Your Health System: Insight Privacy Impact Assessment (October 2015)
4.9 Principle 8: Openness about the management of personal health information........31
4.10 Principle 9: Individual access to, and amendment of, personal health information......31
4.11 Principle 10: Complaints about CIHI’s handling of personal health information........31
5 Privacy assessment summary and conclusion ...............................................................31
The Canadian Institute for Health Information (CIHI) is pleased to publish the following privacy impact assessment in accordance with its Privacy Impact Assessment Policy:

- Your Health System: Insight Privacy Impact Assessment, October 2015

Approved by:

Stephen O'Reilly
Executive Director,
Atlantic Canada and Integrated eReporting

Anne-Mari Phillips
Chief Privacy Officer &
General Counsel

Ottawa – October 2015
10 quick facts about Your Health System: Insight

1. Your Health System: Insight (YHS: Insight) builds on years of experience at the Canadian Institute for Health Information (CIHI) in reporting indicators and measures that support health systems in monitoring performance and managing the systems. It is the first product delivered under CIHI’s Integrated eReporting (IeR) approach.

2. YHS: Insight is an analytical, web-based tool in a secured private environment; it is not publicly accessible.

3. Clients must sign a service agreement with CIHI in order to use YHS: Insight. The service agreement limits clients’ rights to use and disclose information obtained through YHS: Insight.

4. The tool is used by clients (e.g., individual health care facilities, regional health authorities, participating provincial and territorial ministries/departments of health) to get quick, easy access to their results on key performance indicators, as well as the underlying data.

5. It offers clients access to open-year data, increased flexibility to understand performance drivers and pan-Canadian comparisons so they can understand what’s driving their performance, compare their results with others’ across Canada and improve their part of the health system.

6. The initial release of YHS: Insight contained clinical and administrative data from CIHI’s Clinical Administrative Databases (Discharge Abstract Database–Hospital Morbidity Database and National Ambulatory Care Reporting System). This data was collected in its original form through the administration of the health care system in the various jurisdictions and was provided to CIHI as a secondary user.

7. The aggregate data contained in YHS: Insight includes indicators and measures from the acute care setting that are reported at the facility level (by name), as well as at the regional, provincial and national levels, and that are available to all designated users.

8. A key feature of YHS: Insight is the automated return of record-level information, which is the contributing data used to build a particular indicator. This feature allows authorized designated users of clients that are data providers to reconcile their indicator results with their own locally held data, and to use the data to identify underlying factors that may be driving their results.

9. Data in YHS: Insight is refreshed monthly to support clients in monitoring their performance and progress in a timely manner.

10. YHS: Insight was designed in consultation with real users, so it has an intuitive design. Navigation is quick and simple; there are no deeply layered menus.
Definitions

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

**Aggregate data** means record-level data 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 that is specified in CIHI’s Secure Electronic Reporting Services Agreement and that is binding itself to comply with the terms of the service agreement.

**Designated user** means an employee or permitted contractor of a client who has been authorized by the client to access and use YHS: Insight.

**Data provider** means an organization, health care provider or other individual that discloses health information to CIHI. Data providers may include ministries of health, regional health authorities and similar bodies, hospitals and other health care facilities.

**Health facility–identifiable information** means information that directly identifies a health facility by name.

**Record-level data** means data in which each record is related to a single individual.

**Your Health System: Insight data** means any aggregate data and record-level data included in YHS: Insight.

**Contextual measures** refer to the additional information (e.g., number of acute care stays, average length of stay, percentage of alternate level of care days) that helps users explain or interpret the indicator results.
1 Introduction

The Canadian Institute for Health Information (CIHI) collects and analyzes information on health and health care in Canada. Its mandate is to lead the development and maintenance of comprehensive and integrated health information that enables sound policy and effective health system management that improve health and health care. 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 primary purpose of this privacy impact assessment (PIA) is to examine the privacy, confidentiality and security risks associated with CIHI’s Your Health System: Insight (YHS: Insight) tool. It includes a review of the 10 privacy principles set out in the Canadian Standards Association’s Model Code for the Protection of Personal Information. Because YHS: Insight is one of many analytical tools that will be developed under CIHI’s Integrated eReporting (IeR) initiative, this PIA also serves as a foundational PIA for IeR. IeR is a complex, multi-year and multi-stage initiative; thus IeR projects will receive additional PIAs to take into account further changes (e.g., design, new requirements, functionality). The primary driver for this PIA is compliance with CIHI’s Privacy Impact Assessment Policy.

2 Background

In keeping with CIHI’s history and commitment to provide clients and stakeholders with robust and user-friendly technology to access and report on information, CIHI has now invested in and embarked on a multi-year strategic IeR initiative. Under this initiative, CIHI will design an integrated suite of analytical web-based tools for health system data to meet the needs of its customers and stakeholders. IeR will significantly enhance stakeholders’ abilities to access, view, use and analyze information to address complex questions related to health care delivery and performance by bringing together information from multiple sources that has historically been maintained in separate data holdings. The long-term goal is to be able to provide health leaders with an integrated view of their health system.

YHS: Insight builds on CIHI’s years of experience in reporting indicators and measures that support health systems in monitoring performance and managing the systems. It is the first of many web-based tools that will be developed within CIHI’s IeR initiative and serves as a complement to CIHI’s public interactive web tool, Your Health System: In Depth, by providing authorized users with a deeper look at various standardized indicators and summary measures on health system performance.
3 Description of YHS: Insight and user community

3.1 Description of YHS: Insight

YHS: Insight is the first product delivered under the IeR approach that, as a whole, provides a seamless, targeted and integrated reporting experience for CIHI’s stakeholders to support the management of health systems. The tool was implemented in a restricted environment and offers authorized users

- A summary of health system performance and management measures at a glance through visualizations and a summary dashboard;
- Trends and pan-Canadian comparisons with customizable peer groups at the facility, regional, provincial/territorial and national levels;
- A breakdown of indicator results by relevant clinical and administrative data elements (e.g., admission category, triage level, sex, age); and
- The ability to save, print and export results.

Authorized designated users of clients that are data providers will have the added benefit of being able to

- Explore and unpack their indicators;
- Reconcile their indicator results with their own locally held data by allowing them to access and drill down to the underlying patient record-level data and factors that may be driving their results; and
- Save, print and export those results (see Figure 1).

For the initial implementation, YHS: Insight included 10 indicators and contextual measures for each participating hospital/health region. These indicators are grouped as follows and focus on measures from the acute care setting:

- 30-Day Overall Readmissions;
- 30-Day In-Hospital Mortality Following Major Surgery; and
- Emergency Department Wait Times.

In the future, CIHI plans to increase the number of indicators and measures to include those in other CIHI eReporting products.
3.2 Description of YHS: Insight user community

YHS: Insight targets decision-support managers, analysts and clinicians. Access is limited to 2 specific communities:

1. **Data providers** (i.e., those organizations that originally submitted data to CIHI) such as individual health care facilities, regional health authorities and participating provincial and territorial ministries/departments of health.

2. **Selected third-party organizations** that meet all of the following criteria:
   - The requester is a legally constituted organization that has a health care–related public mandate related to supporting the management of the health care system.
   - The requesting organization has expertise in managing record-level data, including appropriate privacy and security policies and processes.
   - The requesting organization is an accountable data custodian with a good track record.
   - The requesting organization is authorized under provincial/territorial legislation to access record-level data to deliver its legislative mandate, or the provincial/territorial ministry of health delegated a mandate (that would ideally include a data sharing agreement between them) to the requesting organization that requires access to record-level data.
The data to be accessed through YHS: Insight is required by the requesting organization to fulfill its mandate.

The ministry of health in the requesting organization’s province/territory supports its access to YHS: Insight.

Third parties wanting to access YHS: Insight must submit an application to CIHI’s executive director for Atlantic Canada and Integrated eReporting for approval. CIHI’s Executive Committee is then informed once approval has been granted.

Data providers and third-party organizations are collectively referred to as clients, which include the following:

- Health care facilities (e.g., hospitals)
- Regional health authorities
- Provincial/territorial ministries of health

- Health quality councils
- Local health integration networks

All clients must sign CIHI’s Secure Electronic Reporting Services Agreement to access YHS: Insight (see Section 4.1.1).

3.3 Description of data accessible through YHS: Insight

The initial release of YHS: Insight contained data from CIHI’s Clinical Administrative Databases (CAD). In future, YHS: Insight may expand to include data from other databases, such as the Ontario Mental Health Reporting System (OMHRS), Continuing Care Reporting System (CCRS) and Canadian MIS Database (CMDB). The purpose of YHS: Insight is to support ongoing quality improvement at the hospital, regional and provincial levels.

3.3.1 CIHI data

Clinical Administrative Databases

The CAD are composed of 2 separate pan-Canadian databases: the Discharge Abstract Database–Hospital Morbidity Database (DAD-HMDB) and the National Ambulatory Care Reporting System (NACRS). These databases contain patient demographic, diagnostic, intervention, other care delivery and administrative information about individual patients resulting from hospital inpatient acute separations, emergency department separations or outpatient (ambulatory care) separations (e.g., clinic, day surgery). YHS: Insight contains a subset of data from the CAD. While the CAD contain address information, full dates of birth, encrypted health card numbers of patients and health care provider numbers (identifiers), YHS: Insight does not. Neither the CAD nor YHS: Insight contains the names of patients or health care providers.
Discharge Abstract Database–Hospital Morbidity Database
The DAD-HMDB contains information on all acute care hospital inpatient and day surgery separations from certain provinces and territories and limited data from long-term care, rehabilitation and mental health facilities.

National Ambulatory Care Reporting System
NACRS contains clinical, administrative and demographic information for hospital-based and community-based ambulatory care, including day surgeries from certain provinces and territories, outpatient clinics and emergency departments.

The CAD’s PIA is available on CIHI’s website.

Health facility–identifiable information
YHS: Insight data includes information that directly identifies a health facility by name.

Aggregate data
Indicator results and contextual measures reported at the facility level (by name), as well as at the provincial and national levels, that are available to all users include but are not limited to rates (e.g., adjusted rate, crude rate) and numerator and denominator counts that may include small cell counts. As many as 15 different factors (e.g., age group, sex, triage level, Case Mix Group, main patient service) can be explored, which can include breakdowns by age and sex.

Record-level data
The record-level data contained in YHS: Insight is the contributing data used to build a particular indicator. It includes data elements such as the facility’s name and number and the patient’s chart number and admission and discharge dates.

For the purposes of this PIA, the record-level data contained in YHS: Insight is collectively considered personal health information because of the sensitive information it contains.

Termination of pregnancy data
Termination of pregnancy data for all provinces and territories is included in the calculation of all indicator results.
3.3.2 Overview of data flow for YHS: Insight

Selected records taken from existing CIHI databases\(^1\) (DAD-HMDB and NACRS) are used by CIHI to create an analytical source of truth (ASOT) within CIHI’s data warehouse to support the calculation of indicator results. Once selected, records are linked to create episodes of care for each patient. Indicator methodologies\(^2\) are then applied, and hierarchical information from the Organization Index (see Section 3.3.3) is used to calculate the indicator results at the facility, regional, provincial/territorial and national levels. The resulting processed data is loaded to the data marts that support the business intelligence tool upon which YHS: Insight is built.

When YHS: Insight launched in March 2015, indicators were available for the reporting period 2011–2012 (closed-year data) to 2014–2015 (open-year data). Indicator results are refreshed monthly.

Designated users log in to YHS: Insight through a secure web interface. Once logged in, users can

- Compare indicator results at the facility, regional, provincial/territorial and national levels;
- Break down indicator results by relevant clinical and administrative data elements (e.g., admission category, triage level, sex, age);
- View their indicator results in different ways, such as by adjusted rate and crude rate; and
- Save, print and export results.

Authorized designated users of clients that are data providers can access their own patient record-level data and factors that may be driving their results.

3.3.3 Supporting application: Organization Index

The Organization Index (OI) is a database that CIHI developed and maintains to

- Reconcile variability in organization information, such as organization names;
- Facilitate organizational linkage across data holdings;
- Track ongoing changes to organizations and their hierarchical relationships with each other; and
- Record changes to organizations over time.

YHS: Insight uses information from the OI as the basis for aggregating results in YHS: Insight to ensure accuracy of reporting at multiple levels (hospital, regional, provincial/territorial, national). For example, when there are multiple regional health authorities under a jurisdiction (e.g., province), the OI ensures that YHS: Insight data can be rolled

---

\(^1\) Other existing CIHI data sources used in calculating indicators include Case Mix Group+ (CMG+), CIHI’s inpatient grouping methodology designed to group patient data originating from the DAD; and Comprehensive Ambulatory Classification System (CACS), CIHI’s ambulatory grouping methodology designed to group ambulatory (e.g., emergency, day surgery, outpatient clinics originating from NACRS) and day surgery visit data from the DAD.

\(^2\) The responsibility for developing indicators rests with the relevant CIHI program area.
• Up to the level of the jurisdiction (e.g., province); or
• Down to the level of
  – Any regional health authority under the jurisdiction; or
  – Any single corporation under the regional health authority; or
  – Any health care facility under a corporation it owns and operates.

Figure 2  Data flow for YHS: Insight

Note
LHIN: Local health integration network.

3.4 Access to YHS: Insight

YHS: Insight is an interactive analytical tool for health system managers and analysts that supports them in understanding, monitoring and improving health care and their health care systems. All designated users will be able to access indicator results, but only authorized designated users of clients that are data providers can access the patient record-level data supporting each indicator.
3.4.1 Access management

The process of granting access permissions to YHS: Insight is a coordinated effort among participating organizations and CIHI’s Central Client Services (CCS) department, which manages access using established Access Management System (AMS) processes for granting and revoking access.

Key components

The key steps of the AMS process include the following:

- **Clients**
  - Enter into a service agreement with CIHI;
  - Assign a designated organization contact; and
  - Identify designated users to CIHI through the organization contact.

- **CCS** authenticates access requests from designated users by
  - Verifying that designated users are affiliated with the correct organization;
  - Contacting the appropriate organization contact to verify the designated user and obtain approval from the organization contact; and
  - Granting the appropriate access privileges following authentication.

For YHS: Insight, access will be managed in 2 streams: general access, and general and record-level access.

**General access**

This stream allows designated users to access aggregate indicator results containing health facility–identifiable information, view their indicator results in different ways (e.g., by adjusted rate, by crude rate) and see numerator and denominator counts that may include small cell sizes.

**General and record-level access**

This stream allows authorized designated users to access aggregate indicator results containing health facility–identifiable information, view their indicator results in different ways and access the patient record-level data supporting each indicator.

All designated users may be granted permission for general access. Authorized designated users of clients that are data providers may be granted permission for general and/or record-level access. The decision about which level of access is to be granted is made by the organization contact on behalf of the client. See Table 1 for an overview of who can access YHS: Insight data.
### Table 1  
Access options by user affiliation

<table>
<thead>
<tr>
<th>Type of data</th>
<th>General access</th>
<th>Access stream by user affiliation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Aggregate-level indicator results as well as the contextual measures</td>
<td>Third-party organizations</td>
</tr>
<tr>
<td>General access</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Access to own record-level data</td>
<td>Underlying patient record-level data that supports each indicator</td>
<td>—</td>
</tr>
</tbody>
</table>

### 4 Privacy analysis

#### 4.1 Authorities governing CIHI and YHS: Insight

**General**

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

**Legislation**

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

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

For provinces and territories that do not currently have health information–specific privacy legislation in place, facilities are governed by public-sector privacy legislation. This legislation authorizes facilities to disclose personal information for statistical purposes without an individual’s consent.

**Agreements**

As indicated above in Section 3.3.1, YHS: Insight contains data sourced from subsets of existing CIHI data holdings. This data flows directly to CIHI via existing applications/systems from data providers (e.g., hospitals, other health care facilities). These existing data flows are governed by CIHI’s *Privacy Policy, 2010*, legislation in the jurisdictions and existing data sharing agreements.
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.

4.1.1 CIHI’s Secure Electronic Reporting Services Agreement

To be able to use YHS: Insight, clients must sign CIHI’s Secure Electronic Reporting Services Agreement. The service agreement outlines obligations around access to YHS: Insight data, as well as security, use and disclosure. It is signed at a senior level in the organization to ensure that clients are aware of their organizational responsibilities and the responsibilities of their users. Compliance with the terms and conditions of the service agreement is mandatory. Failure to uphold the terms and conditions could result in termination of access to YHS: Insight data.

The terms and conditions set out in the service agreement include the following:

**Security, access, use and obligations**

- Clients are responsible for ensuring that users of YHS: Insight in their organizations are aware of and comply with the terms and conditions of the service agreement.
- Where possible, access to YHS: Insight will be done over the client’s network or the client’s facility’s network where the designated users are employed.
- Clients are responsible for facilitating access to and use of YHS: Insight and YHS: Insight data through the organization contact.
- Organization contacts, on behalf of the client, are responsible for providing CIHI with accurate and current registration information, including any changes (e.g., termination of employment) to the designated users.
- Clients
  - Must ensure that designated users successfully complete any applicable educational and training required by CIHI;
  - Are permitted to access and use YHS: Insight data solely for non-commercial purposes that are limited to the client’s internal management, data quality, planning, research, analysis or evidence-based decision-support activities;
  - Must ensure that designated users do not disclose usernames and passwords to any person or entity for any reason; and
  - Must immediately notify CIHI of any
    - Actual or potential unauthorized use of usernames and passwords; and
    - Breach or potential breach of the service agreement that comes to their attention.
- Except in the case of the client’s own data, clients are prohibited from using YHS: Insight data or other information to attempt to identify an individual.
Public reporting

- Except in the case of a client’s own data, a client is permitted to publicly report information obtained from YHS: Insight only if certain conditions are met, such as the following:
  - Prior to the disclosure, the client has obtained written permission from each health facility identified in the information to be reported;
  - The information does not contain cell sizes with fewer than 5 observations;
  - All reasonable steps have been taken to prevent identification of individuals; and
  - When the information is an indicator or rate, the client
    o Uses caution when the number of cases in the denominator is low (i.e., the rate is unstable) and avoids reporting the indicator or rate publicly; and
    o Includes the statement “interpret with caution” when the number of cases in the denominator is less than 50.

4.1.2 Terms and conditions of use

In addition to signing the service agreement, designated users are required to agree to the terms and conditions of use that appear each time they log in to YHS: Insight prior to accessing any data. The terms and conditions of use include obligations such as

- Accessing YHS: Insight only as long as they are authorized users designated by the organization contact in their organization;
- Immediately informing the organization contact in their organization when they no longer require or are no longer entitled to access YHS: Insight;
- Not sharing or transferring their user profiles, usernames or passwords;
- Accessing YHS: Insight only as stipulated in the service agreement between their organization and CIHI;
- Logging out of YHS: Insight after each session; and
- Informing their organization of any breach or potential breach of the terms and conditions.

4.2 Principle 1: Accountability for personal health information

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

YHS: Insight clients are accountable for the application of the service agreement within their respective organizations. They are also subject to the requirements of data protection laws in their respective jurisdictions and the independent oversight of privacy commissioners or their equivalents.
4.2.1 Organization and governance

CIHI’s IeR was established as a program area in April 2013, reporting to the executive director of Atlantic Canada and Integrated eReporting.

The following table identifies key internal positions with responsibilities for YHS: Insight in terms of privacy and security risk management.

<table>
<thead>
<tr>
<th>Position/group</th>
<th>Role/responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive director, Atlantic Canada and Integrated eReporting</td>
<td>Responsible for the overall operation and strategic direction of CIHI’s IeR services</td>
</tr>
<tr>
<td>Performance Reporting and Digital Analytics Steering Committee</td>
<td>Responsible for strategic recommendations and decisions about the direction of CIHI’s IeR program</td>
</tr>
<tr>
<td>Information Management Steering Committee</td>
<td>Responsible for strategic recommendations and decisions related to technology</td>
</tr>
<tr>
<td>Chief privacy officer and general counsel</td>
<td>Responsible for the strategic direction and overall implementation of CIHI’s Privacy Program</td>
</tr>
<tr>
<td>Chief information security officer</td>
<td>Responsible for the strategic direction and overall implementation of CIHI’s Information Security Program</td>
</tr>
<tr>
<td>Manager, Integrated eReporting Services</td>
<td>Responsible for ongoing management, development and deployment of CIHI’s IeR products and program as a whole</td>
</tr>
<tr>
<td>Manager, Integrated Online Analytics, and manager, Health Information Applications</td>
<td>Responsible for ensuring that technical requirements are met for the ongoing development, deployment and maintenance of CIHI’s IeR services and system administration</td>
</tr>
</tbody>
</table>

4.3 Principle 2: Identifying purposes for personal health information

YHS: Insight is a service provided by CIHI to meet the needs of its clients for online access to timely pan-Canadian health care data in a secure environment that safeguards privacy and confidentiality. The purpose of YHS: Insight is to support ongoing health system management as well as quality improvement initiatives at the hospital and regional levels.

CIHI’s service agreement limits the rights of clients to access and use YHS: Insight data solely for non-commercial purposes limited to the client’s internal management, data quality, planning, research, analysis or evidence-based decision-support activities.

4.4 Principle 3: Consent for the collection, use or disclosure of personal health information

CIHI is a secondary collector of data and will not have direct contact with patients. CIHI relies on the 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.
4.5 Principle 4: Limiting collection of personal health information

CIHI is committed to the principle of data minimization. Per sections 1 and 2 of CIHI’s Privacy Policy, 2010, CIHI collects from data providers 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. In accordance with this principle, YHS: Insight uses only the necessary information already held at CIHI in the CAD.iii

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

4.6.1 Limiting use

CIHI limits the use of YHS: Insight data to authorized purposes, as described in Section 4.3. YHS: Insight is a service offered to clients for which access is managed in 2 streams: general access, and general and record-level access (see Section 3.4). CIHI’s service agreement allows clients to access and use YHS: Insight solely for non-commercial purposes limited to the clients’ internal management, data quality, planning, research, analysis or evidence-based decision-support activities.

As described in Section 4.1.1, the service agreement imposes confidentiality and security restrictions and obligations on clients’ use of YHS: Insight. No restrictions are placed on clients’ access to and use of their own patients’ record-level data that supports each indicator result (see Return of own data later on in this section). Failure to comply with the terms and conditions of the service agreement could result in termination of access to and use of YHS: Insight.

CIHI staff are permitted to access and use YHS: Insight data on a need-to-know basis only, including for data processing and quality management purposes, the production of statistics and data files and conducting analyses. CIHI staff who use YHS: Insight are required to sign a confidentiality agreement at the commencement of employment, and they are subsequently required to renew their commitment to privacy yearly.

iii. CIHI plans to expand the amount of data available in YHS: Insight to include data from more of its data holdings.
Privacy risk: Inappropriate access to record-level data (general)

YHS: Insight is classified as a high-risk system in view of the sensitive record-level information it contains. Therefore, it is critical that clients and their designated users access only that information they are authorized to.

The sensitive record-level data contained in YHS: Insight can be accessed only by authorized designated users of clients that are data providers.

Inappropriate access to sensitive record-level data contained in YHS: Insight could occur if there were non-compliance with the administrative controls outlined below.

Mitigation measures currently in place

The administrative controls implemented to mitigate inappropriate access to record-level data begin with CIHI’s service agreement and are supported by:

- CIHI’s AMS processes for granting and revoking access; and
- YHS: Insight’s block approval process for ensuring data-loading activities occur appropriately.

CIHI’s Secure Electronic Reporting Services Agreement

As noted in Section 4.1.1, clients must sign CIHI’s service agreement. Section 2.2 of the service agreement outlines confidentiality and security restrictions and obligations with respect to clients’ access to and use of YHS: Insight, including:

- Making representation that they own, operate, act on behalf of or are otherwise responsible for each client facility they have identified to CIHI by way of reference in a schedule to the service agreement, and have the authority to sign on behalf of, and bind, each client facility;
- Being responsible for facilitating access to and use of YHS: Insight through their organization contact;
- Being responsible for identifying designated users through their organization contact;
- Ensuring that their employees and contractors are aware of and comply with the terms and conditions of the service agreement; and
- Immediately notifying CIHI of any breach or potential breach of the service agreement that comes to their attention.

Section 4 of the service agreement sets out specific obligations of clients related to the following:

1.1 Organization contact, including

- Providing CIHI at all times with accurate and current registration data for the organization contact;
- Notifying CIHI immediately of any change in the organization contact, including when the organization contact will no longer be employed by the client; and
- Ensuring that the organization contact
  - Provides CIHI at all times with accurate information for each designated user, including the level of access to be authorized by the client for each designated user, if applicable; and
  - Notifies CIHI immediately of any change in designated users, including when a designated user will no longer be employed by the client.
1.2 **Designated users**, including ensuring that their designated users successfully complete any applicable education and training required by CIHI.

1.3 **Means of use** (e.g., profile information such as username and password), including

- Ensuring usernames and passwords are not issued to an un-named individual or occupational position;
- Ensuring usernames and passwords are not disclosed to any person or entity for any reason; and
- Immediately notifying CIHI
  - Of any actual or potential unauthorized use of any designated user’s username and password; and
  - If the client ceases to own, operate, act on behalf of or otherwise be responsible for any client facility.

Section 4 of the service agreement also sets out an acknowledgement by clients that CIHI may, at its sole discretion, terminate a designated user’s access to YHS: Insight if

- There has been any actual or potential unauthorized use of any designated user’s username and password; or
- The client no longer owns, operates, acts on behalf of or is otherwise responsible for the client facility where the designated user is employed.

**AMS authentication processes**

CIHI’s AMS process is based on the obligations outlined above to authenticate users. As noted in Section 3.4.1, prior to granting access to YHS: Insight, all designated users must be authenticated:

- CIHI verifies that designated users are affiliated with the correct organization using a list of users identified by the client; and
- CIHI contacts the appropriate organization contact to verify the designated user and to obtain approval from the organization contact to grant access.

**Block approval**

In view of the sensitive information contained in YHS: Insight, an additional safeguard has been implemented. Prior to routine/regular uploading of data, YHS: Insight undertakes an independent double-verification and sign-off process known as **block approval** to ensure that the record-level CAD data-loading activities and indicator calculations occur consistently and correctly. Staff are required to follow the established data-loading activities, as approved by the executive director for Atlantic Canada and Integrated eReporting. If there is a change (e.g., new indicator, updated methodology), then a new block approval must be signed off by the executive director for Atlantic Canada and Integrated eReporting.

The independent double-verification process involves 2 staff members independently confirming that

- There are no changes to previously loaded data when additional year(s) of data are to be loaded;
- Established protocols for handling sensitive information were followed;
- Data is linked to the correct organization;
- Access to record-level data is limited to the data contributing to indicator results; and
- The termination of pregnancy masking protocol has been followed.

Each staff member verifying the above activities must sign off before proceeding to obtain sign-off by the manager of Integrated eReporting.
Privacy and security risk management (PSRM) review

Likelihood of risk occurring: Low
Potential impact of risk occurring: Medium
Risk score (value): Low
Recommended treatment: CCS to increase frequency and coverage of audits for the AMS process

Privacy risk: Inappropriate access to record-level data caused by organizational and/or personnel changes not identified to CIHI

YHS: Insight is classified as a high-risk system in view of the sensitive record-level information it contains. Therefore, it is critical that designated users access YHS: Insight data for only the facilities the client owns, operates, acts on behalf of or is otherwise responsible for.

Organizational changes due to restructuring activities and/or changes in personnel (e.g., when a designated user will no longer be employed by the client) present a set of challenges for access management. For example, when a health region or a hospital corporation is reorganized, resulting in individual facilities moving from the control of one organization to another, AMS processes must be able to accommodate these changes.

Inappropriate access to sensitive record-level data contained in YHS: Insight could occur if there were non-compliance with the administrative controls outlined below.

Mitigation measures currently in place

The following measures specifically address the privacy and security risks related to inappropriate access due to organizational changes and/or changes to personnel within a client’s organization. Compliance with all administrative controls, as outlined below, is critical to ensuring any organizational and/or personnel change is communicated to CIHI so that it is reflected in YHS: Insight as it relates to

- The facilities that clients own, operate, act on behalf of or are otherwise responsible for; and
- The designated users and their level of access,

where the onus is on the client to provide CIHI with accurate and timely information.

CIHI’s Secure Electronic Reporting Services Agreement

Section 2.2 of the service agreement outlines confidentiality and security restrictions and obligations with respect to clients’ access to and use of YHS: Insight, including representation that they own, operate, act on behalf of or are otherwise responsible for each client facility they have identified to CIHI by way of reference in a schedule to the service agreement, and have the authority to sign on behalf of, and bind, each client facility.

Section 4 of the service agreement sets out specific obligations of clients related to the following:

1.1 Organization contact, including

- Providing CIHI at all times with accurate and current registration data for the organization contact;
- Notifying CIHI immediately of any change in the organization contact, including when the organization contact will no longer be employed by the client; and
• Ensuring that the organization contact
  – Provides CIHI at all times with accurate information for each designated user, including the level of access to be authorized by the client for each designated user, if applicable; and
  – Notifies CIHI immediately of any change in designated users, including when a designated user will no longer be employed by the client.

1.2 Means of use (e.g., profile information such as username and password), including immediately notifying CIHI if the client ceases to own, operate, act on behalf of or otherwise be responsible for any client facility.

Section 4 of the service agreement also sets out an acknowledgement by clients that CIHI may, at its sole discretion, terminate a designated user’s access to YHS: Insight if
• There has been any actual or potential unauthorized use of any designated user’s username and password; or
• The client no longer owns, operates, acts on behalf of or is otherwise responsible for the client facility where the designated user is employed.

AMS authentication processes

CIHI’s AMS process is based on the obligations outlined above to authenticate users. As noted in Section 3.4.1, prior to granting access to YHS: Insight, all designated users must be authenticated:
• CIHI verifies that designated users are affiliated with the correct organization using a list of users identified by the client; and
• CIHI contacts the appropriate organization contact to verify the designated user and to obtain approval from the organization contact to grant access.

PSRM review

Likelihood of risk occurring: Medium

Potential impact of risk occurring: Medium

Risk score (value): Medium

Recommended treatment: CCS is to
1. Increase the frequency of audit reviews to the level that would be closer to monitoring, as opposed to conducting infrequent historical audits;
2. Define a process to ensure timely response to jurisdictional/organizational changes (within CIHI);
3. Review and improve, where possible, the process for organization contacts to enter (log) changes for themselves or for users;
4. Define a process to validate that the organization contact is current when making access changes; and
5. Develop a plan to ensure appropriate user awareness within CIHI and with clients.
Privacy risk: Inappropriate access to small cell sizes and health facility–identifiable information by those who are not registered as designated users per Section 4.2 of CIHI’s service agreement

Core Plan users of CIHI’s Learning Management System (LMS) can be divided into 2 subgroups:

- Authorized users of the LMS who are not registered users of a service such as YHS: Insight and whose employers have not signed CIHI’s service agreement; and
- Authorized users of the LMS who are registered users of a service such as YHS: Insight and whose employers have signed CIHI’s service agreement.

The LMS allows all Core Plan members to register for any publicly offered course/training session available through the system. The LMS cannot limit/restrict registration to a particular subgroup of LMS Core Plan users. As a result, users of the LMS who are not registered users of a service such as YHS: Insight would be able to register for courses/training sessions offered specifically for these applications and therefore inappropriately access small cell sizes and health facility–identifiable information with no controls, as would normally be applied through the service agreement.

Mitigation measures currently in place

LMS registration by invitation

An invitation-only approach will be used to ensure that only users of YHS: Insight can register for training on the tool. This process will involve sending an email to all designated users that provides information on upcoming courses that are available. The email will remind invitees that access to the education and training materials are subject to the service agreement that their employer signed with CIHI. Designated users who are interested in attending the training will be asked to respond via email. CCS will register those users who confirm their interest in attending the LMS. 2 weeks prior to the course, CCS will review the list of designated users who have registered for the course to ensure they are still authorized users of YHS: Insight. If a registrant is no longer a designated user, the registration will be cancelled.

CIHI’s Secure Electronic Reporting Services Agreement

s. 1 (e) Definitions: Information means all data and other information, including educational and training materials, submitted to, contained in, or accessed as a result of use of the Service, together with the reports and other submitted information generated through the use of the Service.

s. 5.1 (a) Access to Service: The Client shall restrict access to the Service to its Designated Users and solely for the purposes permitted under paragraph 2.1(a).

s. 6.1 (a) (b) Use of Information

[...] The Client shall:

(a) restrict the use of Information to its employees and Permitted Contractors on a need-to-know basis for the purposes under paragraph 2.1(a) only; and

(b) prohibit the use of the Information to attempt to identify any individual.
PSRM review

Likelihood of risk occurring: Low
Potential impact of risk occurring: Medium
Risk score (value): Low
Recommended treatment: None

Return of own data

Section 34 of CIHI’s Privacy Policy, 2010 establishes that the return of data to the data provider that originally submitted it to CIHI is not considered a disclosure; rather, it is considered a use. A key feature of YHS: Insight is the automated return of record-level information to allow data providers to reconcile their indicator results with their own locally held data and to use the data to identify underlying factors that may be driving their results. For 1 jurisdiction, the return of its own data involves the return of health care numbers.

Data linkage

Data linkages are performed to create episodes of care during the development of indicators. Sections 14 to 31 of CIHI’s Privacy Policy, 2010 govern the linkage of records of personal health information. Pursuant to this policy, CIHI permits the linkage of personal health information under certain circumstances. Data linkage within a single data holding for CIHI’s own purposes is generally permitted. Data linkage across data holdings for CIHI’s own purposes and all third-party requests for data linkage are subject to an internal review and approval process. When carrying out data linkages, CIHI will generally do so using encrypted health card numbers. The linked data remains subject to the use and disclosure provisions in the Privacy Policy, 2010.

Criteria for approval of data linkages are set out in Section 24 of CIHI’s Privacy Policy, 2010, as follows:

1. The individuals whose personal health information is used for data linkage have consented to the data linkage; or
2. All of the following criteria are met:
   a. The purpose of the data linkage is consistent with CIHI’s mandate;
   b. The public benefits of the linkage significantly offset any risks to the privacy of individuals;
   c. The results of the data linkage will not be used for any purpose that would be detrimental to the individuals that the personal health information concerns;
   d. The data linkage is for a time-limited specific project and the linked data will be subsequently destroyed in a manner consistent with sections 28 and 29; or
   e. The data linkage is for purposes of an approved CIHI ongoing program of work where the linked data will be retained for as long as necessary to meet the identified purposes and, when no longer required, will be destroyed in a manner consistent with sections 28 and 29; and
   f. The data linkage has demonstrable savings over other alternatives or is the only practical alternative.
Section 28 of CIHI’s Privacy Policy, 2010 sets out the requirement that CIHI will destroy personal health information and de-identified data in a secure manner, using destruction methodologies appropriate to the format, media or device, such that reconstruction is not reasonably foreseeable.

Section 29 of CIHI’s Privacy Policy, 2010 further requires that for linked data, secure destruction will occur within 1 year after publication of the resulting analysis or 3 years after the linkage, whichever is sooner, in a manner consistent with CIHI’s Information Destruction Standard. For linked data resulting from a CIHI ongoing program of work, secure destruction will occur when the linked data is no longer required to meet the identified purposes, in a manner consistent with CIHI’s Information Destruction Standard. This requirement applies to both data linkages for CIHI’s own purposes and for third-party data requests.

Subject to Section 19 of CIHI’s Privacy Policy, 2010, the linkage of the DAD and NACRS data contained in YHS: Insight was approved by the Privacy, Confidentiality and Security team.

Public use: Not applicable

YHS: Insight is not publicly available. YHS: Insight is a private tool for the community of users specified in Section 3.2.

4.6.2 Limiting disclosure

YHS: Insight contains both aggregate and record-level data. Access control measures, as described in Section 3.4, mitigate the risks of unauthorized access and disclosure of YHS: Insight data.

Health facility–identifiable information

YHS: Insight data contains information that identifies a health facility by name. The availability of and access to aggregate health facility–identifiable information forms part of the service agreement that clients are required to sign.

Aggregate data and small cell sizes

The indicator results obtained through YHS: Insight include rates (e.g., adjusted rate, crude rate) and numerator and denominator counts that may contain small cell sizes (defined as 5 or fewer occurrences) that are not suppressed.

Privacy risk: Re-identification and residual disclosure

Mitigation measures currently in place

The measures to mitigate risks of re-identification and residual disclosure are administrative. CIHI’s service agreement (see sections 6.1 and 6.3) includes the following:

Except in the case of their own data, clients

- Are prohibited from using YHS: Insight data or other information to attempt to identify individuals;
- Are permitted to report information publicly that does not contain cell sizes with fewer than 5 observations;
• Must take all reasonable steps to prevent identification of individuals; and
• Must immediately notify CIHI of any breach or potential breach of the service agreement that comes to their attention.

**PSRM review**

**Likelihood of risk occurring:** Low  
**Potential impact of risk occurring:** Low  
**Risk score (value):** Low  
**Recommended treatment:** None

**Termination of pregnancy data**

Termination of pregnancy data for all provinces and territories is included in the calculation of all indicator results.

**Privacy risk: Contravention of British Columbia’s Freedom of Information and Privacy Act**

Termination of pregnancy data sourced from the DAD and NACRS is contained in YHS: Insight.

**Mitigation measures currently in place**

To mitigate the risk that aggregated YHS: Insight data would reveal information relating to the provision of abortion services in B.C. at the facility level and thereby contravene Section 22.1 of B.C.’s Freedom of Information and Privacy Act, YHS: Insight has implemented specific protective measures to control disclosures, including special protections to mask facility information on sensitive abortion data for all B.C. facilities.

**Block approval**

In view of the sensitive information contained in YHS: Insight, an additional safeguard has been implemented. Prior to routine/regular uploading of data, YHS: Insight undertakes an independent double-verification and sign-off process known as block approval to ensure that the record-level CAD data-loading activities and the indicator calculations occur consistently and correctly. Staff are required to follow the established data-loading activities, as approved by the executive director for Atlantic Canada and Integrated eReporting. If there is a change (e.g., new indicator, updated methodology), then a new block approval must be signed off by the executive director for Atlantic Canada and Integrated eReporting.

The independent double-verification process involves 2 staff members independently confirming that
- There are no changes to previously loaded data when additional year(s) of data are to be loaded;
- Established protocols for handling sensitive information were followed;
- Data is linked to the correct organization;
- Access to record-level data is limited to the data contributing to indicator results; and
- The termination of pregnancy masking protocol has been followed.

Each staff member verifying the above activities must sign off before proceeding to obtain sign-off by the manager of Integrated eReporting.
PSRM review

Likelihood of risk occurring: Low
Potential impact of risk occurring: Low
Risk score (value): Low
Recommended treatment: None

4.6.3 Limiting retention

Data accessible through YHS: Insight forms part of CIHI’s information holdings and is retained by CIHI for as long as required to meet the intended purpose.

4.7 Principle 6: Accuracy of personal health information

The process for ensuring the accuracy of indicator calculations occurs over multiple phases that begin at the time indicators are developed by the relevant CIHI program area and continue through to loading indicators in the data warehouse. Quality assurance (QA) and user acceptance testing (UAT) are performed when indicators are first introduced in YHS: Insight. Once tested, the calculations are automated to minimize human error.

Cautionary notes: Use and interpretation

Indicator results and contextual measures reported in YHS: Insight include rates (e.g., adjusted rate, crude rate) and numerator and denominator counts that may include small cell counts. In compliance with Section 6.3 (b) of the service agreement, clients who want to publish indicators or rates are obligated to

- Use caution when the number of cases in the denominator is low (i.e., the rate is unstable) and avoid reporting the indicator or rate publicly; and
- Include the statement “interpret with caution” when the number of cases in the denominator is less than 50.

4.8 Principle 7: Safeguards for personal health information

4.8.1 CIHI’s Privacy and Security Framework

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

CIHI recognizes that information is secure only if it is secure throughout its entire lifecycle: creation and collection, access, retention and storage, use, disclosure and disposition. Accordingly, CIHI has a comprehensive suite of policies that specifies the necessary controls for the protection of information in both physical and electronic formats, up to and including robust encryption and secure destruction. This suite of policies and the associated standards, guidelines and operating procedures reflect best practices in privacy, information security and records management for the protection of the confidentiality, integrity and availability of CIHI’s information assets.

System control and audit logs are an integral component of CIHI’s Information Security Program. CIHI’s system control and audit logs are immutable. Analysis at CIHI is generally conducted with the use of de-identified record-level data, where the health card number has been removed or encrypted. In exceptional instances, staff will require access to original health card numbers. Section 10 of 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 personal health information as follows:

- Access to health card numbers and patient names (rarely collected) within CIHI’s operational production databases;
- Access to data files containing personal health information extracted from CIHI’s operational production databases and made available to the internal analytical community on an exceptional basis; and
- Changes to permissions in operational production databases.

CIHI’s employees are made aware of the importance of maintaining the confidentiality of personal health information and other sensitive information through a mandatory privacy and security training program and through ongoing communications about CIHI’s privacy and security policies and procedures. Employees attempting to access a CIHI information system must confirm, prior to each login 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.
4.9 Principle 8: Openness about the management of personal health information

CIHI makes information available about its privacy policies, data practices and programs relating to the management of personal health information on its corporate website. As well, this PIA is accessible on CIHI’s website (www.cihi.ca).

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

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

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

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

5 Privacy assessment summary and conclusion

This PIA summarizes CIHI’s assessment of the privacy implications of YHS: Insight. It identified 5 privacy risks. Following the application of CIHI’s Privacy and Security Risk Assessment Methodology, the risk value for 3 of the 5 risks was assessed to be low and no recommendations were made. The risk value for 1 of the 5 risks was assessed to be low and a recommendation was made.

For the privacy risk involving inappropriate access to record-level data caused by organizational and/or personnel changes not identified to CIHI, where the risk value was assessed to be medium, 5 recommendations were made to CCS. PSRM requires an assessment of what risk would remain if all the recommendations were implemented (i.e., residual risk, the new calculation of the likelihood and impact of the risk given the treatment). For this risk, the residual risk was assessed to be medium and therefore requires additional risk treatment until the risk is low or the untreated/residual risk is accepted by CIHI.

This PIA will be updated or renewed in compliance with CIHI’s Privacy Impact Assessment Policy.
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

www.cihi.ca
copyright@cihi.ca

© 2015 Canadian Institute for Health Information

Cette publication est aussi disponible en français sous le titre Évaluation des incidences sur la vie privée de l'outil Votre système de santé : En profondeur (octobre 2015).
Talk to us

CIHI Ottawa
495 Richmond Road, Suite 600
Ottawa, Ontario K2A 4H6
Phone: 613-241-7860

CIHI Toronto
4110 Yonge Street, Suite 300
Toronto, Ontario M3P 2B7
Phone: 416-481-2002

CIHI Victoria
880 Douglas Street, Suite 600
Victoria, British Columbia V8W 2B7
Phone: 250-220-4100

CIHI Montréal
1010 Sherbrooke Street West, Suite 300
Montréal, Quebec H3A 2R7
Phone: 514-842-2226

CIHI St. John’s
140 Water Street, Suite 701
St. John’s, Newfoundland and Labrador A1C 6H6
Phone: 709-576-7006