



National System for Incident Reporting

Privacy Impact Assessment

March 2022



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

copyright@cihi.ca

© 2022 Canadian Institute for Health Information

How to cite this document:

Canadian Institute for Health Information. *National System for Incident Reporting Privacy Impact Assessment, March 2022*. Ottawa, ON: CIHI; 2022.

Cette publication est aussi disponible en français sous le titre *Système national de déclaration des accidents et incidents : évaluation des incidences sur la vie privée, mars 2022*.

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

- *National System for Incident Reporting Privacy Impact Assessment, March 2022*

Approved by

Brent Diverty
Vice President, Data Strategies and Statistics

Rhonda Wing
Executive Director, Chief Privacy Officer and General Counsel, Office of the Chief Privacy Officer and Legal Services

Ottawa, March 2022

Table of contents

Quick facts about the National System for Incident Reporting	5
Definitions	6
1 Introduction	7
2 Background	7
2.1 Introduction to NSIR	8
2.2 Data collection	9
2.3 Access management, data submission and flow for NSIR	12
3 Privacy analysis	17
3.1 Privacy and Security Risk Management Program	17
3.2 Authorities governing NSIR data	18
3.3 Principle 1: Accountability for de-identified NSIR data	20
3.4 Principle 2: Identifying purposes for de-identified NSIR data	21
3.5 Principle 3: Consent for the collection, use or disclosure of de-identified NSIR data	21
3.6 Principle 4: Limiting collection of de-identified NSIR data	21
3.7 Principle 5: Limiting use, disclosure and retention of de-identified NSIR data	22
3.8 Principle 6: Accuracy of de-identified data	25
3.9 Principle 7: Safeguards for de-identified data	25
3.10 Principle 8: Openness about the management of personal health information	27
3.11 Principle 9: Individual access to, and amendment of, personal health information	27
3.12 Principle 10: Complaints about CIHI's handling of personal health information	27
4 Conclusion	27
Appendices	28
Appendix A: National System for Incident Reporting — Medication Minimum Data Set	28
Appendix B: National System for Incident Reporting — Radiation Treatment Minimum Data Set	31
Appendix C: Text alternative for images	33

Quick facts about the National System for Incident Reporting

1. The National System for Incident Reporting (NSIR) at the Canadian Institute for Health Information (CIHI) is a voluntary reporting system designed to facilitate sharing of and learning from medication and radiation treatment (RT) incidents. It enables analysis at the local and national levels, and helps to identify rare and emerging patient safety occurrences.
2. More than 900 health care facilities currently participate in NSIR. Collectively, they have contributed more than 78,000 medication incidents and more than 6,000 RT incidents.
3. Through its web-based application, NSIR collects a standardized set of information on incidents. Individual records can be manually entered as single incidents, or facilities can submit data directly from their local risk management systems via batch upload or application programming interface (API)ⁱ method.
4. NSIR does not collect any identifiers (patient, provider or facility).
5. NSIR provides users with an Analytical Tool to create summary reports or comparison reports, as well as a Communication Tool to enable private, non-identifying discussions with other participating facilities.
6. NSIR is CIHI's contribution to the Canadian Medication Incident Reporting and Prevention System (CMIRPS), a collaboration between Health Canada, CIHI, the Institute for Safe Medication Practices Canada and the Canadian Patient Safety Institute. The goal of CMIRPS is to reduce and prevent harmful medication incidents in Canada.
7. The NSIR-RT Advisory Committee and the Canadian Association for Provincial Cancer Agencies are key collaborators for RT incident reporting.

i. An API is a set of subroutine definitions, protocols and tools for building application software (https://en.wikipedia.org/wiki/Application_programming_interface).

Definitions

For the purposes of this privacy impact assessment, these terms have the following meanings:

Aggregate data means record-level data related to records of incidents that has been compiled to a level of aggregation that ensures that the identity of individuals cannot be determined by reasonably foreseeable methods.

Client means the organization specified in the NSIR Service Agreement, for either data providers or non-submitters, that is binding itself to comply with the terms of the agreement.

Designated user means a client's employee or permitted contractor (e.g., partner organization) that has been authorized by the client to access and use NSIR.

Data provider means any federal/provincial/territorial ministry, department or agency, regional health authority, health care facility, public or private institution, or organization participating in NSIR that provides incident records to CIHI.

Incident record means record-level data related to records of medication or RT incidents provided to CIHI for the purposes of NSIR.

Medication incident means any preventable circumstance or event that may cause or lead to inappropriate medication use or patient harm while the medication/IV fluid is in the control of the health care professional, patient or consumer.

NSIR data means all de-identified record-level incident data contained within NSIR and any aggregate data generated by NSIR.

Own data means medication and/or RT incident records that were originally provided to CIHI by a data provider for the purposes of NSIR.

Partner organization means an organization that has entered into an NSIR Service Agreement for Non-Submitters with CIHI, which permits it to access NSIR for the purposes specified in the agreement.

Radiation treatment incident means any preventable circumstance or event related to patient assessments, imaging, treatment planning and delivery, pre-treatment review and verification, quality management and post-treatment completion that causes harm or has the potential to cause harm.

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 System for Incident Reporting (NSIR). This PIA is an update to include the assessment of the application programming interface (API)ⁱⁱ submission method for the radiation treatment (RT) module, replacing the January 2018 version. The PIA includes a review of the 10 privacy principles set out in the Canadian Standards Association's *Model Code for the Protection of Personal Information* and how the principles apply to NSIR, as well as a look at 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](#).

2 Background

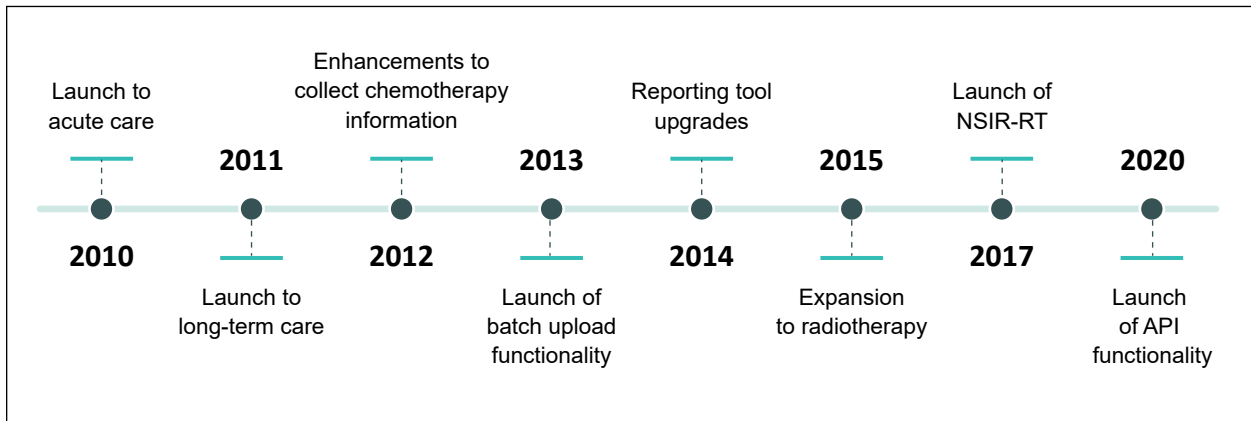
Incidents are, by definition, preventable events. Examples include prescribing Lasix for a patient instead of Losec (medication incident) or performing RT on the wrong anatomical site (RT incident). NSIR aims to identify how incidents occur in Canadian health care facilities and how similar incidents may be prevented. NSIR is a voluntary reporting system designed to securely and anonymously support the collection, sharing and analysis of standardized incident data. Anonymized reporting encourages participation and protects the identity of patients, providers and facilities who participate in NSIR. Its data and related analyses inform quality improvement activities at local, regional, provincial, territorial and national levels to foster improvements in health care delivery.

ii. An API is a set of subroutine definitions, protocols, and tools for building application software (https://en.wikipedia.org/wiki/Application_programming_interface).

2.1 Introduction to NSIR

NSIR officially launched in 2010. At that time, its focus was to collect medication incident data from acute care health care facilities across Canada. Since then, NSIR has steadily expanded its scope. The collection of medication incident data from long-term care (LTC) facilities was launched in 2011, and the collection of RT incident data was launched in 2017.

Figure 1 NSIR timeline



NSIR is part of the multi-organizational Canadian Medication Incident Reporting and Prevention System (CMIRPS) initiative, which contributes information, tools and expertise to the prevention of harmful medication incidents. CIHI’s contribution to CMIRPS is NSIR, which collects medication incident data from Canadian health care facilities. The NSIR system includes the Analytical and Communication tools to support the analysis and sharing of medication incidents and preventive strategies. CIHI produces analytical reports from the NSIR data to support enhancements to the medication use system.

CIHI collaborated with the Canadian Partnership for Quality Radiotherapy to develop and implement NSIR-RT, a national system for reporting RT incidents in Canada. NSIR-RT was built as a response to the need for a dedicated, scalable RT incident management system to support not only local quality improvement activities, but also incident learning across programs and jurisdictions.

The 2 types of NSIR users are data providers and partner organizations; they are collectively referred to as clients (see the [Definitions](#) section). Data providers include participating organizations that submit and analyze NSIR data according to their signed service agreements. Partner organizations have signed a specific agreement, the NSIR Service Agreement for Non-Submitters, that allows them to access NSIR data for specified analytical purposes.

As of April 2021, clients of NSIR include the following:

Data providers

- Health care facilities (e.g., hospitals, LTC facilities)
- Cancer treatment centres
- Regional health authorities (RHAs)
- Provincial/territorial ministries of health
- Organizations that submit data on behalf of facilities and RHAs (e.g., BC Patient Safety & Learning System)

Partner organizations

- Institute for Safe Medication Practices Canada
- Health Canada (Marketed Health Products Directorate)
- Saskatchewan Ministry of Health
- Ontario Ministry of Health
- Ontario Health

NSIR's objectives for both medication and RT incidents are to

- Collect high-quality standardized incident data;
- Facilitate sharing of and learning from incidents;
- Enable analysis at local, regional and national levels;
- Identify rare and emerging patient safety occurrences; and
- Develop partnerships that create and disseminate strategies, recommendations and solutions to patient safety issues.

2.2 Data collection

As previously indicated, NSIR is designed to collect incident data securely and anonymously. NSIR does not include the collection of direct identifiers (e.g., patient-/resident-identifiable information such as name, health card number, chart number or date of admission or discharge; provider-identifiable information such as name or registration number).

NSIR includes a minimum data set (MDS) for each medication incident record and RT incident record (see [Table 1](#) and [appendices A and B](#)), and the following tools:

Reporting Tool

Data providers electronically submit data using the Reporting Tool. It is a secure web-based application designed to accept incident records using the following methods: single-incident submission; batch upload; or API. Individual records can be entered using the single-incident submission method. Facilities can submit multiple incident records that have been extracted and grouped together as a batch file or via API.

Data providers use the Reporting Tool to submit a number of mandatory and optional data elements (see [Table 1](#) and [appendices A and B](#)). This includes a free-text field for a description of the incident, which provides a detailed, factual description of what happened during the incident.

Analytical Tool

De-identified incident records released to the NSIR repository can be accessed via a business intelligence tool that allows designated users, including data providers and partner organizations, to build template reports that can be customized to some extent. Reports generated by users are anonymous and do not identify the source facilities, except in situations where a data provider is accessing its own data, or where a user has granted another user permission to view data that identifies the health facility. Within any NSIR report, users are able to drill down from aggregate totals to individual de-identified incident records and export results into PDF or Microsoft Excel format. Comparison reports, subject to the service agreement, allow for provincial, regional, corporation, site-level and peer group (i.e., groups of similar facilities) views.

Communication Tool

The Communication Tool is similar to a web-based email application. It allows for non-identifying (private and anonymous) discussion between data providers. Messages sent by data providers are anonymous — email addresses of senders and recipients are replaced with system-generated facility pseudonyms to maintain anonymity. Within NSIR, individual de-identified incident records include a hyperlink to the Communication Tool, where users can also send an anonymous email to the submitting facility.

CIHI and the partner organizations can also send emails via the Communication Tool, but their emails are not anonymous. They are not assigned a pseudonym and are identified by organizational name in their messages to and from other NSIR users.

Table 1 Information domains for the NSIR minimum data sets

Information domain	Medication incident MDS (Appendix A)	RT incident MDS (Appendix B)
Incident Impact	Categorization of the outcomes (actual and/or potential) and effects of the incident	Characterization of the incident (actual/near miss/programmatic hazard) and effects (acute, dosimetric and latent) of the incident
Incident Discovery	The discovery of the incident: time, place and roles of health providers associated with the incident	
Patient/Resident Characteristics	Demographic characteristics of the patient	Demographic and disease characteristics of the patient
Incident Details	Specific medication incident details	Specific RT incident details
Drug Product Information	Information pertaining to drug product(s) reported in the incident, such as drug name, strength, form and route	Not applicable
Treatment Delivery	Not applicable	Specific details regarding the treatment delivery, including the RT technique, dose and fraction prescription, technologies and equipment used, site treated and treatment intent
Incident Investigation and Findings	Information pertaining to actions planned or implemented to help prevent a similar incident from occurring in the future	Information pertaining to actions taken to ameliorate the incident outcome, as well as to safety barriers and actions planned to reduce the risk of incident recurrence

One of the guiding principles for the development of NSIR was anonymity of patients/residents, health care providers and health care facilities. As a result, the de-identified incident records held in NSIR cannot be used to determine the identity of patients or providers by a reasonably foreseeable method (see [Section 3.6](#)).

2.3 Access management, data submission and flow for NSIR

NSIR is designed to support learning and sharing, and anonymity of data providers is paramount. In addition to the use of pseudonyms, as described in [Section 2.2](#), access management ensures that NSIR data is accessible only by those authorized to access and use the NSIR system to submit incidents and analyze data. This includes data providers (medication and RT incidents) and partner organizations.

Access to CIHI's secure applications is managed by CIHI's Product Management and Client Experience (PMCE) department. PMCE manages access to CIHI's secure applications using established access management system (AMS) processes for granting and revoking access.

Access to NSIR to submit radiation treatment incidents via API

In order to access NSIR to submit RT data through the use of APIs, the system that is sending data to CIHI must be registered with CIHI. The system can be registered by data providers or their authorized software vendors. The registration process for access is outlined below.

System registration

Data providers or their authorized software vendors are required to sign CIHI's Health Information Standards and Specifications Agreementⁱⁱⁱ (including Schedule A — Product Terms and Conditions), which governs the access to and use of the products^{iv} as well as the rights, restrictions and obligations pertaining to the environment^v and products (see also [Section 3.2](#)). Data providers and their authorized software vendors must also complete a Vendor Testing Form identifying the individual(s) who will be completing the system registration(s).

To register a system with CIHI, a representative of the data provider or their authorized software vendor must create a CIHI profile. CIHI uses the profile information along with information provided in the Vendor Testing Form to grant representative(s) access to register the system for the appropriate organization(s). Once authenticated through CIHI's AMS, data flows directly from the data provider's system repository or the data provider's authorized software vendor application to CIHI's NSIR system.

iii. CIHI's Health Information Standards and Specifications Agreement includes Schedule B, which consists of forms for terminating use of the product.

iv. "Products" means the CIHI products, specifications, documentation, software and other materials and related services, including but not limited to support and updates, selected by clients pursuant to the agreement. For greater certainty, this also includes all methods, techniques, algorithms, information and data disclosed within the products.

v. "Environment" means the web pages of cihi.ca on which CIHI's standards and specifications are hosted.

Access to data within NSIR

A second layer of access management requirements has been implemented for NSIR, based on the stages involved in creating and completing NSIR records. See Table 2 for an overview of who can access what data in NSIR from the time incident records are created to the time they are released into the NSIR repository.

Table 2 User access by affiliation during staging of NSIR records

Stage/condition of records	Access by user's affiliation			
	Data provider (source facility)	Data provider (non-source facility)	CIHI (NSIR team)	Partner organization
<p>Stage 1: Pre-submission (draft)</p> <p><i>Single-incident processing:</i> Incident records are entered in NSIR but not submitted.</p> <p><i>Batch or API submission:</i> Incident records reside in the data provider's incident reporting system. No records have been extracted via the batch upload or API methods.</p>	Yes	No	No	No
<p>Stage 2: Submitted (under review)</p> <p>Incident records have been submitted via</p> <ul style="list-style-type: none"> • Single-incident submission; • Batch upload; or • API. <p>Incident records undergo 2-step data quality processing:</p> <p>Step 1: Automated review of codified data.</p> <p>Step 2: Manual review of free-text fields.</p>	Yes	No	Yes	No
<p>Stage 3: Complete (final)</p> <p>2-step data quality processing is complete and all issues have been corrected.</p> <p>Incident records are confirmed as de-identified and released into the NSIR repository for analysis and reporting.</p> <p>Users are able to drill down from aggregate totals to individual de-identified incident records.</p>	Yes	Yes Reports are anonymous and do not identify the source facilities	Yes	Yes Reports are anonymous and do not identify the source facilities

Data flows

In NSIR, each record is a single incident. As of April 2021, NSIR contained more than 73,000 medication incidents and 5,500 RT incidents submitted by more than 900 health care facilities.

When an incident occurs (medication or RT), it is reported within the health care facility and reviewed internally. Once the internal review is complete, the incident record is sent from a data provider to CIHI. Data is submitted from data providers to NSIR through the Reporting Tool via single-incident, batch or API submission. For single-incident submissions, incident data is entered directly into NSIR. For batch or API submissions, incident data entered in the data provider's incident reporting system is extracted and securely transmitted to NSIR via either the batch upload or API method. Once received in NSIR, all incident records — regardless of whether they were received through the single-incident, batch or API submission — undergo a 2-step data quality assessment process.

Step 1: Automated data quality processing

The first step is an automated process, where codified data is assessed to be valid and in the proper format.

Single-incident submissions

For single-incident submissions, edit checks are performed automatically by the system as the details of an incident are entered. If the record passes all the edit checks, all data moves on to Step 2, manual data quality processing (see below). If any data quality issues are discovered in Step 1, they are flagged in real time to data providers to be corrected.

Batch or API submissions

For batch or API submissions, edit checks are also performed automatically. If the record passes all the edit checks, all data moves on to Step 2 (see below). However, unlike with single-incident submissions, any data quality issues discovered in Step 1 are returned to data providers by way of a submission report via the batch or API method. Corrections made by data providers are resubmitted to NSIR via the batch or API method.

Step 2: Manual data quality processing

The second step is a manual data quality review process that focuses on the free-text fields of incident records. These are reviewed daily by the NSIR support team for the presence of any personal and geographic identifiers (e.g., actual names, initials, abbreviations) that may be associated with patients/residents, health care providers and health care facilities that may have been submitted inadvertently by the data provider.

If no issues are discovered, the incident record (including both codified and free-text data fields) is made available within 24 hours for analysis and reporting by all those authorized to access and use NSIR.

If any issues are discovered, the incident records are returned to data providers for correction. The record is suppressed until the data provider makes the correction (i.e., removes the identifier). Once the correction has been confirmed by NSIR staff, these incident records are deemed to be de-identified and are released into the NSIR repository, where they are made available within 24 hours for analysis and reporting by all those authorized to access and use NSIR.

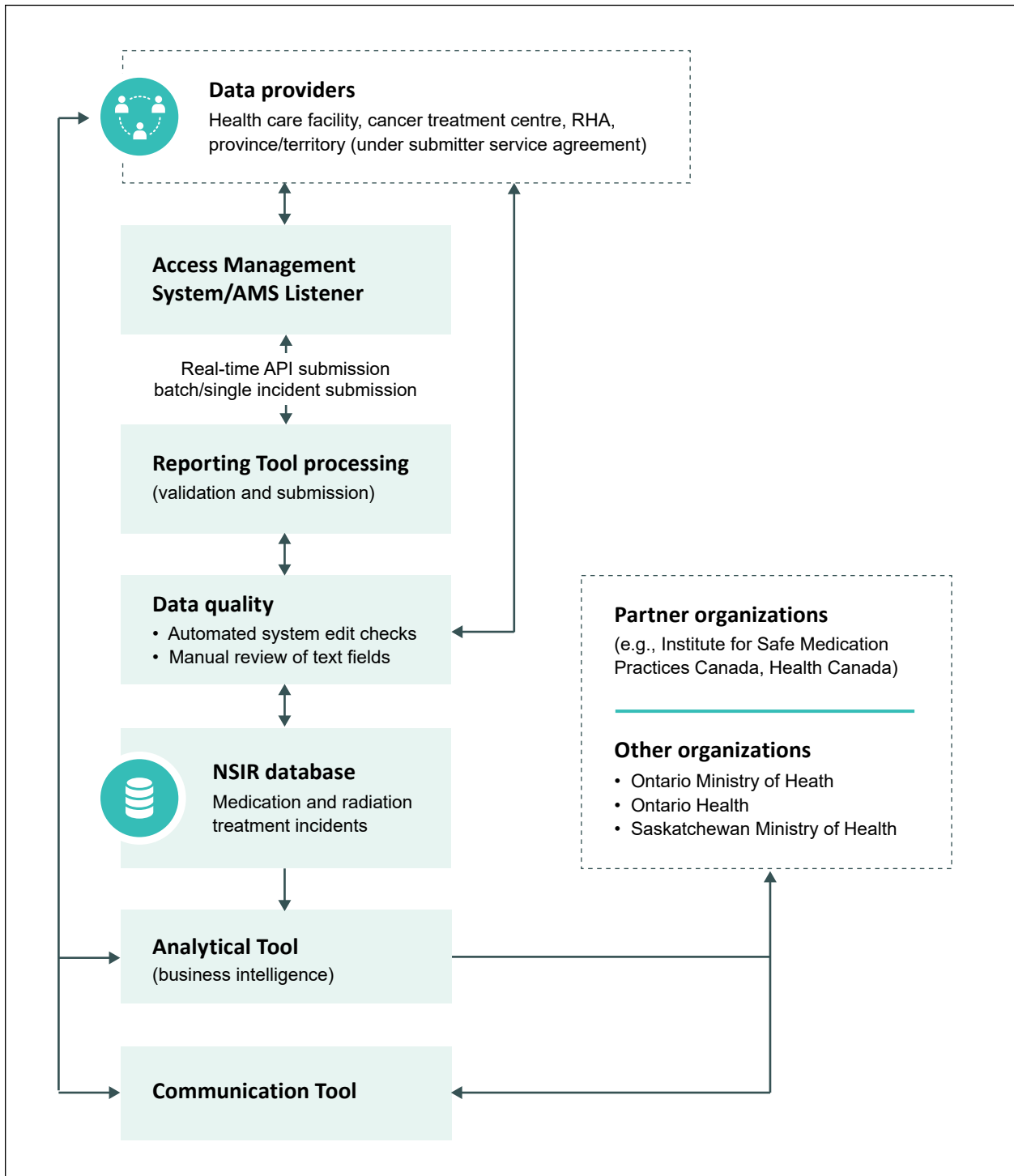
The NSIR team reviews free-text fields for single-incident, batch and API submissions of data. The team works with data providers to establish the level of monitoring required for free-text fields. This depends in large part on the data provider's level of experience and compliance with data submission requirements, the data quality processes in place at the submitting facility and the quality of the data received. The degree of scrutiny of CIHI's data quality review process will be determined together with the data provider to balance the risk of an identifier appearing in an NSIR record with the resources needed by both organizations to mitigate these risks. Batch and API submissions of incident data bring unique challenges with the review of free-text fields due to the potential large volume of data that may be received at a time and the resources required to review and release these records in a timely manner. In contrast, single-incident submissions are received in much smaller numbers and are generally easier to manage. The NSIR team reassesses the process for reviewing free-text fields on a case-by-case basis. Any reassessment of this nature will be included in CIHI's Privacy and Security Risk Register.^{vi} To date, no patient identifiers have been found in the more than 84,000 medication and RT incident records submitted to NSIR. While some facility and provider identifiers have been detected, all were confirmed as de-identified and removed before the associated records were released into NSIR.

Copies of CIHI data and applications are retained on backup systems.

All the NSIR data flows are highlighted in Figure 2.

vi. A consolidated list of CIHI's current identified privacy and security risks.

Figure 2 Overview of NSIR data flow



3 Privacy analysis

3.1 Privacy and Security Risk Management Program

Privacy and security risk management 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, monitoring and reviewing 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 Executive Committee on behalf of the corporation.

There were no new privacy and security risks identified as a result of this PIA.

3.2 Authorities governing NSIR data

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 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: 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 the *Personal Health Information Protection Act of Ontario*, 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.

In 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, NSIR data is governed by CIHI’s [Privacy Policy, 2010](#), by legislation in the jurisdictions and by 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.

NSIR Service Agreement

As previously indicated in Section 2.1, clients are required to sign the appropriate NSIR Service Agreement, of which there are 2: one for submitters (data providers) and one for non-submitters (participating organizations). These agreements govern access to and use of NSIR and use and disclosure of NSIR data. They outline the obligations around access to NSIR data, as well as its security, use and disclosure. The service agreements are signed at a senior level in the organization to ensure that clients are aware of both their organizational responsibilities and the responsibilities of their users.

These service agreements contain a schedule that is specific to each client and sets out the terms and conditions under which de-identified record-level data and/or aggregate data generated by NSIR is accessed, used and disclosed. The terms and conditions set out in these agreements include, among other things,

- A requirement to immediately notify CIHI of any unauthorized use, access or other breach of confidentiality or security of which the client becomes aware; and
- A requirement to ensure that those authorized to access and use NSIR complete the NSIR training (e.g., NSIR demonstration, NSIR eLearning).

Compliance with the terms and conditions of the agreements is mandatory. Failure to uphold the terms and conditions could result in termination of access to NSIR data.

Health Information Standards and Specifications Agreement

Clients must sign a Health Information Standards and Specifications Agreement (including Schedule A — Product Terms and Conditions), which governs access to and use of CIHI's specifications, standards and other materials to develop the API software.

The Health Information Standards and Specifications Agreement also includes Schedule B — Notice of Termination of Product, which are forms for terminating use of the product that must be completed in accordance with Section 9. 2 of the agreement.

3.3 Principle 1: Accountability for de-identified NSIR data

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 NSIR data in terms of privacy and security risk management:

Table 3 Key positions and responsibilities

Position/group	Roles/responsibilities
Vice president, Data Strategies and Statistics	Responsible for the overall operations and strategic direction of NSIR
Director, Pharmaceuticals and Health Workforce Information Services	Accountable for NSIR and responsible for strategic and operational decisions about NSIR
Manager, Pharmaceuticals	Responsible for ongoing management, development and deployment of NSIR, and chair of the NSIR Advisory Committee
NSIR Advisory Committee	Responsible for providing input and advice to facilitate the ongoing management of and enhancements to NSIR
Vice president and chief information officer, Information Technology and Services	Responsible for the strategic direction and overall operations and implementation of CIHI's technological and security solutions
Chief information security officer	Responsible for the strategic direction and overall implementation of CIHI's Information Security Program
Executive director, chief privacy officer and general counsel, Office of the Chief Privacy Officer and Legal Services	Responsible for the strategic direction and overall implementation of CIHI's Privacy Program

3.4 Principle 2: Identifying purposes for de-identified NSIR data

NSIR supports the secure and anonymous collection, sharing and analysis of incidents occurring in Canadian health care facilities. The aim is to reduce the occurrence of harmful incidents by helping to identify how incidents occurred and how similar incidents may be prevented. These intended purposes and the scope of NSIR are clearly identified in this PIA (see [Section 2.1](#)), in NSIR reports and bulletins and on CIHI's website (cihi.ca).

3.5 Principle 3: Consent for the collection, use or disclosure of de-identified NSIR data

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 de-identified NSIR data

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 or monitoring of the health care system.

CIHI limits the collection of data to that which is necessary to achieve the purposes and goals of NSIR. The NSIR MDS and NSIR-RT MDS (see [Table 1](#) and [appendices A and B](#)) were developed in collaboration with an extensive network of experts. For patients/residents, month and year of birth and sex are optional data elements to collect, and they can be used to group incidents by patient/resident demographics. For health care providers, job role (e.g., registered nurse, radiation therapist) is also optional and can be used to group incidents by the role of the individuals involved in the incident.

From a privacy perspective, NSIR is designed to securely and anonymously collect, share, analyze and discuss incidents without disclosing the identity of any individual. It does not include the collection of direct identifiers (e.g., patient-/resident-identifiable information such as name, health card number, chart number or date of admission or discharge; provider-identifiable information such as name or registration number).

The only possible source of patient, provider or facility identifiers would be in one of the following NSIR free-text fields (for more details, see [Section 2.3](#)):

Medication incident reporting

- Description of Incident
- Future Strategies/Recommendations
- Actions/Circumstances That Prevented Harm
- Special Drug Product Name
- Drug Product Batch/Lot Number

RT incident reporting

- Description of Incident

3.7 Principle 5: Limiting use, disclosure and retention of de-identified NSIR data

Limiting use

The NSIR Service Agreement restricts use of the data to non-commercial purposes limited to the client's internal *incident analysis, data submission and related patient safety activities*.

Clients

CIHI limits the use of NSIR data to authorized purposes, as described in [Section 3.4](#). These include comparative analyses within and among jurisdictions; trend analyses to assess/monitor the impact of differences in policy, practices and service delivery; and production of statistics to support planning, management and quality improvement.

CIHI staff

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. 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.

Staff access to the SAS analytical environment is provided through CIHI's centralized SAS data access process managed through CIHI's Service Desk. This environment is a separate, secure space for the storage of general use data and other analytical data files, where staff can conduct and store the outputs from their analytical work. The general use data files are pre-processed files that are designed specifically to support internal analytical users' needs; the pre-processing includes removing personal health information (e.g., unencrypted health care number) and privacy-sensitive variables (e.g., date of birth, full postal code), which are replaced by a set of standard derived variables (e.g., patient's full birth date is removed and a derived age variable is added).

The process ensures that all requests for access, including access to the NSIR data, are traceable and authorized, in compliance with Section 10 of CIHI's [Privacy Policy, 2010](#). The SAS data access process is subject to an annual audit to ensure that staff are accessing data on a need-to-know basis. [Section 3.9](#) includes additional information about how the various procedural and technical measures are deployed to prevent unauthorized access and to otherwise secure the NSIR data.

Data linkage

NSIR data is de-identified and does not contain identifiers (e.g., name, health care [card] number) that allow for data linkages to be performed.

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 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). The return of own data is considered a use and not a disclosure.

CIHI may return NSIR data, as authorized, via NSIR, as described in [Section 2.3](#). CIHI routinely makes available to data providers data quality reports (e.g., submission reports) on the outcome of their data submissions to NSIR.

As stipulated in the NSIR Service Agreement, at their sole risk, data providers may disclose their own identifiable data in any manner they choose or otherwise forego the confidentiality of some or all of their data.

Limiting disclosure

NSIR data is not published by CIHI.

Third-party data requests

To date, NSIR has not processed any external third-party data requests. Any future requests will be considered on a case-by-case basis in accordance with CIHI's [Privacy Policy, 2010](#). Only CIHI may respond to third-party data requests; under the terms of the service agreements for data providers and non-submitters, those organizations must refer third-party requests to CIHI. If CIHI were to consider responding to a third-party data request, an assessment of the privacy risks would be undertaken and data would be disclosed in accordance with its [Privacy Policy, 2010](#) and through its Third-Party Data Request Program that contains and ensures appropriate privacy and security controls within the recipient organization.

Public release

As described in [Section 3.2](#), both submitters (data providers) and non-submitters (partner organizations) who enter into the appropriate NSIR Service Agreement have specified terms and conditions under which they can disclose NSIR data. Data providers and partner organizations are prohibited from disclosing incident records in any manner except as otherwise permitted under the agreement, as required by law or where express prior written authorization from the data provider has been obtained. The NSIR Service Agreement stipulates that among other things, except in the case of the client's own data, the client is not permitted to publicly report information, unless

- All reasonable attempts are employed to prevent the identification of any individual; and
- All reasonable attempts are employed to prevent the identification of any subscriber^{vii} or any province or territory, except where the subscriber has given the client written permission to publicly report that information; and
- CIHI's written permission has been obtained prior to disclosure.

Limiting retention

NSIR 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.

Clients are permitted to retain NSIR data and analytical products for as long as their agreement with CIHI is in effect. Data providers can retain their own data in accordance with their organization's own record retention policies.

vii. "Subscriber" means the client, a health facility, a provincial or territorial ministry or department of health, a regional health authority or any other organization or entity that has access to the service.

3.8 Principle 6: Accuracy of de-identified data

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, NSIR is subject to a data quality assessment on a regular basis, 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 NSIR data.

3.9 Principle 7: Safeguards for de-identified data

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 the NSIR 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 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 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 upon first receipt. In exceptional instances, staff will require access to original health care numbers. CIHI's internal *Privacy Policy and Procedures, 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 the 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 (cihi.ca).

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

The data in NSIR does not contain any personal health information (e.g., name, address, health card number) and therefore this section is not applicable.

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

This PIA summarizes CIHI's assessment of the privacy implications of NSIR. This assessment has been updated to include the application programming interface (API) submission method for submitting radiation treatment (RT) incidents via the RT module only.

No new risks were identified. The NSIR team will continue to apply the same rigorous data quality process to review all free-text fields for identifiers submitted in medication and RT records prior to making them accessible in the NSIR repository. Any changes to process or risk value resulting from reassessments of this nature are to be included in CIHI's Privacy and Security Risk Register, as stated in the January 2018 version of the NSIR PIA.

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

Appendices

Appendix A: National System for Incident Reporting — Medication Minimum Data Set

Mandatory and optional data elements are specified based on the degree of harm of the medication incident.

M = Mandatory O = Optional n/a = Not applicable

Data element number	Data element name	Reportable circumstance	Near miss	None	Mild	Moderate	Severe	Death
1.0	Incident Impact							
1.1	Description of the Medication Incident	O	O	O	O	O	O	O
1.2	Degree of Harm	M	M	M	M	M	M	M
1.3	Potentially Severe Medication Incident	M	M	M	M	M	n/a	n/a
2.0	Incident Discovery							
2.1	Functional Area(s)	M	M	M	M	M	M	M
2.2	Ward/Unit	O	O	O	O	O	O	O
2.3	Date Incident Was Detected	M	M	M	M	M	M	M
2.4	Time Incident Was Detected	O	M	M	M	M	M	M
2.5	Time Period When Incident Was Detected		(1) [†]	(1) [†]	(1) [†]	(1) [†]	(1) [†]	(1) [†]
2.6	Date Incident Occurred	n/a	O	O	O	O	O	O
2.7	Time Incident Occurred	n/a	O	O	O	O	O	O
2.8	Time Period When Incident Occurred		(1) [†]	(1) [†]	(1) [†]	(1) [†]	(1) [†]	(1) [†]
2.9	Health Care Provider(s) and/or Others Who Detected Incident	O	O	O	O	O	O	O
2.10	Health Care Provider(s) and/or Others Who Were Involved in Incident	O	O	O	O	O	O	O
3.0	Patient/Resident Characteristics							
3.1	Month and Year of Birth	n/a	O	O	O	O	O	O
3.2	Patient/Resident Sex	n/a	O	O	O	O	O	O

Data element number	Data element name	Reportable circumstance	Near miss	None	Mild	Moderate	Severe	Death
4.0	Medication Incident Details							
4.1	Medication/IV Fluid Use Process [†]	M	M	M	M	M	M	M
4.2	Medication/IV Fluid Problem [†]	M	M	M	M	M	M	M
4.3	Repeated Administrations	n/a	n/a	O	O	O	O	O
4.4	Contributing Factor(s) [†]	M	M	M	M	M	M	M
4.5	Chemotherapy Regimen	O	O	O	O	O	O	O
5.0	Drug Product Information							
5.1	Type of Drug Product	*	M	M	M	M	M	M
5.2	Drug Identification Number (DIN)	Note Only 1 value for data elements 5.2 to 5.5 is required.						
5.3	Generic Name of Drug Product							
5.4	Brand Name of Drug Product							
5.5	Special Drug Product Name							
5.6	Correct or Incorrect Drug Product	*	*	*	*	*	*	*
5.7	Dosage Form	O	O	O	O	O	O	O
5.8	Incorrect Dosage Form	*	*	*	*	*	*	*
5.9	Strength	O	O	O	O	O	O	O
5.10	Route of Administration	O	O	O	O	O	O	O
5.11	Incorrect Route of Administration	*	*	*	*	*	*	*
5.12	Batch Number/Lot Number	O	O	O	O	O	O	O
6.0	Investigation and Findings							
6.1	Patient/Resident Informed of Incident	n/a	O	O	O	O	O	O
6.2	Likelihood of Recurrence	O	O	O	O	O	O	O
6.3	Intervention(s) Required	n/a	n/a	O	O	O	O	O
6.4	Extended Length of Stay	n/a	n/a	n/a	O	O	O	O
6.5	Unplanned Admission/Readmission	n/a	n/a	n/a	O	O	O	O
6.6	Root Cause Analysis Status	n/a	O	O	O	O	O	O
6.7	Future Strategies/Recommendations	O	O	O	O	O	O	O
6.8	Actions or Circumstances That Prevented Harm	O	O	O	n/a	n/a	n/a	n/a

Data element number	Data element name	Reportable circumstance	Near miss	None	Mild	Moderate	Severe	Death
7.0	Unique Identifiers							
7.1	NSIR Case Identifier	CIHI assigned						
7.2	HCF Case Record Number	O	O	O	O	O	O	O
7.3	HCF Unique Identifier	CIHI assigned						
8.0	HCF Service Profile							
8.1	Principal Type of Health Care Provided	Mandatory						
8.2	Type of Setting	Mandatory						
8.3	Number of Beds Staffed and In Operation	Mandatory						
8.4	Type of Drug Distribution System	Mandatory						
8.5	Computerized Prescriber Order Entry	Mandatory						

Notes

* The requirement of the data elements (mandatory versus not applicable or optional) is based on the selection of Medication/IV Fluid Problem.

† Only 1 value is required.

‡ Adapted from MEDMARX®, © 2005 The United States Pharmacopeial Convention, Inc. All rights reserved. Used with permission.

Appendix B: National System for Incident Reporting — Radiation Treatment Minimum Data Set

Mandatory and optional data elements are specified based on whether it is an actual incident, a near miss or a programmatic hazard.

M = Mandatory O = Optional n/a = Not applicable

Data element number	Data element name	Programmatic hazard	Near miss	Actual incident (all known values)
1.0	Incident Impact			
1.1	Incident Description	M	M	M
1.2	Type of Radiation Treatment Incident	M	M	M
1.3	Acute Medical Harm	n/a	n/a	M
1.4	Dosimetric Impact	n/a	n/a	M
1.5	Latent Medical Harm	n/a	n/a	M*
2.0	Incident Discovery			
2.1	Functional Work Area	M	M	M
2.2	Date Incident Was Detected	M	M	M
2.3	Date Incident Occurred	n/a	O	O
2.4 and 2.5	Time or Time Period Incident Was Detected	M	M	M
2.6 and 2.7	Time or Time Period the Incident Occurred	O	O	O
2.8	Health Care Provider(s) and/or Other Individual(s) Who Detected the Incident	O	O	O
2.9	Health Care Provider(s) and/or Other Individual(s) Involved in the Incident	O	O	O
3.0	Patient Characteristics			
3.1	Patient Month of Birth	n/a	O	O
3.2	Patient Year of Birth	n/a	O	O
3.3	Patient Gender	n/a	O	M
3.4	Diagnosis Relevant to Treatment	n/a	M	M
4.0	Incident Details			
4.1	Process Step Where Incident Occurred	M	M	M
4.2	Process Step Where Incident Was Detected	M	M	M
4.3	Primary Problem Type	M	M	M
4.4	Contributing Factors	M	M	M
4.5	Number of Patients Affected	n/a	n/a	M

Data element number	Data element name	Programmatic hazard	Near miss	Actual incident (all known values)
5.0	Treatment Delivery			
5.1	Radiation Treatment Technique(s)	M	M	M
5.2	Total Dose Prescribed	n/a	M	M
5.3	Number of Fractions Prescribed	n/a	M	M
5.4	Number of Fractions Delivered Incorrectly	n/a	n/a	M
5.5	Hardware Manufacturer and Model Involved	O	O	O
5.6	Software Manufacturer and Model Involved	O	O	O
5.7	Body Region(s) Treated	n/a	O	M
5.8	Treatment Intent	n/a	O	O
6.0	Incident Investigation			
6.1	Immediate Ameliorating Actions	O	M	M
6.2	Safety Barrier(s) That Failed to Identify the Incident	O	M	M
6.3	Safety Barrier(s) That Identified the Incident	O	M	n/a
6.4	Actions Taken or Planned to Reduce Risk, and Other Recommendations	O	O	O
7.0	Unique Identifiers			
7.1	NSIR Case Identifier	System generated	System generated	System generated
7.2	HCF Case Record Number	O	O	O
7.3	HCF Unique Identifier	n/a	n/a	n/a
8.0	HCF Service Profile			
8.1	Principal Type of Health Care Provided	n/a	n/a	n/a
8.2	Type of Setting	n/a	n/a	n/a
8.3	Number of Beds Staffed and in Operation	n/a	n/a	n/a
8.4	Type of Drug Distribution System	n/a	n/a	n/a
8.5	Computerized Prescriber Order Entry	n/a	n/a	n/a

Note

* Not applicable when Acute Medical Harm is death or Dosimetric Impact is none.

Appendix C: Text alternative for images

Text alternative for Figure 1: NSIR timeline

This timeline extends from 2010 to 2020. It highlights key milestones in the development of NSIR and NSIR-RT. In 2010, NSIR launched its system to acute care hospitals to collect medication incidents. In 2011, NSIR expanded its scope to include long-term care facilities. In 2012, NSIR made enhancements to its system and its medication incident minimum data set (MDS) to include the collection of chemotherapy information. In 2013, NSIR met a significant system development milestone with the launch of batch upload functionality. In 2014, the NSIR Reporting Tool was upgraded to incorporate changes to the MDS and to assist in data submissions. In 2015, NSIR expanded its scope of incident collection to radiation treatment with the development of an NSIR-RT MDS and system module. In 2017, the NSIR-RT module was officially launched, and in 2020 the API submission method for the RT module was implemented.

**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

12660-0522

