Our Vision
Better data. Better decisions.
Healthier Canadians.

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

Our Values
Respect, Integrity, Collaboration, Excellence, Innovation
The Canadian Institute for Health Information (CIHI) is pleased to publish the following privacy impact assessment in accordance with its Privacy Impact Assessment Policy:

- Canadian Patient Experiences Reporting System Privacy Impact Assessment, January 2015

Approved by:

Brent Diverty  
Vice President, Programs

Anne-Mari Phillips  
Chief Privacy Officer & General Counsel

Ottawa – January 2015
# Table of Contents

Quick Facts About the Canadian Patient Experiences Reporting System .................................6

1 Introduction ............................................................................................................................7

2 The Canadian Patient Experiences Reporting System at CIHI ..............................................7
   2.1 Background ...................................................................................................................7
   2.2 Data Flow ......................................................................................................................8

3 Privacy Analysis ....................................................................................................................9
   3.1 Authorities Governing CIHI and the Canadian Patient Experiences Reporting System 9
   3.2 Principle 1: Accountability for Personal Health Information ........................................10
   3.3 Principle 2: Identifying Purposes for Personal Health Information .................................11
   3.4 Principle 3: Consent for the Collection, Use or Disclosure of Personal Health Information ..............................................................................................................11
   3.5 Principle 4: Limiting Collection of Personal Health Information ....................................12
   3.6 Principle 5: Limiting Use, Disclosure and Retention of Personal Health Information ....14
   3.7 Principle 6: Accuracy of Personal Health Information ................................................16
   3.8 Principle 7: Safeguards for Personal Health Information ..............................................17
   3.9 Principle 8: Openness About the Management of Personal Health Information ..........18
   3.10 Principle 9: Individual Access to, and Amendment of, Personal Health Information ....18
   3.11 Principle 10: Complaints About CIHI’s Handling of Personal Health Information ....19

4 Privacy Assessment Summary and Conclusion ....................................................................19

Appendix ...................................................................................................................................20
Quick Facts About the Canadian Patient Experiences Reporting System

1. The Canadian Patient Experiences Reporting System (CPERS) will collect and report on patient experiences within the health care system in Canada, beginning with inpatient acute care hospitals. The purpose of the CPERS is to provide standardized patient experience information from across Canada.

Information from the CPERS will be used by health care providers, health system managers, policy-makers and patients to

- Analyze the patient experience aspect of quality of care for reporting, monitoring and comparing performance;
- Identify and inform quality and efficiency improvements and assess the effectiveness of health interventions to better support the integration of care for improved patient-centred care.

2. The Canadian Institute for Health Information (CIHI), with input from a broad range of experts, led the development of the standardized Canadian Patient Experiences Survey—Inpatient Care (CPES-IC). CPES-IC data to be submitted to the new CPERS is focused on patient experiences with inpatient acute care hospital stays.

3. CPERS will contain personal health information, including patient identifiers in the form of health card numbers, as well as responses to patient experience survey questions and demographic information.

4. Participating hospitals, health regions, health quality councils and/or ministries of health, or their designates, will contact patients following discharge from a hospital in order to collect information about their inpatient care experience, and then submit the data to the CPERS based on the CPES-IC minimum data set and pre-set specifications.

5. CIHI will use CPERS data for standardized reporting and analysis, as well as linkage of person-level data across data holdings and across time. Subject to its Privacy Policy, 2010, CIHI will make CPERS data available to enable more responsive and effective health-system planning and decision-making.

6. In spring 2014, following confirmation of jurisdictional commitment, CIHI began developing the CPERS in order to be ready to receive data by April 1, 2015.

7. With additional future support, CPERS data collection may expand to other health care sectors, such as emergency departments and long-term care.
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 directly from hospitals and other health facilities, long-term care homes, regional health authorities, medical practitioners and governments. This data includes health information about services provided to patients, residents and clients; registration and practice information about health professionals; and health expenditure information.

The purpose of this privacy impact assessment (PIA) is to document the privacy, confidentiality and security risks associated with the Canadian Patient Experiences Reporting System (CPERS) developed by CIHI. The scope of the current assessment is development of an operational system at CIHI that will begin accepting patient experience data by April 1, 2015, collected by, or on behalf of, jurisdictions using the new CPERS data standard.

This assessment includes a review of the 10 privacy principles set out in the Canadian Standards Association’s Model Code for the Protection of Personal Information as they apply to the development of the database and methods for submitting data to the CPERS.

The primary driver for this PIA is compliance with CIHI’s Privacy Impact Assessment Policy.

2 The Canadian Patient Experiences Reporting System at CIHI

2.1 Background

Understanding and improving a patient’s experience when he or she receives health services, interventions and care are integral to providing patient-centred care. In Canada, patient experience surveys are currently administered using a variety of tools and data collection methods that do not allow for pan-Canadian comparisons. Using a standard survey tool is key to measuring and improving performance through comparative reporting.

To address information gaps and the lack of standardized patient experience information, the CPERS is being established to provide standardized, comparable patient experience information from across Canada.
Information from the CPERS will help us better understand and compare patient perspectives on health services, interventions and care received to inform and improve patient-centred care and patient outcomes in Canada. It will be used by health care providers, health system managers and policy-makers to

- Provide comparable data on the patient experience aspect of quality of care for reporting, monitoring and comparing performance; and
- Provide data from which to identify and inform quality and efficiency improvements and assess the effectiveness of health interventions to better support the integration of care for improved patient-centred care.

The CPERS will collect data about patient experiences in inpatient hospital stays across 3 hospital service lines (i.e., medical, surgical and maternity) via the Canadian Patient Experiences Survey—Inpatient Care (CPES-IC). Future expansions may include other sectors of care.

2.2 Data Flow

Figure 1 illustrates the anticipated high-level flow of CPES-IC data into the CPERS. Hospitals, regions, health councils or ministries of health (i.e., providers of data to CIHI) will survey patients directly about their experiences following an episode of hospital care within the respective jurisdiction. The data that will be submitted to CIHI is required by facilities/jurisdictions to improve the quality of the planning, conduct and management of the delivery of health care services for their patients.

CIHI is a secondary data collector and user of patient experience information. CIHI will rely on the submission of data from data providers or their designates (e.g., a third party contracted to deliver and/or administer patient experience surveys on behalf of, and at the direction of, the respective data provider).

Data providers will extract the CPES-IC minimum data set (MDS) from their existing data sources and prepare the data for submission. Submission of data to CIHI for use in the CPERS is expected to conform to CIHI’s submission and editing specifications. (CIHI provides detailed data submission specifications to participating data providers prior to their submission of data.)

After the data files have been submitted using CIHI’s secure web-based file submission service, the data will be processed by the CPERS, and error reports will be produced for the data provider (accessible via CIHI’s web-based eServices). Error reports describe the outcome of the file submission, including data quality concerns identified during processing. The data provider is responsible for reviewing data quality feedback from CIHI and resubmitting any corrections, as required.
3 Privacy Analysis

3.1 Authorities Governing CIHI and the Canadian Patient Experiences Reporting System

General

CIHI adheres to its Privacy Policy, 2010 and to any applicable privacy legislation and/or agreements.

Legislation

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

All provinces and territories have public-sector privacy legislation in place. This legislation includes provisions that authorize public bodies covered by the acts to disclose person-identifiable data, without the consent of the individual, for statistical purposes. Alberta, Saskatchewan, Manitoba, Ontario, New Brunswick, Newfoundland and Labrador and Nova Scotia also have health information-specific privacy legislation with express lawful authority to use and disclose personal health information, without individual consent, for purposes of managing the health system, including statistical analysis and reporting.
For example, CIHI is recognized as a prescribed entity under the *Personal Health Information Protection Act* of Ontario. Custodians in Ontario may disclose personal health information to CIHI without patient consent pursuant to Section 29 as permitted by Section 45(1) of the act.

**Agreements**

As indicated in Section 2.2, data will flow directly to CIHI from data providers, such as provincial and territorial ministries of health, hospital or entities under contract to these parties that are responsible for the delivery and/or administration of patient experience surveys. These data flows will be governed by CIHI’s *Privacy Policy, 2010*, existing legislation in the jurisdictions and existing data-sharing agreements with the provinces and territories. The data-sharing agreements set out the purpose, use, disclosure, retention and disposal requirements of personal health information provided to CIHI, as well as any subsequent disclosures that may be permitted.

The agreements also describe the legislative authority under which personal health information is disclosed to CIHI. Where required, existing data-sharing agreements will be updated to include the provision of CPERS data to CIHI, prior to the submission of data to CIHI.

### 3.2 Principle 1: Accountability for Personal Health Information

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

**Organization and Governance**

The following table identifies key internal senior positions with responsibilities for the CPERS in terms of privacy and security risk management:

<table>
<thead>
<tr>
<th>Position/Group</th>
<th>Roles/Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vice President, Programs</td>
<td>Responsible for the overall operations and strategic direction of the CPERS</td>
</tr>
<tr>
<td>Director, Acute and Ambulatory Care Information Services</td>
<td>Responsible for strategic and operational decisions about the CPERS</td>
</tr>
<tr>
<td>Manager, Joint Replacement and Multiple Sclerosis Registries</td>
<td>Responsible for ongoing management and uptake of the CPERS; makes day-to-day operational decisions about the CPERS and supports the CPERS working groups and/or committees</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>Chief Privacy Officer</td>
<td>Responsible for the strategic direction and overall implementation of CIHI’s Privacy program</td>
</tr>
<tr>
<td>Manager, ITS Health Information Applications</td>
<td>Responsible for ensuring that technical requirements for ongoing operations and enhancements for the CPERS are met; acts as system administrator for the CPERS</td>
</tr>
<tr>
<td>Manager, Central Client Services</td>
<td>Responsible for managing external client access to restricted web-based eServices</td>
</tr>
</tbody>
</table>
Working Groups and Committees

CIHI has established 2 jurisdictional working groups to provide input and advice on the CPERS database development and reporting. One group provides input on the business and system requirements for data collection and submission. The other group provides input on the development of patient experience measures and reports.

CIHI also plans to continue to participate in a pre-existing group: the Inter-Jurisdictional Patient Satisfaction Group. This group enables regular communication across jurisdictions and provides CIHI with the additional knowledge, expertise and insights necessary to establish meaningful survey measures and indicators, and efficient data submission/operational processes.

3.3 Principle 2: Identifying Purposes for Personal Health Information

As described in Section 2.1, the information from the CPERS will help to better understand and compare patient perspectives on health services, interventions and care received to inform and improve patient-centred care and patient outcomes in Canada.

The CPERS will contain personal health information, including patient identifiers in the form of health card numbers, in order to facilitate linkage of person-level data across data holdings and across time. Collection of patient identifiers, for example, enables CIHI to add (i.e., link) CPERS survey responses to information that it already holds about a patient’s contact with the health care system (e.g., hospital stay data collected in the Discharge Abstract Database and National Ambulatory Care Reporting System). Bringing this information together is essential to better understand where patient experiences differ and why they differ across facilities, regions within a province or territory and Canada.

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

Patients will respond to patient experience surveys deployed in jurisdictions on a voluntary basis. CIHI has prepared a procedure manual, available on its corporate website (www.cihi.ca), to guide jurisdictions in the administration of the survey. The procedure manual identifies information to be communicated to potential survey respondents, including details about how CIHI intends to use the prospective respondent’s information. CIHI’s intent to conduct linkage is described, specifically, as follows: CIHI will be adding the survey responses to information it already holds about respondents’ contact with the health care system.

CPERS data is disclosed to CIHI for purposes of planning and managing the health system, including statistical analysis and reporting, under specific legislative authority or by legal agreements governing the flow of data. CIHI is a secondary collector of data and will not have direct contact with the data subjects. 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.
3.5 Principle 4: Limiting Collection of Personal Health Information

CIHI is committed to the principle of data minimization. Per sections 1 and 2 of CIHI’s Privacy Policy, 2010, CIHI collects from data providers only the information that is reasonably required for health system uses, including statistical analysis and reporting, in support of the management, evaluation or monitoring of the health care system.

CIHI limits its collection of personal health information to that which is necessary for the purposes of the CPERS. A critical deliverable for development of the CPERS was identifying the information that will be collected by this system.

Questions found in the CPES-IC constitute the bulk of CPERS data collection. CIHI developed the CPES-IC with input from a broad range of stakeholders, using the Hospital Consumer Assessment of Healthcare Providers and Systems (HCAHPS) survey as a base. Stakeholders included the Inter-Jurisdictional Patient Satisfaction Group, Accreditation Canada, the Canadian Patient Safety Institute and The Change Foundation. The CPES-IC MDS that will be collected consists of client experience survey information and other information, representing the minimum information necessary to address CPERS’ purposes.

The submission information portion of the CPES-IC MDS contains data elements to facilitate submissions to CIHI (e.g., Submitting Organization Identifier) and survey methodology–related data elements necessary for analysis and reporting (e.g., sample size, number of eligible discharges, sampling method).

Examples of the types of information to be collected by the CPES-IC appear below. The rationale for the collection of data elements with an increased risk of direct or indirect identification of an individual is provided in the appendix.

Record Identifiers

- Source Organization Identifier: A unique CIHI-assigned identifier for the organization rendering the health care services

Patient Identifiers

- Health Care Number: A jurisdictionally unique number used to identify a patient who has received or is receiving health care–related services or goods
- Organization Patient Identifier: An organization-assigned unique number that identifies a patient who has received or is receiving health care–related services or goods
- Birthdate: The year, month and day that represent the date on which the patient was born or is officially deemed to have been born

---
i. The HCAHPS survey has been rigorously validated and used in the United States for more than a decade.
Survey Administrative Information

- Discharge Date: The date, in full, on which the patient was formally discharged
- Survey Language: A 3-letter code representing the language of the survey

Canadian Patient Experiences Survey—Inpatient Care Questions

- Nurses Courtesy and Respect: A code used to indicate the patient-reported frequency with which the nurses treated him or her with courtesy and respect
- Doctors Listen Carefully Frequency: A code used to indicate the patient-reported frequency with which doctors listened carefully to him or her
- Cleanliness: A code used to indicate the patient-reported frequency with which his or her room and bathroom were kept clean
- Needed Medicine for Pain Flag: A code used to indicate whether the patient reported needing medicine for pain
- Possible Side Effects Described: A code used to indicate the patient-reported frequency with which hospital staff described the possible side effects of any new medicine in a way he or she could understand
- Admission Information: A code used to indicate the extent to which the patient reported receiving enough information about his or her admission to the hospital
- Discuss Help After Discharge: A code used to indicate the patient reporting that doctors, nurses or other hospital staff spoke with him or her about having the help needed once he or she leaves the hospital
- Recommend Hospital to Friends and Family: A code used to indicate whether the patient would recommend the hospital to friends and family
- Overall Physical Health: A code used to indicate the patient’s self-reported overall physical health
- Overall Mental or Emotional Health: A code used to indicate the patient’s self-reported overall mental or emotional health
- Education Level: A code representing the patient-reported level of schooling attained or received
- In Hospital for Childbirth Experience: A code used to indicate whether the patient reported that her most recent hospital stay was for a childbirth experience
- Race/Ethnicity: A patient’s self-declared affiliation with 1 or more social groups that have a common national or cultural tradition

Special Projects

- Special Project Code and Value: Fields used to collect supplemental data (i.e., data not already collected through the CPES-IC MDS) to meet the information needs of CIHI, the organization, the health authority or the ministry of health
3.6 Principle 5: Limiting Use, Disclosure and Retention of Personal Health Information

Limiting Use

CIHI will limit the use of data in the CPERS to authorized purposes, as described in Section 3.3. These include comparative analyses within and among jurisdictions; trend analyses to assess/monitor the impact of differences in policy, practices and service delivery; as well as statistics to support planning, management and quality improvement. CIHI staff will be permitted to access and use data on a need-to-know basis only, including for data processing and quality management, the production of statistics and data files, and conducting analyses. All CIHI staff are required to sign a confidentiality agreement at the commencement of employment, and they are subsequently required to renew their commitment to privacy yearly.

Since 2009, data sets used for internal CIHI analysis purposes do not contain direct identifiers, such as unencrypted health card numbers. Health card numbers in an unencrypted form are available to CIHI staff on an exceptional, need-to-know basis only, subject to internal approval processes, as set out in CIHI’s Privacy Policy and Procedures, 2010.

Data Linkage

Data linkages will be performed using CPERS data and other data sources CIHI holds. The value of patient experience data is enhanced when linked to the service episode record it pertains to, as this provides information about the complexity and other aspects relevant to the experience, such as adverse events. While data linkage potentially creates a greater risk of identification of an individual, CIHI will undertake the following mitigating steps to reduce the risk.

Sections 14 to 31 of CIHI’s Privacy Policy, 2010 govern linkage of records of personal health information. Pursuant to this policy, CIHI permits the linkage of personal health information under certain circumstances. Data linkage within a single data holding for CIHI’s own purposes is generally permitted. Data linkage across data holdings for CIHI’s own purposes and all third-party requests for data linkage are subject to an internal review and approval process. When carrying out data linkages, CIHI will generally do so 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 both to data linkages for CIHI’s own purposes and to third-party data requests.

Return of Own Data

Section 34 of CIHI’s Privacy Policy, 2010 establishes that the return of data to the health care facility that originally provided it to CIHI is not considered a disclosure; rather, it is considered a use. CIHI may return CPERS data via its web-based eServices, which permits authorized and restricted users to access CPERS data via industry-standard, encrypted, secure socket layer (SSL) sessions.

Limiting Disclosure

Public Release of CPERS Data

As part of its mandate, CIHI releases aggregate data only in a manner designed to minimize any risk of identification and residual disclosure. Aggregate statistics and analyses are made available on CIHI’s website. This generally requires a minimum of 5 observations per cell.

Third-Party Data Requests

Customized de-identified record-level and/or aggregate data from the CPERS may be requested by a variety of users, such as various levels of government, health care decision-makers and researchers.
CIHI administers a third-party data request program that contains and ensures appropriate privacy and security controls within the recipient organization. Furthermore, as set out in sections 45 to 47 of CIHI’s Privacy Policy, 2010, CIHI’s data disclosures are made at the highest degree of anonymity possible while still meeting the research and/or analytical purposes of the requester. This means that, whenever possible, data is aggregated. When aggregate data is not sufficiently detailed for the intended purpose, record-level data that has been de-identified may be disclosed to the recipient on a case-by-case basis, when the recipient has entered into a data protection agreement or other legally binding instrument with CIHI. Only those data elements necessary to meet the intended purpose may be disclosed.

In 2009, CIHI adopted a complete lifecycle approach to data management. As part of that lifecycle, CIHI’s Privacy and Legal Services (PLS) department developed and is responsible for the ongoing compliance monitoring process whereby all data sets that are disclosed to third-party data recipients are tracked and monitored for secure destruction at the end of their lifecycle. Prior to disclosing data, third-party recipients sign a data protection agreement and agree to comply with the conditions and restrictions imposed by CIHI relating to the collection, purpose, use, security, disclosure and return or disposal of data.

Data requestors are required to submit a written request. They must also sign an agreement wherein they agree to use the data only for the purpose specified. All data protection agreements with third parties specify that receiving organizations must keep de-identified record-level data strictly confidential and not disclose such data to anyone outside the organization. Moreover, CIHI imposes obligations on these third-party recipients, including:

- Secure destruction requirements;
- CIHI’s right to audit;
- Restriction on the publication of cell sizes less than 5; and
- Strong encryption technology that meets or exceeds CIHI’s standards where mobile computing devices are used.

As of January 2011, in addition to the compliance monitoring process, which leverages data captured to monitor compliance with data destruction requirements, PLS contacts third-party data recipients on an annual basis to certify that they continue to comply with their obligations as set out in the data request form and data protection agreement signed with CIHI.

### Limiting Retention

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

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

CIHI has a comprehensive data quality program. Any known data quality issues will be addressed by the data provider or documented in data limitations documentation, which CIHI makes available to all users.
Similar to other CIHI data holdings, the CPERS will be subject to a data quality assessment on a regular basis, based on CIHI’s Data Quality Framework. The process of completing the framework includes numerous activities to assess the various dimensions of quality, including the accuracy of the CPERS data.

3.8 Principle 7: Safeguards for Personal Health Information

CIHI’s Privacy and Security Framework

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

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 Privacy Policy and Procedures, 2010 sets out strict controls to ensure 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; 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 logon attempt, their understanding that they may not access or use the computer system without CIHI’s express prior authority or in excess of that authority.

CIHI is committed to safeguarding its IT ecosystem, securing its data holdings and protecting information with administrative, physical and technical security safeguards appropriate to the sensitivity of the information. Audits are an important component of CIHI’s overall Information Security program; they are intended to ensure that best practices are being followed and to assess compliance with all information security policies, procedures and practices implemented by CIHI. Audits are used to assess, among other things, the technical compliance of information processing systems with best practices and published architectural and security standards; CIHI’s ability to safeguard its information and information processing systems against threats and vulnerabilities; and the overall security posture of CIHI’s technical infrastructure, including networks, servers, firewalls, software and applications.

An important component of CIHI’s audit program is regular third-party vulnerability assessments and penetration tests of its infrastructure and selected applications. All recommendations resulting from third-party audits are tracked in the Corporate Action Plan Master Log of Recommendations, and action is taken accordingly.

3.9 Principle 8: Openness About the Management of Personal Health Information

CIHI makes information available about its privacy policies, data practices and programs relating to the management of personal health information. Specifically, CIHI’s Privacy and Security Framework, February 2010 and Privacy Policy, 2010 are available to the public on its corporate website (www.cihi.ca).

3.10 Principle 9: Individual Access to, and Amendment of, Personal Health Information

Personal health information held by CIHI is not used by CIHI to make any administrative or personal health decisions affecting the individual. Requests from individuals seeking access to their personal health information will be processed in accordance with sections 60 to 63 of CIHI’s Privacy Policy, 2010.
3.11 Principle 10: Complaints About CIHI's Handling of Personal Health Information

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

4 Privacy Assessment Summary and Conclusion

There are no recommendations at this time and privacy risks identified during this assessment have been mitigated. This PIA will be updated or renewed in compliance with CIHI's Privacy Impact Assessment Policy.
## Appendix

The following table describes personal identifiers and other data elements that could present an increased risk of direct or indirect identification of an individual, including data element definitions, information about when this data is collected and a rationale for its collection.

<table>
<thead>
<tr>
<th>Element/Definition</th>
<th>When Collected</th>
<th>Reason for Collection/Comments</th>
</tr>
</thead>
</table>
| **Health Care Number**                           | Collected from the hospital’s administrative system, needed at time of submission to CIHI | • To link with other CIHI data holdings to provide an enriched source of data for analysis and reporting  
• To identify unique clients within a jurisdiction |
| A jurisdictionally unique number used to identify a patient who has received or is receiving health care–related services or goods. This includes the code that identifies the jurisdiction that issued the Health Care Number. |                                                     |                                                                                                |
| **Organization Patient Identifier**              | Collected from the hospital’s administrative system, needed at time of submission to CIHI | • To link a Canadian Patient Experiences Survey—Inpatient Care record with the corresponding hospital encounter (e.g., Discharge Abstract Database record), when an identifiable Organization Patient Identifier is provided (in conjunction with Discharge Date)  
• To uniquely identify a person within a Source Organization in the event that Health Care Number is not available |
| An organization-assigned unique number (e.g., chart number) that identifies a patient who has received or is receiving health care–related services or goods. |                                                     |                                                                                                |
| **Discharge Date**                               | Collected from the hospital’s administrative system when determining survey sample | • To link a Canadian Patient Experiences Survey—Inpatient Care record with the corresponding hospital encounter (e.g., a Discharge Abstract Database record in conjunction with an identifiable Organization Patient Identifier) |
| The date, in full, on which the patient was formally discharged |                                                     |                                                                                                |
| **Birthdate**                                    | Collected from the hospital’s administrative system or patient-reported at time of survey completion. May be used when determining survey sample (e.g., identifying patients 18 and older) and at time of submission to CIHI. | • To calculate age, which is required to conduct analysis by age and to enhance linkage with other CIHI data holdings |
| The year, month and day that represent the date on which the patient was born or is officially deemed to have been born |                                                     |                                                                                                |
| **Gender**                                       | Collected from the hospital’s administrative system or patient-reported at time of survey completion | • To permit analysis of differences in patient experiences between genders |
| A code used to indicate the gender of the patient |                                                     |                                                                                                |
| **Race/Ethnicity**                              | Patient-reported at time of survey completion       | • To permit analysis of differences in patient experiences across various racial and ethnic groups |
| A patient’s self-declared affiliation with one or more social groups that have a common national or cultural tradition |                                                     |                                                                                                |
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 M2P 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