National System for Incident Reporting

A component of the Canadian Medication Incident Reporting and Prevention System

Privacy Impact Assessment

Toronto, March 2026

Institute for Safe Medication Practices Canada

The Institute for Safe Medication Practices Canada (ISMP Canada) is a national, independent, and not-for-profit organization that purposefully partners with organizations, practitioners, consumers, and caregivers to advance medication safety in all healthcare settings. Our team of experts analyze reports of medication errors from across the country and provide resources, education, and consulting services to improve medication safety. guide

We analyze reports of medication errors and other issues so we can learn about the risks related to medications and collaboratively develop strategies to address them. We share lessons learned, including compelling actionable, evidence-informed recommendations that organizations, practitioners, consumers, and caregivers can use to reduce the risks related to medications. We partner to implement, sustain, and evaluate medication safety improvements in practice.

Additional information about ISMP Canada, and its products and services, is available at www.ismpcanada.ca

Purposeful Partnerships

Focus & Impact

Data Driven

Production of this document is made possible by financial contributions from Health Canada, and with input from the Canadian Institute for Health Information. The views expressed herein do not necessarily represent the views of Health Canada or of the Canadian Institute for Health Information.

Institute for Safe Medication Practices Canada
4711 Yonge Street
Suite 706
Toronto ON
M2N 6K8

Telephone: 416-733-3131 or toll free 1-866-544-7672
Fax: 416-733-1146
www.ismpcanada.ca
info@ismpcanada.ca

How to cite this document:

Institute for Safe Medication Practices Canada. National System for Incident Reporting Privacy Impact Assessment, March 2026. Toronto, ON: ISMP Canada, 2026.

Quick facts about the National System for Incident Reporting

1. NSIR was officially launched in 2010 by the Canadian Institute for Health Information (CIHI). 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.
2. On November 13, 2025, CIHI and ISMP Canada announced the transition of the management and operations of the NSIR to ISMP Canada by March 2026. The transition includes both the medication and radiation treatment (NSIR-RT) reporting programs.
3. Incidents are, by definition, preventable events. 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. NSIR Data and related analyses inform quality improvement activities at local, regional, provincial, territorial and national levels to foster improvements in health care delivery.
4. While NSIR Data does not include personal health information or identifiable information, ISMP Canada is committed to protecting the privacy, confidentiality, and security of information with which it is entrusted in order to carry out its mandate.
5. The 2 types of NSIR users are submitters (Data Providers/Participating Organizations) and non-submitters (Partner Organizations); they are collectively referred to as Clients (see the Definitions section).
6. Submitters (Data Providers/Participating Organizations) include Participating Organizations that submit and analyze NSIR Data according to their signed NSIR Data Sharing and Service Agreements for Submitters.
7. Non-Submitters (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.
8. 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).
9. Submitters electronically send 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.

10. De-identified Incident Records released to the NSIR repository can be accessed via a business intelligence tool (i.e., Microsoft Power BI) that allows Designated users, including submitters and non-submitters, to build template reports that can be customized to some extent.

11. ISMP Canada depends on the individuals and institutions to report information that is as accurate, complete, and up-to-date as possible. In cases where ISMP Canada has questions about the accuracy of the information it receives, it will contact reporters for follow-up, if possible.

12. NSIR Data is governed by ISMP Canada's Privacy Policy, 2026, by applicable legislation in the jurisdictions and by NSIR Agreements.

13. In some jurisdictions, an NSIR Provincial/Territorial agreement outlines jurisdictional support for submission of data to NSIR. These jurisdictional agreements are signed at the ministry or other level in the jurisdiction.

14. Clients are required to sign the appropriate agreement, of which there are 2:
    - NSIR Data Sharing and Service Agreement for Submitters: for submitters (Data Providers/ Participating Organizations) and
    - NSIR Service Agreement for Non-Submitters: for non-submitters (Partner Organizations).

    These agreements govern access to and use of NSIR and use and disclosure of NSIR data.

15. NSIR is part of the multi-organizational Canadian Medication Incident Reporting and Prevention System (CMIRPS) initiative, which contributes information, tools and expertise toward the prevention of harmful Medication Incidents.

16. The NSIR-RT Advisory Committee and the Canadian Association of Provincial Cancer Agencies are key collaborators for RT incident reporting.

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 Data Sharing and Service Agreement for Submitters (Data Providers/Participating Organizations), or in the NSIR Service Agreement for Non-Submitters (Partner Organizations), 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 reports of incidents to ISMP Canada.

Incident Record means record-level data related to reports of medication or RT incidents provided to ISMP Canada 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 reports of Medication and/or RT incidents (Incident Records) that were originally provided to ISMP Canada by a submitter for the purposes of NSIR.

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

Participating Organization means an organization that has entered into an NSIR Data Sharing and Service Agreement for Submitters that provides reports of incidents to ISMP Canada.

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 Institute for Safe Medication Practices Canada (ISMP Canada) is a national, independent, and not-for-profit organization that purposefully partners with organizations, practitioners, consumers, and caregivers to advance medication safety in all healthcare settings.

Learn. We synthesize knowledge by collecting, aggregating, and analyzing data on medication safety from practitioners, consumers, caregivers, and others

Share. We disseminate lessons learned with compelling, actionable, evidence-informed recommendations across the health system.

Act. We partner to implement, sustain, and evaluate medication safety improvements in practice

While NSIR Data does not include personal health information or identifiable information, ISMP Canada is committed to protecting the privacy, confidentiality, and security of information with which it is entrusted in order to carry out its mandate. 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). 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.

2. Background

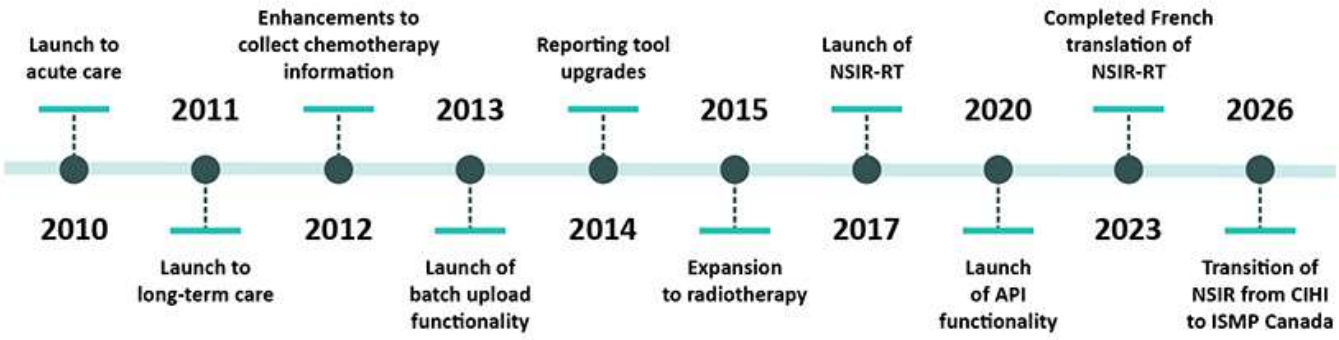
Incidents are, by definition, preventable events. NSIR aims to identify how incidents occur in Canadian health care facilities and how similar incidents may be prevented. NSIR is a voluntary reporting system designed to securely and anonymously support the collection, sharing and analysis of standardized incident data. Anonymized reporting encourages participation and protects the identity of patients, providers and facilities who participate in NSIR. NSIR Data and related analyses inform quality improvement activities at local, regional, provincial, territorial and national levels to foster improvements in health care delivery.

2.1. Introduction to NSIR

NSIR was officially launched in 2010 by the Canadian Institute for Health Information (CIHI). 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.

On November 13, 2025, CIHI and ISMP Canada announced the transition of the management and operations of the NSIR to ISMP Canada by March 2026. The transition includes both the medication and radiation treatment (NSIR-RT) reporting programs.

Figure 1 **NSIR timeline**



NSIR is part of the Canadian Medication Incident Reporting and Prevention System (CMIRPS) which contributes information, tools and expertise to the prevention of harmful medication incidents.

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 NSIR-RT Advisory Committee and the Canadian Association of Provincial Cancer Agencies are key collaborators for RT incident reporting.

The 2 types of NSIR users are submitters (Data Providers/Participating Organizations) and non-submitters (Partner Organizations); they are collectively referred to as Clients (see the Definitions section).

- Submitters (data providers/Participating Organizations) include Participating Organizations that submit and analyze NSIR Data according to their signed NSIR Data Sharing and Service Agreements for Submitters.
- Non-Submitters (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.

Clients of NSIR include the following:

Submitters (Data Providers/Participating Organizations)

- 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)

Non-Submitters (Partner Organizations)

- Health Canada (Marketed Health Products Directorate)
- Saskatchewan Ministry of Health
- Ontario Ministry of Health
- Ontario Health
- Canadian Association of Provincial Cancer Agencies

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

Submitters electronically send 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.

Submitters use the Reporting Tool to send 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 (i.e., Microsoft Power BI) that allows Designated users, including submitters and non-submitters, 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 submitter 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 submitters. Messages sent by submitters 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.

ISMP Canada 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 (MDS)**

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

2.3. Access management, data submission and flow for NSIR

NSIR is designed to support learning and sharing, and anonymity of submitters 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 submitters (medication and RT incidents) and non-submitters.

Access management for Submitters (Data Providers/Participating Organizations)

- ✓ An NSIR Data Sharing and Service Agreement for Submitters identifies the Organizational Contact(s)
- ✓ Organizational contacts are invited by ISMP Canada staff to self-register using Microsoft EntraID. The registration is validated and approved by ISMP Canada staff.
- ✓ Organization contacts in a healthcare facility can invite staff from their healthcare facility to self-register as a Data Submitter. Data Submitters are validated and approved by the Organizational Contact.
- ✓ Secure processes are developed by ISMP Canada to manage, monitor, and revoke access.

System registration for use of an API

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

Submitters or their authorized software vendors are required to sign ISMP Canada's Data Submission Protocol Agreement which governs the access to and use of the API and related products[i] (see also Section 3.2). Submitters 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 ISMP Canada, a representative of the submitter or their authorized software vendor must create an ISMP Canada profile. ISMP Canada 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 by ISMP Canada, data flows directly from the submitter's system repository or the submitter's authorized software vendor application to ISMP Canada's NSIR system.

---

i. "Products" means the ISMP Canada 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.

Access management for Non-Submitters (Partner Organizations)

- ✓ A Service Agreement for Non-Submitters identifies Organizational Contact(s)
- ✓ Organizational contacts are invited by ISMP Canada staff to self-register using Microsoft EntraID. The registration is validated and approved by ISMP Canada staff.
- ✓ Secure processes are developed by ISMP Canada to manage, monitor, and revoke access.

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			
	Submitter (Data Provider - source facility)	Submitter (Data Provider -non-source facility)	ISMP Canada (NSIR team)	Non-Submitter (Partner Organization)
Stage 1: Pre-submission (draft) *Single-incident processing:* Incident Records are entered in NSIR but not submitted. *Batch or API submission:* Incident Records reside in the submitter's incident reporting system. No records have been extracted via the batch upload or API methods.	Yes	No	No	No
Stage 2: Submitted (under review) Incident Records have been submitted via • Single-incident submission; • Batch upload; or • API. Incident Records undergo 2-step data quality processing: Step 1: Automated review of codified data. Step 2: Manual review of free-text fields.	Yes	No	Yes	No
Stage 3: Complete (final)	Yes	Yes	Yes	Yes

Stage/condition of records	Access by user's affiliation			
	Submitter (Data Provider - source facility)	Submitter (Data Provider -non-source facility)	ISMP Canada (NSIR team)	Non-Submitter (Partner Organization)
2-step data quality processing is complete and all issues have been corrected. Incident Records are confirmed as de-identified and released into the NSIR repository for analysis and reporting. Users are able to drill down from aggregate totals to individual de-identified incident Records.		Reports are anonymous and do not identify the source facilities		Reports are anonymous and do not identify the source facilities

Data flows

In NSIR, each record is a single incident. 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 report of the incident (NSIR Incident Record) is sent from a submitter to ISMP Canada. Data is submitted 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 submitter'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 submitters 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 submitters by way of a submission report via the batch or API method. Corrections made by submitters 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 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 submitter.

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.

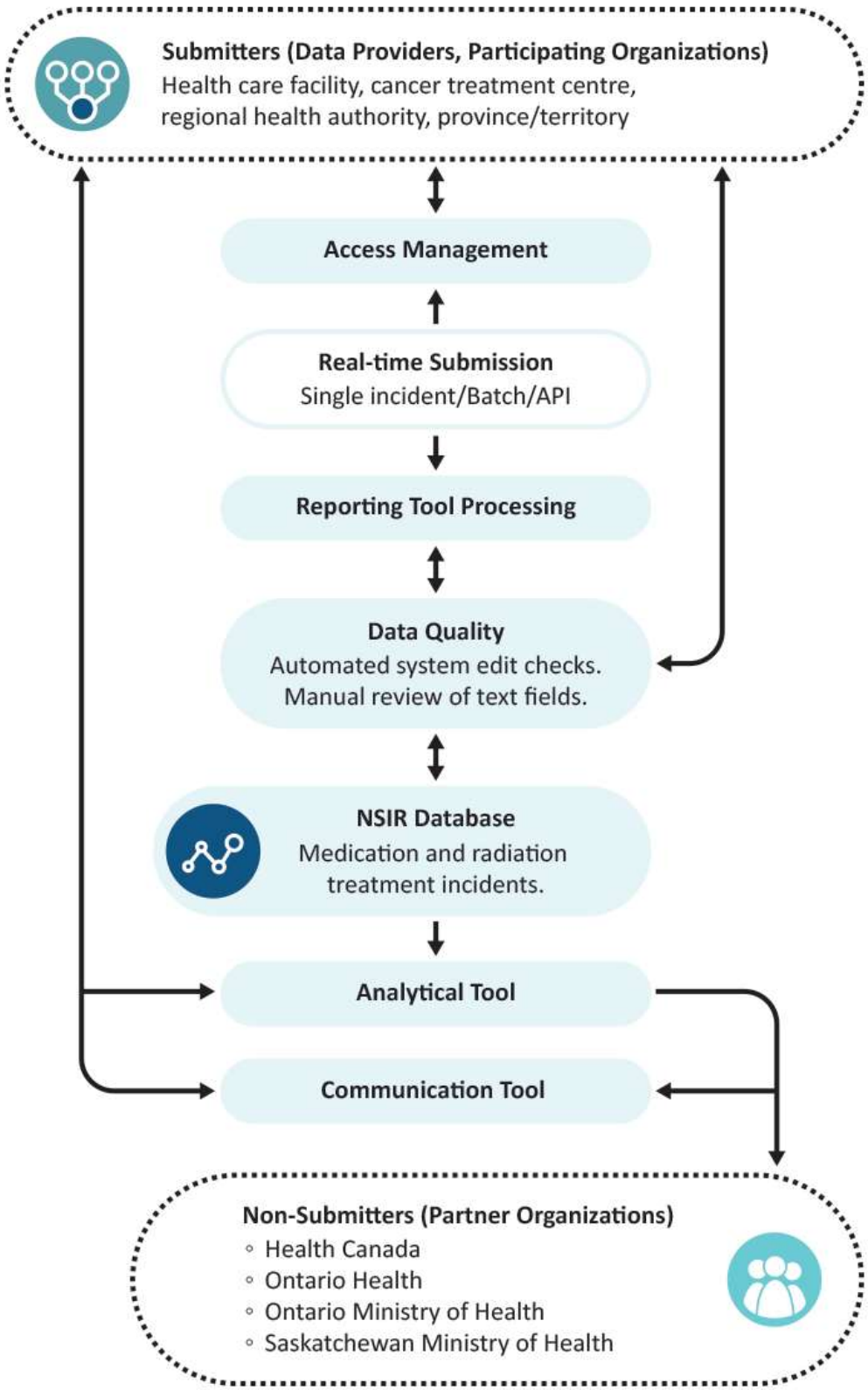
If any issues are discovered, the Incident Records are returned to submitters for correction. The record is suppressed until the submitter makes the correction (i.e., removes the identifier). Once the correction has been confirmed by NSIR staff, these Incident Records are deemed to be de-identified and 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 submitters to establish the level of monitoring required for free-text fields. This depends in large part on the submitter'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 ISMP Canada's data quality review process will be determined together with the submitter 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 and updates the process for reviewing free-text fields on a regular basis.

Copies of ISMP Canada data and applications are retained on backup systems.

All the NSIR Data flows are highlighted in Figure 2.

Figure 2 Overview of NSIR Data flow



3. Privacy analysis

3.1. Enterprise Risk Management Program

ISMP Canada has an Enterprise Risk Management (ERM) Program.

Where privacy and/or security risks to the organization are identified, they are entered into the ERM Risk Register Report and categorized as **high**, **medium** or **low**, based on the likelihood and impact of a risk event.

3.2. Authorities governing NSIR data

General

NSIR Data does not include personal health information and, therefore, is not subject to privacy legislation.

One of the guiding principles for the development of NSIR is the 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).

At ISMP Canada, NSIR Data is governed by ISMP Canada's Privacy Policy, 2026, by applicable legislation in the jurisdictions and by NSIR Agreements.

NSIR Agreements

NSIR Provincial/Territorial Agreements

In some jurisdictions, an NSIR Provincial/Territorial agreement outlines jurisdictional support for submission of data to NSIR (e.g., in a Letter of Understanding). These jurisdictional agreements are signed at the ministry or other level in the jurisdiction.

NSIR Service Agreements

As previously indicated in Section 2.1, Clients are required to sign the appropriate Agreement, of which there are 2:

- **NSIR Data Sharing and Service Agreement for Submitters**: for submitters (Data Providers/ Participating Organizations) and

- **NSIR Service Agreement for Non-Submitters:** for non-submitters (Partner 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 agreements set 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 ISMP Canada 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 have received NSIR training (e.g., NSIR demonstration).

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.

Data Submission Protocol Agreement for Use of the API

Clients wishing to use the API for submission of data must sign a Data Submission Protocol Agreement which governs access to and use of ISMP Canada's specifications, standards and other materials for the API software.

3.3. Principle 1: Accountability for de-identified NSIR data

ISMP Canada's chief executive officer is accountable for ensuring compliance with ISMP Canada's *Privacy Policy, 2026*. ISMP Canada has a privacy officer and privacy officer delegate, a legal advisor, a Governance Committee of its Board of Directors, and engages external privacy consultants on an as-needed basis.

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
Chief Executive Officer	Responsible for implementing the strategic plan and overall implementation of ISMP Canada's Programs, including Privacy and Technology
Vice President, Operations and Privacy Officer	Responsible for the operations of NSIR and implementation of ISMP Canada's privacy program.
Director, NSIR	Responsible for ongoing management, development and deployment of NSIR, and chair of the NSIR Advisory Committees
NSIR Advisory Committees	Responsible for providing advice to facilitate the ongoing management of and enhancements to NSIR
Director, Information Technology	Responsible for the implementation of ISMP Canada's technological and security solutions

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 ISMP Canada's website (ismpcanada.ca).

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

ISMP Canada is a secondary collector of data and does not have direct contact with patients. ISMP Canada relies on submitters 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

ISMP Canada 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, age range and sex or gender 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 Data Sharing and Service Agreement for Submitters, and NSIR Service Agreement for Non-Submitters, restrict use of the data to non-commercial purposes limited to incident analysis, and related patient safety activities.

Clients

ISMP Canada 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.

ISMP Canada staff

ISMP Canada 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 ISMP Canada staff are required to sign a confidentiality agreement at the commencement of employment or engagement, and they are subsequently required to renew their commitment to privacy yearly.

Staff access to ISMP Canada's secure analytical environment is provided through ISMP Canada's data access process and controls. This environment is a separate, secure space for analytical data files, where staff are required to conduct and store the outputs from their analytical work. NSIR Data sets used for internal ISMP Canada analysis do not contain direct identifiers.

Section 3.9 includes additional information about how the various procedural and technical measures are deployed to prevent unauthorized access and to otherwise secure NSIR data.

Data linkage

ISMP Canada does not conduct data linkages within the NSIR data.

Return of Own Data

The return of Own Data is considered a use and not a disclosure.

As described in Section 2.3. , if any issues are discovered during manual data quality processing, the Incident Records are returned to submitters for correction.

Limiting disclosure

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 ISMP Canada's *Privacy Policy, 2026*. Only ISMP Canada may respond to third-party data requests; under the terms of the service agreements for submitters and non-submitters, those organizations must refer third-party requests to ISMP Canada. If ISMP Canada 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, 2026 and* appropriate privacy and security controls within the recipient organization.

Public release by submitters and non-submitters

As described in Section 3.2, both submitters (Data Providers/Participating Organizations) and non-submitters (Partner Organizations) who enter into the appropriate NSIR agreement have specified terms and conditions under which they can disclose NSIR data. Submitters and non-submitters 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 submitter has been obtained. The NSIR agreements stipulate 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 client, health facility, provincial or territorial ministry or department of health, regional health authority or any other organization or entity that has access to the service, except when Client written permission has been given to publicly report that information; and
- ISMP Canada's written permission has been obtained prior to disclosure.

Limiting retention

NSIR forms part of ISMP Canada'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 ISMP Canada is in effect. Submitters can retain their Own Data in accordance with their organization's own record retention policies.

3.8. Principle 6: Accuracy of de-identified data

Similar to other ISMP Canada data holdings, NSIR is subject to a data quality assessment on a regular basis. ISMP Canada depends on the individuals and institutions to report information that is as accurate, complete, and up-to-date as possible. In cases where ISMP Canada has questions about the accuracy of the information it receives, it will contact reporters for follow-up, if possible.

3.9. Principle 7: Safeguards for de-identified data

Key aspects of ISMP Canada's system security with respect to the NSIR Data are highlighted below.

System security

ISMP Canada 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, ISMP Canada has policies that specify the necessary controls for the protection of information in both physical and electronic formats. The policies and associated operating procedures reflect reasonable industry standard efforts in privacy, information security and records management for the protection of the confidentiality, integrity and availability of ISMP Canada's information assets.

Analysis at ISMP Canada is generally conducted with the use of deidentified record-level data. For a record to be considered deidentified, modifications include the removal of direct personal identifiers and the replacement of high-risk indirect personal identifiers (e.g., date of birth) with derived variables (e.g., age range). ISMP Canada's internal privacy procedures set 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.

ISMP Canada is committed to safeguarding its data holdings and protecting information with administrative, physical and technical security safeguards appropriate to the sensitivity of the information.

An important component of ISMP Canada's information security is regular third-party vulnerability assessments and penetration tests of its infrastructure and selected applications. All recommendations resulting from third-party audits are shared with the ISMP Canada leadership team, and action is taken accordingly.

3.10. Principle 8: Openness about the management of personal health information and de-identified data

ISMP Canada makes information available about its privacy policies, data practices and programs relating to the management of data. Specifically, ISMP Canada's *Privacy Policy, 2026 is* available to the public on ismpcanada.ca.

3.11. Principle 9: Access to 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. For further information, see ISMP Canada's *Privacy Policy, 2026*.

3.12. Principle 10: Challenging Compliance with ISMP Canada's Privacy Policy and Practices

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. For further information, see ISMP Canada's Privacy Policy, 2026.

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

Domain	Data element number	Data element name	Reportable circumstance	Near miss	None	Mild	Moderate	Severe	Death
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
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 (1)†	M (1)†	M (1)†	M (1)†	M (1)†	M (1)†
	2.5	Time Period When Incident Was Detected	O	M (1)†	M (1)†	M (1)†	M (1)†	M (1)†	M (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

Domain	Data element number	Data element name	Reportable circumstance	Near miss	None	Mild	Moderate	Severe	Death
Incident Discovery (continued)				(1)†	(1)†	(1)†	(1)†	(1)†	(1)†
	2.8	Time Period When Incident Occurred	n/a	O (1)†	O (1)†	O (1)†	O (1)†	O (1)†	O (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
Patient/Resident Characteristics	3.1	Age Group	n/a	O	O	O	O	O	O
	3.2	Patient/Resident Sex	n/a	O	O	O	O	O	O
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
Drug Product Information	5.1	Type of Drug Product	*	M	M	M	M	M	M
	5.2	Drug Identification Number (DIN)	§	§	§	§	§	§	§
	5.3	Generic Name of Drug Product	§	§	§	§	§	§	§

Domain	Data element number	Data element name	Reportable circumstance	Near miss	None	Mild	Moderate	Severe	Death
	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
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

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

§ Only 1 value for data elements 5.2 to 5.5 is required.

n/a: Not applicable.

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

Domain	Data element number	Data element name	Programmatic hazard	Near miss	Actual incident (all known values)
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*
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
Patient Characteristics	3.1	Age Group	n/a	O	O
	3.2	Patient Gender	n/a	O	M
	3.3	Diagnosis Relevant to Treatment	n/a	M	M
Incident Details	4.1	Process Step Where Incident Occurred	M	M	M

Domain	Data element number	Data element name	Programmatic hazard	Near miss	Actual incident (all known values)
	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
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
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
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
	8.1	Principal Type of Health Care Provided	n/a	n/a	n/a

Domain	Data element number	Data element name	Programmatic hazard	Near miss	Actual incident (all known values)
HCF Service Profile	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

Notes

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

n/a: Not applicable.

Appendix C: Text alternative for images

Text alternative for Figure 1: NSIR timeline

This timeline extends from 2010 to 2023. 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. In 2020, the API submission method for the RT module was implemented, and in 2023 the French translation of NSIR-RT was completed. CIHI and ISMP Canada announced the transition of the management and operations of the NSIR to ISMP Canada by March 2026. The transition includes both the medication and radiation treatment (NSIR-RT) reporting programs.