating room information), physician services, special care units and whether the trauma team was activated, among other items. On average, about 4,000 new cases are added to the OTR CDS every year. In 2012, the definitions of some of the existing data elements in the OTR CDS were standardized; these new definitions are primarily clinical in nature.

Ontario Trauma Registry Death Data Set

The OTR DDS contains records on all deceased victims of trauma; data is collected by the Office of the Chief Coroner of Ontario upon completion of its investigations. The first data set was received in 1993; the OTR DDS is updated intermittently as data becomes available. Currently, the OTR DDS contains 22 years of data (1986 to 2007).

---

\(^1\) Tertiary care (or Level 1) hospitals, designated by the MOHLTC to provide severely injured trauma victims with a high level of care, including coordination with pre-hospital care and transport systems (both land and air ambulance services), the provision of in-hospital treatment, and stabilization and discharge from hospital to community rehabilitation. Lead trauma hospitals are also known as regional trauma centres.
Ontario Trauma Registry Minimum Data Set

The OTR MDS is sourced from an existing CIHI data holding—the Discharge Abstract Database–Hospital Morbidity Database (DAD-HMDB)—and, as such, is covered under the PIA for that database. It is created, as needed, by extracting Ontario cases from the DAD-HMDB that meet the trauma registries’ definition of trauma.

National Trauma Registry

The NTR was established in 1997 and contains data on patients hospitalized due to major trauma in Canada. It is made up of two distinct data sets: the Comprehensive Data Set (CDS) and the Minimum Data Set (MDS).

National Trauma Registry Comprehensive Data Set

The NTR CDS contains data on a subset of severely injured patients submitted to CIHI by provincial trauma registries in five provinces (British Columbia, Alberta, Quebec, Nova Scotia and Newfoundland and Labrador) and by individual hospitals in three provinces (Saskatchewan, Manitoba and New Brunswick). Data is collected on trauma patients with an Injury Severity Score greater than 12.

The NTR CDS was revised in 2011–2012 to include additional data elements, to standardize the definitions across the provinces and to be more consistent with international standards. As of 2012–2013, the NTR CDS contains 87 data elements. These new data elements are primarily clinical in nature and do not include any unique personal identifiers.

The number of cases added to the NTR CDS annually varies depending on the number of participating provincial registries or individual hospitals. At the time of the 2005 PIA, the number of new cases ranged from 6,400 to 9,313 annually. Since then, the number of participating provinces and hospitals has increased, and there are currently, on average, 14,000 new cases added every year.

CIHI’s 2005 PIA mentioned that the NTR was to be enhanced with a Death Data Set (DDS). This statement reflected an announcement, at the time, of the intent to develop a national Canadian Coroners’ and Medical Examiners’ Database (CCMED). However, the enhancement of the NTR has been delayed because the CCMED is still being developed.

---

ii. A provincial trauma registry contains data from multiple hospitals.

iii. New Brunswick has developed its own provincial trauma registry. It is expected to start submitting data to the NTR CDS in 2012–2013.

iv. The Injury Severity Score is an international scoring system that was created to allow the severity of injury to be calculated in a consistent way, which allows for international comparability.
National Trauma Registry Minimum Data Set

The NTR MDS is sourced from the DAD-HMDB. It is created annually by extracting cases that have an International Classification of Diseases (ICD)\textsuperscript{v} external cause of injury code that is included in the trauma registries’ definition of trauma.

Approximately 15,000 cases are extracted annually. The NTR MDS currently includes 260 data elements and contains data back to 1994–1995.

2.2 Description of Trauma Registries Data/Data Collection, Data Storage and Overview of Data Flow

Description of Trauma Registries Data

The data collected includes demographic information, administrative information (for example, pre-admission information, ambulance transfers and circumstances of injury), clinical information (for example, diagnoses and procedures) and patient outcomes information.

The following are examples of the common data elements collected by the OTR and NTR that are considered privacy-sensitive. For data element definitions, please refer to the NTR CDS Data Dictionary, the OTR CDS metadata documentation and the DAD documentation.

<table>
<thead>
<tr>
<th>Data Element and Description</th>
<th>OTR CDS</th>
<th>OTR DDS</th>
<th>NTR CDS</th>
<th>NTR MDS</th>
<th>Notes/Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trauma Number: This number uniquely identifies a case within an institution and is retained for quality assurance processing.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Unique personal identifier (usually Health Card Number): Participating trauma hospitals typically submit unencrypted (original) health card numbers (HCNs) to the NTR and OTR to uniquely identify records or cases and to allow linkages to be made.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Some jurisdictions, such as Manitoba and Quebec, encrypt HCNs prior to submission to CIHI.</td>
</tr>
<tr>
<td>Patient Age: This element is required to identify, quantify and analyze differences in injury hospitalizations by age or age group.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>In the NTR CDS, for Quebec cases where the individual is older than 85, age is given as the median of the 85+ age group.</td>
</tr>
<tr>
<td>Patient Sex: This element is required to identify, quantify and analyze differences in injury hospitalizations by sex.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Patient Postal Code: Postal codes are used to support regional reporting and analysis of injury patterns or trends in particular geographic areas.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Quebec provides only the first three digits of the postal code.</td>
</tr>
<tr>
<td>Regional Identifier of Incident Location: This geographic information is required to support analyses of injury patterns, including where injuries occur, rather than where the injured persons reside. This data element helps to inform public health policies.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

\textsuperscript{v} The ICD is a World Health Organization initiative that classifies morbidity and mortality information for statistical purposes, for the indexing of hospital records by diseases and operations, and for the appropriate storage and retrieval of data.
### Data Collection, Data Storage and Overview of Data Flow

All of the trauma registries’ data is electronically captured from facilities using specialized software and is submitted to CIHI through its secure, web-based electronic Data Submission Services (eDSS). With the exception of that for the NTR MDS, data is supplied to CIHI on a monthly basis. The NTR MDS is created annually by CIHI’s Information Technology and Services (ITS) operations staff by extracting selected DAD-HMDB records. Similar to the NTR CDS and OTR CDS, cases selected for inclusion in the NTR MDS are those with an ICD external cause of injury code that is included in the trauma registries’ definition of trauma.

Data is received either directly from a data provider or indirectly from an existing CIHI data holding (such as the DAD-HMDB) that sources a registry. Once in CIHI’s possession, data is processed and validated (that is, run through edit checks) on central data servers. Prior to loading or extracting data onto the NTR/OTR servers, where it will be used and accessed for internal and external reporting and analysis, CIHI applies various formulas to the data to make it meaningful for analysis.

The following figures present an overview of the data flow for the trauma registries.

---

<table>
<thead>
<tr>
<th>Data Element and Description</th>
<th>OTR CDS</th>
<th>OTR DDS</th>
<th>NTR CDS</th>
<th>NTR MDS</th>
<th>Notes/Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Injury Date:</strong> Occurrence of injuries (numbers and types) varies substantially throughout the year. This data element is required to track injury trends throughout the year.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>Injury Date is referred to as Death Date in the OTR DDS.</td>
</tr>
<tr>
<td><strong>Accident Number:</strong> This unique number is assigned by the investigating police department to identify a specific car crash.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>The decision to include these data elements in the OTR CDS was made by the MOHLTC and the TRAC.</td>
</tr>
<tr>
<td><strong>Patient Date of Birth:</strong> While not disclosed or used directly in analysis reports, this data element is useful in ensuring the accuracy of reported ages.</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Organ Donation:</strong> For patients who died, there is a flag to indicate whether or not an organ was donated and, if so, the type of organ involved.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Figure 3: National Trauma Registry Comprehensive Data Set

Data Providers
1. Provincial Trauma Registries
   (B.C., Alta., Que., N.S., N.L.)
2. Hospitals
   (Sask., Man., N.B. *)

Data Submission (eDSS)

Back-Up Tapes
(Off-Site Storage)

Public Reports
• Annual Report
• Analysis in Brief
• Data Quality Summary Report

Submission Status Reports
(Errors/Corrections/Warnings)

NTR CDS

Third-Party Data Requests
(Record Level and Aggregate)

OTR CDS
(All Records)

Provincial/Territorial Data Quality Report

Note
* New Brunswick is developing a provincial registry.

Figure 4: National Trauma Registry Minimum Data Set

DAD-HMDB
Data Providers
(see CAD PIA for more details)

Data Submission (eDSS)

NTR MDS/ OTR MDS

DAD-HMDB
1. All jurisdictions submitting to the DAD-HMDB
2. Records of patients with an external Cause code(s)

Public Reports
• Trauma eReport
• Analysis in Brief
• Quick Stats

Third-Party Data Requests, Where Authorized by MOH/ TC
(Record Level and Aggregate)
3 Privacy Analysis

3.1 Authorities Governing CIHI and the Trauma Registries

General

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

Legislation

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

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

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

Agreements

As indicated above, the data flows directly to CIHI via existing applications/systems from data providers, for example, from provincial hospitals and trauma registries and the Office of the Chief Coroner of Ontario. For the most part, these existing data flows are governed by CIHI’s *Privacy Policy, 2010*, existing legislation in the jurisdictions and data-sharing agreements with the provinces and territories or organizations. The data-sharing agreements set out the purpose, use, disclosure and retention requirements as well as any subsequent data sharing that may be permitted. The agreements also describe the legislative authority under which personal health information is disclosed to CIHI. For Ontario trauma data specifically, the MOHLTC has set up a contract with CIHI to manage the OTR.
Advisory Committees

The NTRAC is made up of provincial representation from trauma care experts and provincial trauma registries from each of the participating provinces across Canada, as well as representatives from the Trauma Association of Canada. The NTRAC plays a pivotal role in the development and maintenance of the NTR by providing advice on its goals and objectives, potential uses of the data, definitions, inclusion/exclusion criteria, data quality issues, report formats and development of promotional strategies.

The multidisciplinary TRAC provides guidance to the MOHLTC about the OTR. The TRAC is managed by the MOHLTC and includes representatives from CIHI; the ministries of Health and Long-Term Care, Labour and Transportation; the Office of the Chief Coroner; data analysts; injury prevention organizations; epidemiologists; and trauma care providers.

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 team, a Privacy and Data Protection Subcommittee of its Board of Directors and an external Chief Privacy Advisor.

Organization and Governance

The trauma registries are managed by the Clinical Registries department, under the Primary Health Care Information and Clinical Registries branch.

The following table identifies key internal senior positions with responsibilities for the trauma registries 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 the overall operations and strategic direction of the trauma registries.</td>
</tr>
<tr>
<td>Director, Primary Health Care Information and Clinical Registries</td>
<td>Fully accountable for the trauma registries. Responsible for strategic and operational decisions about the trauma registries and ensuring their continued successful development.</td>
</tr>
<tr>
<td>Manager, Clinical Registries</td>
<td>Responsible for ongoing management, development and deployment of the trauma registries. Makes operational decisions about the trauma registries and manages consultation with NTR and OTR stakeholders as appropriate.</td>
</tr>
<tr>
<td>Chief Technology Officer</td>
<td>Responsible for the strategic direction and overall operations/implementation of CIHI’s technological and security solutions.</td>
</tr>
<tr>
<td>Chief Privacy Officer</td>
<td>Responsible for the strategic direction and overall implementation of CIHI’s privacy program.</td>
</tr>
</tbody>
</table>
3.3 Principle 2: Identifying Purposes for Personal Health Information

The specific goals of the trauma registries are to

- Collect, process and analyze data about trauma hospitalizations;
- Play a role in reducing injuries and related deaths by providing data for national injury assessments;
- Facilitate provincial and international injury comparisons;
- Increase awareness of injury as a public health problem in Canada;
- Assist and inform injury prevention and treatment programs by providing national data; and
- Support injury-related approved analysis and research.

The data contained in the trauma registries is used by trauma prevention coalitions, trauma health care providers, researchers and injury prevention programs to

- Quantify trauma and educate Canadians about trauma and its consequences;
- Support efforts related to trauma prevention by providing a framework to better target public education or outreach campaigns toward vulnerable populations or high-risk activities; and
- Facilitate an examination of potential mechanisms to improve trauma treatment and access to trauma care.

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

The trauma registries data is disclosed to CIHI without individual consent for purposes of the planning and management of the health system, including statistical analysis and reporting.

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 personal health information and de-identified data that is reasonably required for health system uses, including statistical analysis and reporting, in support of the management, evaluation or monitoring of the allocation of resources to, or planning for, the health care system in Canada, including support for the improvement of the overall health of Canadians.

CIHI limits its collection of personal health information to that which is necessary to support authorized data quality and analytical activities. The data elements collected and their purposes have been identified and agreed upon in consultation with appropriate stakeholders (such as the NTRAC and TRAC) and are deemed to be the most pertinent to trauma surveillance and research initiatives.

The trauma registries do not capture the names of patients or their addresses (that is, street number and street name) from any source.
3.6 Principle 5: Limiting Use, Disclosure and Retention of Personal Health Information

3.6.1 Limiting Use

CIHI limits the use of data in the trauma registries to authorized purposes, as described in Section 3.3. This includes comparative analyses within and among jurisdictions; trend analyses to assess/monitor the impact of differences in policy, practices and service delivery; and statistics to support planning, management and quality improvement. Access to and use of trauma data is permitted on a need-to-know basis only. This includes access and use for data processing and quality management, producing statistics and data files, and conducting analyses. All authorized users are made aware of their obligations and responsibilities for privacy and confidentiality. All CIHI staff are required to sign a confidentiality agreement at the commencement of employment and are subsequently required to renew their commitment to privacy yearly.

Since 2009, data sets used for analysis purposes do not contain direct identifiers such as unencrypted (original) health card numbers. Health card numbers in an unencrypted form are available to CIHI staff on an exceptional, need-to-know basis only, and only with director-level approval.

Data Linkage

Data linkages are performed using trauma data and other data sources. While this potentially creates risk from a privacy perspective, CIHI has undertaken the following mitigating steps to reduce the risk.

Sections 14 to 31 of CIHI’s *Privacy Policy, 2010* govern linkage of records of personal health information. Pursuant to this policy, CIHI permits the linkage of personal health information under certain circumstances. Data linkage within a single data holding for CIHI’s own purposes is generally permitted. Data linkage across data holdings for CIHI’s own purposes and all third-party requests for data linkage are subject to an internal review and approval process. When carrying out data linkages, CIHI will generally do so without using names or personal health 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 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, ongoing program of work at CIHI 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.

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 one year after publication of the resulting analysis or three years after the linkage, whichever is sooner, in a manner consistent with CIHI’s Information Destruction Standard. For linked data resulting from an ongoing program of work at CIHI, 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 both to data linkages for CIHI’s own purposes and to third-party data requests.
3.6.2 Return of Own Data

Section 34 of CIHI’s Privacy Policy, 2010 establishes that the return of data to the health care facility that originally provided it to CIHI is not a disclosure; rather, it is considered a use. CIHI returns NTR CDS and OTR CDS data in the following ways:

- **Error/correction reports**: Record-level reports provide details of data quality issues that exist in a particular submission file. CIHI makes available to data providers reports on the outcome of their data submissions, including details of records that contain errors, so these organizations can investigate and, where necessary, correct and resubmit data.

- **Customized record-level and aggregate data files**: CIHI provides, when requested, data cuts (copies of the record-level data) back to the original data providers and their respective provincial or territorial ministries of health. Such data cuts may contain personal health information and are returned to the original data provider in accordance with CIHI’s Privacy Policy, 2010 procedures.

At the request of the MOHLTC and when the data is available, CIHI creates a report for the ministry.

3.6.3 Limiting Disclosure

Public Release of NTR and OTR Data

As part of its mandate, CIHI publishes aggregated data only in a manner designed to minimize any risk of identifiability and residual disclosure in compliance with sections 32 and 33 of its Privacy Policy, 2010. The trauma registries release public reports, specialized reports and province-specific reports, which are carefully scrutinized to limit the possibility of identifying individuals. Aggregate statistics and analyses made available on CIHI’s website (for example, annual reports, media releases, Quick Stats tables and Analysis in Brief reports such as ATV Injury Hospitalizations in Canada, 2004–2005) generally require a minimum of five observations per cell.\(^{vi}\)

---

\(^{vi}\) The 2005 NTR PIA indicated that in the past CIHI had released tables with cells containing fewer than five observations. The trauma registries comply with sections 32 and 33 of CIHI’s Privacy Policy, 2010, and now ensure that all publications and data cuts are reviewed by a second analyst, program lead, manager and, in certain cases, director.
Disclosures to Data Provider Community

The trauma registries make data available to the data provider community through CIHI’s eReporting service (known as CIHI Portal), a secure web-based application that allows authorized users to view trauma data via eReports that can be customized to meet their needs. CIHI creates statistics based on the trauma registries and discloses them to registered clients (that is, organizations that participate in the trauma registries and their respective provincial or territorial ministries of health). The eReports include aggregated de-identified information on client characteristics, clinical outcomes, service utilization, and quality and performance indicators. They also include organization-specific reports and reports comparing information across organizations, but they do not contain any person-identifying information (such as health card numbers, full dates of birth or full postal codes).

Disclosures to Third-Party Data Requestors

For OTR data, the MOHLTC is responsible for disclosing data to third parties. However, on a case-by-case basis, and with approval from the ministry, CIHI will disclose OTR data to third parties on its behalf. Otherwise, when requested, the trauma registries periodically disclose customized, record-level, de-identified data and/or aggregate data to a variety of users, such as the federal government, health care decision-makers, researchers and the media.

For all requests involving record-level NTR data, CIHI undertakes a rigorous multi-step review process; this review is administered through CIHI’s third-party data request program, which contains and ensures tight 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. Where aggregate data is not sufficiently detailed for the intended purpose, data that has been de-identified may be disclosed to the recipient on a case-by-case basis, where 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.

In 2009, CIHI adopted a complete lifecycle approach to data management. As part of that lifecycle, Privacy and Legal Services (PLS) 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 lifecycle. 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.

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 continue to comply with their obligations as set out in the Third-Party Data Request Form and Data Protection Agreement signed with CIHI.
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 research specified. All data protection agreements with third parties specify that receiving organizations must keep de-identified record-level data strictly confidential and not disclose such data to anyone outside the organization. Moreover, CIHI imposes obligations on these third-party recipients, including

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

### 3.6.4 Limiting Retention

The trauma registries form part of CIHI’s information holdings and, consistent with its mandate and core functions, CIHI retains such information for as long as necessary to meet the identified purposes.

### 3.7 Principle 6: Accuracy of Personal Health Information

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

Similar to other CIHI data holdings, the trauma registries are subject to an annual data quality assessment, based on CIHI’s *Data Quality Framework*. This framework provides an objective approach to applying consistent data-flow processes that focus on data quality priorities, assessing the data quality of a data holding and producing standard data holding documentation with the ultimate goal of continuous improvement in data quality for CIHI’s data holdings. It considers data quality from a user’s perspective, whereby quality is defined as “fitness for use.” Data quality is assessed based on 19 characteristics rolled up into five dimensions: timeliness, usability, relevance, accuracy and comparability. The process of completing the framework contains numerous activities to assess the accuracy of the 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 security system with respect to the trauma registries are described below.
Personnel Security

CIHI fosters and maintains a strong information privacy and data security culture. On initial employment and annually thereafter, all CIHI staff must sign confidentiality agreements and complete mandatory privacy and security training.

Physical Security

CIHI’s offices provide a secure physical site for information assets and staff through, for example, the use of controlled access to its premises, secured-access elevators and restricted access to individual floors requiring multi-factor authentication. Further restrictions are imposed within CIHI’s premises on its server rooms/data centres, where access is provided to only those employees who require such access for their employment, contractual or other responsibilities.

Data Communications Security

Participating data providers submit trauma data to CIHI through eDSS. The eDSS application uses a secure, encrypted SSL (secure sockets layer) session between CIHI and data providers for the purpose of data transfer. The level of encryption used is considered the industry standard and is used for most internet banking and e-commerce applications. The encrypted file transmission from eDSS is maintained in encrypted form until it is moved promptly into the protected area, where it is decrypted. The protected area has additional firewalls and is not linked to externally facing servers.

Similarly, trauma data–providing facilities access online error reports through CIHI’s secure, web-based Common Document Dissemination Service using an encrypted SSL session. Only users from authorized facilities, which have signed agreements with CIHI, may access the online reports using password-protected accounts.

Information Processing Security

The trauma files reside and are processed on secure servers that are maintained by CIHI’s ITS department. Once the data is on CIHI’s premises, it is stored in a database on a secure network that is not accessible outside the premises. CIHI’s electronic networks, systems and computing devices are restricted to authorized personnel on a need-to-know/-access basis. Staff’s desktop computers are subject to session time-outs that automatically log a user out after a pre-set period of inactivity, and technical and procedural barriers prevent unauthorized software from being installed by users. All corporate laptops employ disk encryption, and CIHI’s Policy on the Use of Mobile Computing Equipment restricts work that can be completed on mobile equipment.

Audits and Assessments

CIHI is committed to safeguarding its IT environment; to securing its data holdings; and to 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 and are intended to ensure that best practices are being followed and used 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 risk register, 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 to the public on its corporate website (www.cihi.ca).

3.10 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 health decisions affecting the individual. 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.

3.11 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 personal health information are investigated by the Chief Privacy Officer. The Chief Privacy Officer may direct an inquiry or complaint to the privacy commissioner of the jurisdiction of the person making the inquiry or complaint.

4 Conclusion

CIHI’s assessment of the trauma registries did not identify any privacy risks.