



# Trauma Registries

## Privacy Impact Assessment

May 2019



Canadian Institute  
for Health Information

Institut canadien  
d'information sur la santé

Production of this document is made possible by financial contributions from Health Canada and provincial and territorial governments. The views expressed herein do not necessarily represent the views of Health Canada or any provincial or territorial government.

All rights reserved.

The contents of this publication may be reproduced unaltered, in whole or in part and by any means, solely for non-commercial purposes, provided that the Canadian Institute for Health Information is properly and fully acknowledged as the copyright owner. Any reproduction or use of this publication or its contents for any commercial purpose requires the prior written authorization of the Canadian Institute for Health Information. Reproduction or use that suggests endorsement by, or affiliation with, the Canadian Institute for Health Information is prohibited.

For permission or information, please contact CIHI:

Canadian Institute for Health Information

495 Richmond Road, Suite 600

Ottawa, Ontario K2A 4H6

Phone: 613-241-7860

Fax: 613-241-8120

[cihi.ca](http://cihi.ca)

[copyright@cihi.ca](mailto:copyright@cihi.ca)

© 2019 Canadian Institute for Health Information

Cette publication est aussi disponible en français sous le titre *Registres des traumatismes : évaluation des incidences sur la vie privée, mai 2019*.

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

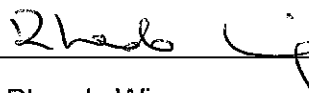
- **Trauma Registries**

Approved by:



---

Brent Diverty  
Vice President, Programs



---

Rhonda Wing  
Chief Privacy Officer & General Counsel

Ottawa – May 2019

# Table of contents

Quick facts about the trauma registries (National Trauma Registry and Ontario Trauma Registry) . . . . .	5
1 Introduction . . . . .	6
2 Background . . . . .	7
2.1 Introduction to the trauma registries . . . . .	7
2.2 OTR CDS data collection . . . . .	10
2.3 Access management, data submission and flow for OTR CDS . . . . .	11
3 Privacy analysis . . . . .	14
3.1 Privacy and Security Risk Management Program . . . . .	14
3.2 Authorities governing CIHI and the trauma registries . . . . .	15
3.3 Principle 1: Accountability for personal health information . . . . .	16
3.4 Principle 2: Identifying purposes for personal health information . . . . .	17
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 . . . . .	22
3.9 Principle 7: Safeguards for personal health information . . . . .	22
3.10 Principle 8: Openness about the management of personal health information . . . . .	24
3.11 Principle 9: Individual access to, and amendment of, personal health information . . . . .	24
3.12 Principle 10: Complaints about CIHI’s handling of personal health information . . . . .	24
4 Conclusion . . . . .	25
Appendix: Text alternative for images . . . . .	26

# Quick facts about the trauma registries (National Trauma Registry and Ontario Trauma Registry)

1. The creation of the trauma registries began with the Ontario Trauma Registry (OTR) in 1992, through funding from the Ontario Ministry of Health and Long-Term Care (MOHLTC).
2. The National Trauma Registry (NTR) was established in 1997. It was discontinued on March 31, 2014, due to a variety of factors that included the changing priorities of stakeholders, the limited use of the NTR Comprehensive Data Set by jurisdictions and the availability of some of the data elsewhere within the Canadian Institute for Health Information (CIHI).
3. The Ontario MOHLTC has set up a contract with CIHI to manage the OTR.
4. The OTR Comprehensive Data Set (OTR CDS) is currently CIHI's only trauma-specific holding that is routinely collecting data.
5. The OTR CDS is composed of approximately 200 data elements.
6. The trauma registry data collected features a variety of information, including demographic, administrative (e.g., preadmissions, ambulance transfers, circumstances of injury), clinical (e.g., diagnoses, procedures) and patient outcomes information.
7. The trauma registries do not capture the names of patients or their addresses (i.e., street number and street name) from any source.

# 1 Introduction

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

The purpose of this privacy impact assessment (PIA) is to examine the privacy, confidentiality and security risks associated with the National Trauma Registry (NTR) and the Ontario Trauma Registry (OTR), collectively referred to as the trauma registries. This PIA, which replaces the December 2012 version, includes a review of the 10 privacy principles set out in the Canadian Standards Association's *Model Code for the Protection of Personal Information*, as the principles apply to the trauma registries, and the application of CIHI's [Privacy and Security Risk Management Framework](#). The primary driver for this PIA is compliance with CIHI's [Privacy Impact Assessment Policy, August 2017](#).

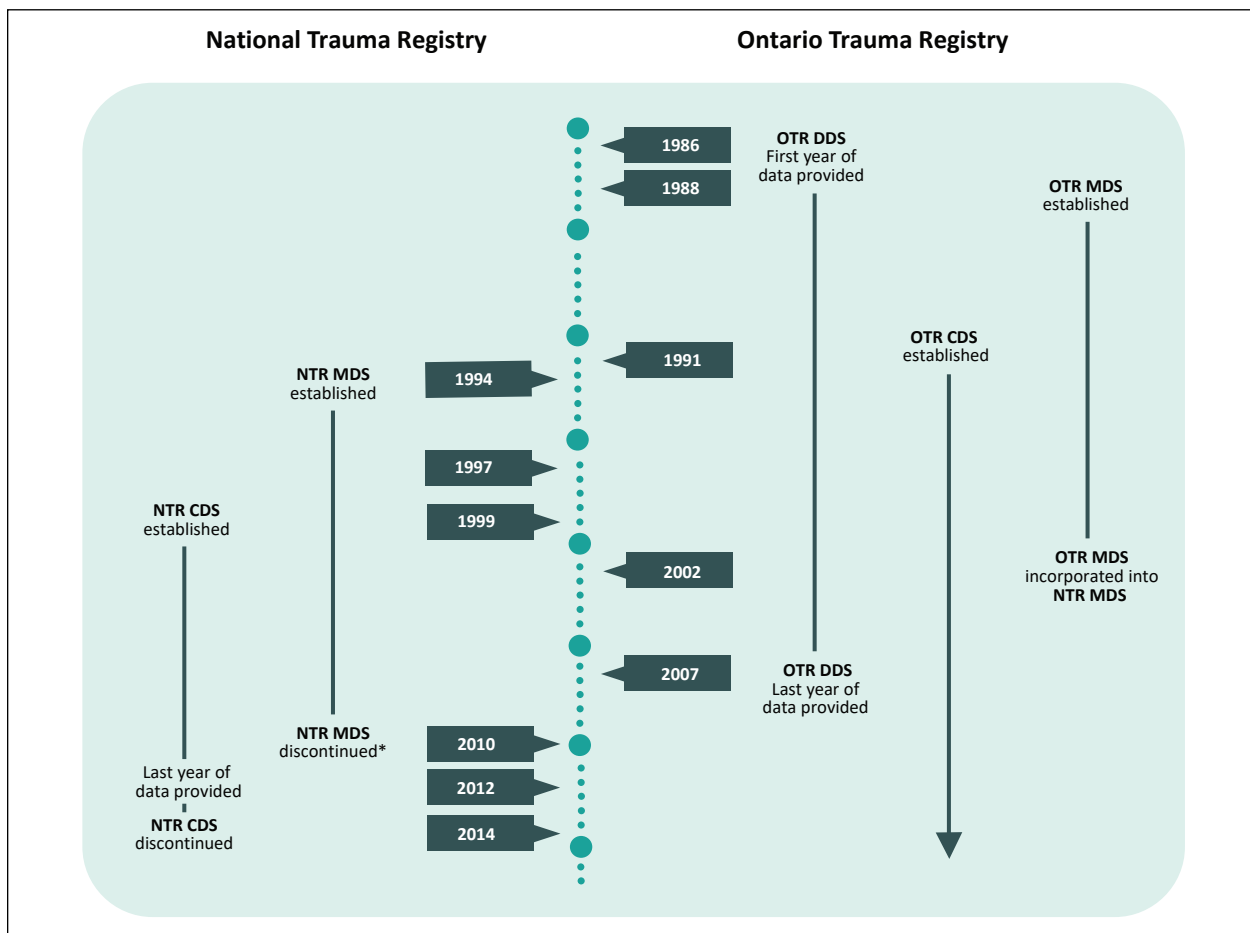
## 2 Background

### 2.1 Introduction to the trauma registries

The trauma registries are managed by CIHI’s Acute and Ambulatory Care Information Services branch. They consist of 5 separate trauma data holdings (see Figure 1):

1. OTR Comprehensive Data Set (OTR CDS), 1991–current;
2. Historical OTR Minimum Data Set (OTR MDS), 1988–2002;
3. Historical NTR Comprehensive Data Set (NTR CDS), 1999–2012;
4. Historical NTR Minimum Data Set (NTR MDS), 1994–2012; and
5. Historical OTR Death Data Set (OTR DDS), 1986–2007.

**Figure 1** Historical timelines of data years for the trauma registries



**Note**

\* NTR MDS data can be extracted from the Discharge Abstract Database–Hospital Morbidity Database for subsequent years.

The OTR CDS is currently CIHI's only trauma-specific holding that is routinely collecting data. The other data holdings contain historical data only and are securely stored, used and disclosed in accordance with CIHI's privacy and security policies.

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

## OTR

The OTR, which was created in 1992 through funding from the Ontario Ministry of Health and Long-Term Care (MOHLTC), contains data on patients hospitalized or killed due to trauma in Ontario. It is composed of 3 distinct data sets: the OTR CDS, the historical OTR DDS and the historical OTR MDS.

The goal of the OTR is to facilitate the reduction of injury hospitalizations and deaths in the province of Ontario.

### OTR CDS

The OTR CDS, which continues to routinely collect data, is composed of detailed information on patients hospitalized or who died in the emergency department with major trauma<sup>i</sup> in 11 participating facilities across 14 sites in the province.<sup>ii</sup> The data set is composed of approximately 200 data elements and includes information on the medical exam (i.e., vital signs, computerized tomography [CT] scans, operating room information), physician service information, special care unit information and trauma team activation flag. On average, the OTR CDS is populated with about 7,000 new records every year.

### Historical OTR DDS

OTR DDS data, which is no longer collected by CIHI, is composed of records of all deceased victims of trauma, where data is collected by the Office of the Chief Coroner of Ontario upon completion of its investigations. The first data set was received in 1986. The Office of the Chief Coroner of Ontario ceased providing data to the OTR in 2010. The last death data set provided to CIHI was for calendar year 2007. Currently, the OTR DDS contains 22 years of data (1986 to 2007). CIHI retains this historical data for the purposes of conducting statistical analyses and responding to third-party data requests when directed by the Ontario MOHLTC (see [Section 3.7](#)).

- 
- i. The definition of major trauma is based either on the Injury Severity Score (an international scoring system created to calculate the severity of injury) and an appropriate International Classification of Diseases External Cause of Injury Code or on the activation of a trauma team regardless of other criteria.
  - ii. Tertiary care (or Level 1) hospitals are designated by the MOHLTC to provide severely injured trauma victims with a high level of care, including the coordination with pre-hospital care and transport systems (both land and air ambulance services), the provision of in-hospital treatment, and the stabilization and discharge from hospital to community rehabilitation. Lead trauma hospitals are also known as regional trauma centres, according to the Provincial Trauma Network.



## Historical OTR MDS

The OTR MDS data set contains demographic, diagnostic and procedural information on all acute care hospitalizations due to injury and trauma in Ontario. Records for the OTR MDS are extracted from CIHI's Discharge Abstract Database–Hospital Morbidity Database<sup>iii</sup> (DAD-HMDB) that met the trauma registries' definition of trauma. The OTR MDS was a stand-alone database from 1988 until 2002, when the OTR MDS was incorporated into the NTR MDS (see below for more information about the NTR MDS). With the decommissioning of the NTR in March 2014, the OTR MDS can now be downloaded directly from the DAD-HMDB on an as-needed basis. CIHI retains the historical OTR MDS data back to 1988 and continues to use it for the purposes of conducting statistical analyses and responding to third-party data requests approved by the Ontario MOHLTC (see [Section 3.7](#)).

## NTR

The NTR was established in 1997 and contains data on patients hospitalized due to major trauma in Canada. The NTR is composed of 2 distinct data sets: the NTR CDS and the NTR MDS.

### Historical NTR CDS

The NTR CDS was discontinued in March 2014.

The NTR CDS is composed of a subset of severely injured patients submitted to CIHI by (a) provincial trauma registries<sup>iv</sup> from 5 provinces (Newfoundland and Labrador, Nova Scotia, Quebec, Alberta, British Columbia); and (b) individual hospitals from 4 provinces (New Brunswick, Ontario, Manitoba, Saskatchewan). Data was collected on trauma patients with an Injury Severity Score<sup>v</sup> of greater than 12.

The NTR CDS originally included 67 data elements. It was revised in 2011–2012 to include additional data elements and to standardize definitions across the provinces, and to be more consistent with international standards. In 2012–2013, the NTR CDS was expanded to include 87 data elements. These new data elements were primarily clinical in nature and did not include any unique personal identifiers.

---

iii. See the *Clinical Administrative Databases Privacy Impact Assessment* for more information about the DAD-HMDB.

iv. A provincial trauma registry is composed of data from multiple hospitals.

v. The Injury Severity Score is an international scoring system that was created to standardize the calculation of the severity of injury in a consistent way to allow for comparability internationally.

The number of records added to the NTR CDS annually varied depending on the number of participating provincial registries or individual hospitals. The total number of records available in the NTR CDS for 2012–2013 is 15,714. These records were submitted by 112 individual hospitals from 9 different provinces.

After the NTR CDS was discontinued in March 2014, CIHI retained this historical data and continues to use it for the purposes of conducting statistical analyses and responding to third-party data requests<sup>vi</sup> (see [Section 3.7](#)).

## Historical NTR MDS

The NTR MDS data includes trauma records extracted from CIHI's DAD-HMDB that had an International Classification of Diseases<sup>vii</sup> external cause of injury code included in the trauma registries' definition of trauma.

Approximately 15,000 records were extracted annually. The NTR MDS includes 260 data elements and contains data from 1994–1995 to 2010–2011, at which point CIHI ceased data extraction to populate the stand-alone NTR MDS. Since 2011–2012, NTR MDS data has been extracted directly from the DAD-HMDB on an as-needed basis.

## 2.2 OTR CDS data collection

The OTR CDS continues to routinely collect detailed data on major trauma patients from Ontario's lead trauma hospitals. Less detailed information on all trauma-related hospital admissions is reported to CIHI's hospitalization database (DAD-HMDB). The OTR CDS features a variety of information, including demographic, administrative (e.g., preadmissions, ambulance transfers, circumstances of injury), clinical (e.g., diagnoses, procedures) and patient outcomes information.

The following are examples of privacy-sensitive OTR CDS data elements that are common to the trauma registries. For data element definitions, please refer to the [OTR CDS data dictionary](#) and the [OTR CDS data element list](#).

**Trauma number** — This number uniquely identifies a case within an institution and is retained for quality assurance processing.

**Unique personal identifier (usually a health card number)** — Participating trauma hospitals typically submit unencrypted (original) health card numbers to the NTR and OTR for the purposes of uniquely identifying records and performing linkages.

---

vi. Approval from the MOHLTC is not required for third-party disclosure of NTR CDS data.

vii. The International Classification of Diseases is a World Health Organization initiative that classifies morbidity and mortality information for statistical purposes to assist the indexing of hospital records by disease and operations and the appropriate storage and retrieval of data.

**Patient age** — This element is required to identify, quantify and analyze differences in injury hospitalizations by age or age groupings.

**Patient sex** — This element is required to identify, quantify and analyze differences in injury hospitalizations by sex.

**Patient postal code** — Postal codes are used to support regional reporting and analysis of injury patterns or trends in particular geographic areas.

**Regional identifier of incident location** — This geographic information is required to support analyses of injury patterns, including where the injuries occur rather than where the injured persons reside. This data element helps to inform public health policies.

**Injury date** — This data element is required to track injury trends throughout the year. The occurrence of injuries (numbers and types) varies substantially during the year.

**Accident number** — This is a unique number assigned by the investigating police department that is used to identify a specific car crash.

**Patient date of birth** — This data element is useful in ensuring the accuracy of reported ages.

**Organ donation** — 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.

## 2.3 Access management, data submission and flow for OTR CDS

Access to CIHI's secure applications is subject to CIHI's role-based access management process, which is managed by CIHI's Client Support Applications (CSA) department. CSA manages access to CIHI's secure applications using established access management system (AMS) processes for granting and revoking access.

Once authenticated through CIHI's AMS, OTR CDS data providers submit record-level data electronically captured from facilities using specialized software to CIHI through CIHI's secure web-based electronic Data Submission Services.

At the time of processing, all submitted OTR CDS data automatically undergoes validation and a data quality check for errors and inconsistencies against specifications outlined in the [data dictionary](#). The data processing system is internal to CIHI, with no external connection.

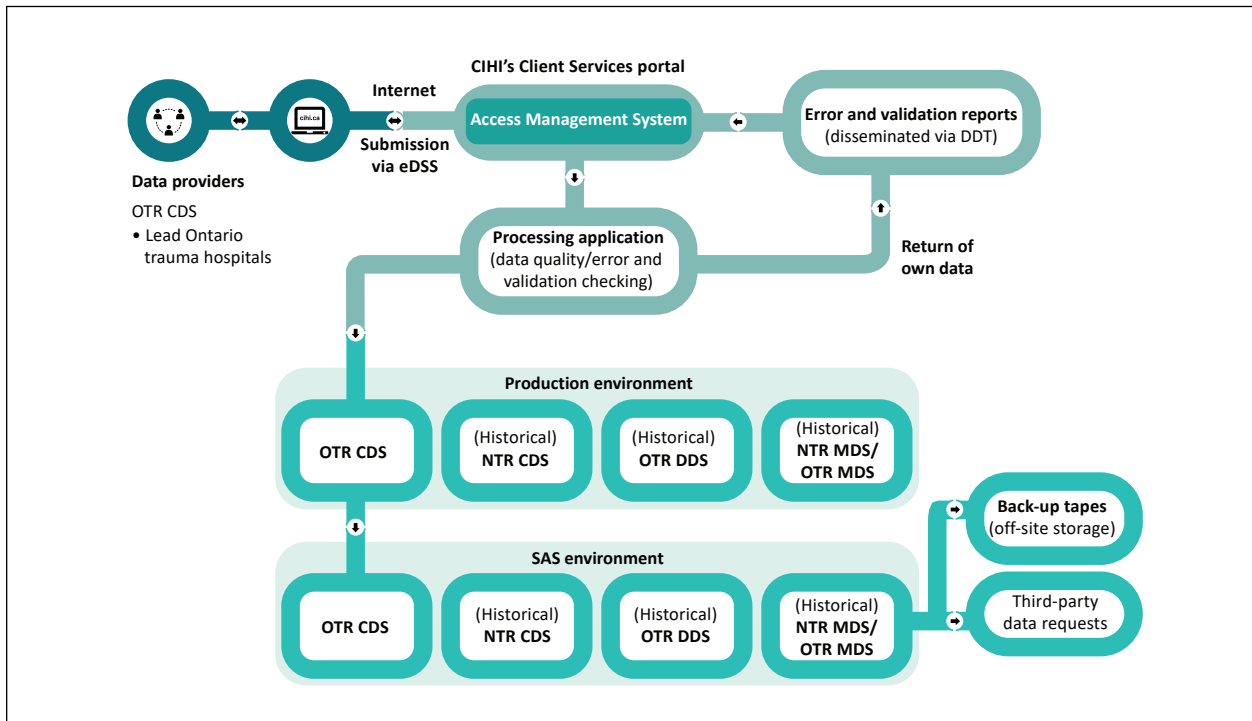
Error and validation reports generated at the time of processing are made available to the respective data providers via the Data Dissemination Tool in compliance with CIHI's *Secure Information Transfer Standard*. These reports identify records (using institution numbers and trauma numbers) with errors; specify the number of records a data provider has successfully submitted; indicate the reason records were rejected or the relevant warning message; and permit the data provider to correct errors in the records and resubmit them to OTR CDS.

Once the iterative error correction process is completed, final summary reports of file processing results are returned to data providers via email. A de-identified copy of the OTR CDS data set is then uploaded to the production database and subsequently to CIHI's SAS analytical environment where it is made available to approved CIHI staff for CIHI purposes. CIHI returns OTR CDS data to the Ontario MOHLTC. On behalf of the Ontario MOHLTC, CIHI also discloses aggregate and de-identified record-level data to third-party requestors and aggregate data to the public. Figure 2 is a high-level illustration of the data flows for the trauma registries.

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, including access to OTR CDS 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. [Section 3.9](#) includes additional details about how various procedural and technical measures are deployed to prevent unauthorized access and otherwise secure OTR CDS data.

All historical data within the NTR MDS, NTR CDS and OTR DDS remains securely stored, used and disclosed in accordance with CIHI's privacy and security policies.

**Figure 2** An overview of the data flow for the trauma registries



## 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 privacy and security risks.

Privacy and security risks may be identified from a variety of sources — including, for example, PIAs. Once identified, risks are entered into the Privacy and Security Risk Register and categorized as **high**, **medium** or **low** based on the likelihood and impact of a risk event.

- **High:** High probability of risk occurring and/or controls and strategies are not reliable or effective;
- **Medium:** Medium probability of risk occurring and/or controls and strategies are somewhat reliable or effective; or
- **Low:** Low probability of risk occurring and/or controls and strategies are reliable and effective.

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 how serious a risk is. 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 must be undertaken 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 CIHI and the trauma registries

### General

CIHI adheres to its [Privacy Policy, 2010](#) and to any applicable privacy legislation and/or legal agreements.

### Privacy legislation

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

The following provinces and territories have enacted health information–specific privacy legislation: Newfoundland and Labrador, Prince Edward Island, Nova Scotia, New Brunswick, Ontario, Manitoba, Saskatchewan, Alberta, Yukon and the Northwest Territories. Health information–specific privacy legislation authorizes facilities to disclose personal health information without patient consent for the purposes of health system use, provided that certain requirements are met. For example, CIHI is recognized as a prescribed entity under Ontario’s *Personal Health Information Protection Act, 2004*, 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

At CIHI, OTR CDS data is governed by CIHI’s [Privacy Policy, 2010](#), legislation in the jurisdictions and data-sharing agreements with the provinces and territories.

The 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. Specifically for Ontario trauma data, the Ontario MOHLTC has set up a contract with CIHI to manage the OTR.

### 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 trauma registries are managed by the Decision Support, Canadian Organ Replacement Register (CORR) and Trauma Registries department, in the Acute and Ambulatory Care Information Services branch.

The table below identifies key internal senior positions with responsibilities for the trauma registries data in terms of PSRM:

**Table** Key positions and responsibilities

<b>Position/group</b>	<b>Role/responsibilities</b>
<b>Vice president, Programs</b>	Responsible for overall strategic direction of the trauma registries
<b>Director, Acute and Ambulatory Care Information Services</b>	Responsible for overall operations and strategic business decisions about the trauma registries
<b>Manager, Decision Support, CORR and Trauma Registries</b>	Responsible for ongoing management, development and deployment of the trauma registries; makes operational decisions about the trauma registries and manages consultation with OTR stakeholders as appropriate
<b>Chief information security officer</b>	Responsible for the strategic direction and overall implementation of CIHI’s Information Security Program
<b>Chief privacy officer</b>	Responsible for the strategic direction and overall implementation of CIHI’s Privacy Program



## 3.4 Principle 2: Identifying purposes for personal health information

CIHI collects OTR CDS data for purposes consistent with those identified in [Section 2.1](#).

CIHI collects only personal health information required for achieving the goals of the trauma registries. The OTR CDS was initially defined in consultation with appropriate stakeholders.

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

- Quantify 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.

For definitions of data elements, please refer to the [OTR CDS data dictionary](#), the [OTR CDS data element list](#), the [NTR metadata](#), the [NTR CDS data dictionary](#) and the [DAD metadata](#).

This documentation is publicly available on CIHI's website.

## 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. Under sections 1 and 2 of CIHI's [Privacy Policy, 2010](#), CIHI collects from data providers only the information that is reasonably required for health system uses, including statistical analysis and reporting, in support of the management, evaluation and monitoring of the health care systems. In accordance with this principle, the OTR CDS collects only the information necessary to achieve the goals and purposes of the OTR CDS, as outlined in [Section 3.4](#).

The data elements collected by the OTR CDS and their purpose were identified and agreed upon in consultation with appropriate stakeholders, and deemed the most pertinent to trauma surveillance and research initiatives.

The rationale for limiting the collection (i.e., decommissioning holdings or discontinuing the flow) of NTR MDS, NTR CDS and OTR DDS data was due to a number of factors:

- The changing priorities of our stakeholders;
- The timeliness of data submission by providers;
- The limited use of the NTR CDS by jurisdictions; and
- The availability of some of the data elsewhere within CIHI.

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

### Limiting use

CIHI limits the use of data in the trauma registries to authorized purposes as described in [sections 2.1](#) and [3.4](#).

CIHI uses the trauma registries' data for the purposes of conducting statistical analyses and responding to third-party data requests. This includes conducting trend analyses to assess/monitor the impact of differences in policy, practices and service delivery, and providing statistics to support planning, management and quality improvement.

CIHI staff are permitted to access and use data on a need-to-know basis only, including for data processing and quality management, for producing statistics and data files, and for conducting analyses. 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.

Data sets used for internal CIHI analysis purposes do not contain direct identifiers, such as unencrypted health card numbers. They are removed from records before being moved to the OTR CDS analytical environment ([see Section 2.3](#)). Health card numbers in an unencrypted form and other direct identifiers are available to authorized CIHI staff on an exceptional, need-to-know basis only, subject to approval processes as set out in CIHI's internal 2010 privacy policy and procedures.

## Data linkage

Data linkages are performed between the trauma registries' data and other CIHI data sources. While this potentially causes greater risk of identification of an individual, CIHI undertakes mitigating steps to reduce risks. One such step is de-identification — removing patient identifiers and assigning meaningless transaction numbers.

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 using consistently encrypted health card 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:

- Section 23: The individuals whose personal health information is used for data linkage have consented to the data linkage; or
- Section 24: All of the following criteria are met:
- a. The purpose of the data linkage is consistent with CIHI's mandate;
  - b. The public 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 card number, and the province or territory that issued the health card number. 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 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.

For time-limited specific projects, Section 29 of CIHI's [Privacy Policy, 2010](#) further requires that the secure destruction of linked data 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 *Secure Destruction Standard*. For linked data resulting from an 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 *Secure Destruction Standard*. These requirements apply to data linkages both for CIHI's own purposes and for third-party data requests.

## Return of own data

In addition to returning data to submitting facilities, Section 34 of CIHI's [Privacy Policy, 2010](#) establishes that CIHI may return records to the relevant ministry of health for data quality purposes and for purposes consistent with their mandate. An example would be for health services and population health management, including planning, evaluation and resource allocation. The return of own data is considered a use and not a disclosure.

## Limiting disclosure

### Third-party requests

For OTR data, the Ontario MOHLTC is responsible for disclosures of 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.

CIHI continues to respond to third-party requests for customized de-identified record-level and/or aggregated data from the NTR.

CIHI administers a third-party data request program that establishes privacy and security controls that must be met by 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 aggregated 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.

CIHI has adopted a complete life cycle approach for record-level third-party data requests. As part of that life cycle, the Privacy and Legal Services branch 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 complete and submit a data request form. 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;
- Restrictions on the publication of cell sizes less than 5; and
- Strong encryption technology that meets or exceeds CIHI's standards where mobile computing devices are used.

In addition to the ongoing compliance monitoring process, whereby all data sets that are disclosed to third-party data recipients are tracked and monitored for secure destruction at the end of their life cycle, the Privacy and Legal Services branch contacts third-party data recipients on an annual basis to certify that they continue to comply with their obligations as set out in the data request form and data protection agreement that they signed with CIHI.

## **Public release of trauma data**

The trauma registries no longer release public reports, specialized reports or province-specific reports.

## **Disclosures to data provider community**

The trauma registries no longer make data available to the data provider community through CIHI's eReporting service.

## **Limiting retention**

The trauma registries data 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 in compliance. Accordingly, CIHI continues to retain historical NTR data for the purposes of conducting statistical analyses and responding to third-party data requests.

## **3.8 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 OTR CDS is subject to an annual data quality assessment, based on [CIHI's Information Quality Framework](#). The process of completing the framework includes numerous activities to assess the various dimensions of quality, including the accuracy of OTR CDS data.

## **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 enterprise 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 to provide an integrated view of the organization's information management practices. Key aspects of CIHI's system security with respect to trauma registry data are highlighted below.

## System security

CIHI recognizes that information is secure only if it is secure throughout its entire life cycle: during creation and collection, access, retention and storage, use, disclosure and destruction. Accordingly, CIHI has a comprehensive suite of policies that specify 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 integral components 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 card number has been removed or encrypted upon first receipt. In exceptional instances, staff will require access to original health card numbers. CIHI's internal 2010 privacy policy and procedures 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 card 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 communications about CIHI's privacy and security policies and procedures. 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 to the public on its corporate website at [cihi.ca](http://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](#), questions, concerns or complaints about CIHI's handling of information are investigated by the chief privacy officer, who may direct an inquiry or complaint to the privacy commissioner of the jurisdiction of the person making the inquiry or complaint.



## 4 Conclusion

CIHI's assessment of the trauma registries did not identify any privacy or security risks.

This PIA will be updated or renewed in compliance with CIHI's [Privacy Impact Assessment Policy, August 2017](#).

# Appendix: Text alternative for images

## **Text alternative for Figure 1: Historical timelines of data years for the trauma registries**

The NTR MDS was established in 1994 — a precursor to establishing the NTR in 1997, which included establishing the NTR CDS in 1999. The flow of data to CIHI was discontinued in 2010 for the NTR MDS. NTR MDS data can be extracted from the Discharge Abstract Database–Hospital Morbidity Database for subsequent years. 2012 was the last year of data provided for the NTR CDS and the flow of data was discontinued in 2014.

The flow of data to CIHI began in 1986 for the OTR DDS and ended in 2007.

The OTR MDS was established in 1988; in 2002, OTR MDS data was incorporated in the NTR MDS.

The OTR CDS was established in 1991 and is currently CIHI's only trauma-specific holding routinely collecting data.

## **Text alternative for Figure 2: An overview of the data flow for the trauma registries**

Data providers such as lead Ontario trauma hospitals electronically submit trauma records to CIHI using specialized software through CIHI's secure web-based electronic Data Submission Services (eDSS).

Once submitted within CIHI's secure environment, all OTR CDS data undergoes processing activities that include a data quality check for errors and inconsistencies before being integrated into the OTR CDS production and analytical (SAS) environments. Errors and inconsistencies are identified in error and validation reports and are returned to the original data submitters for correction via CIHI's data dissemination tools.

All trauma registry data (NTR and OTR) stored in the SAS environment is backed up and stored off-site, and is used by program staff to respond to third-party requests.

**CIHI Ottawa**

495 Richmond Road  
Suite 600  
Ottawa, Ont.  
K2A 4H6  
**613-241-7860**

**CIHI Toronto**

4110 Yonge Street  
Suite 300  
Toronto, Ont.  
M2P 2B7  
**416-481-2002**

**CIHI Victoria**

880 Douglas Street  
Suite 600  
Victoria, B.C.  
V8W 2B7  
**250-220-4100**

**CIHI Montréal**

1010 Sherbrooke Street West  
Suite 602  
Montréal, Que.  
H3A 2R7  
**514-842-2226**

---

cihi.ca

20436-0719

