Canadian Organ Replacement Register

PRIVACY IMPACT ASSESSMENT

(June 2017)

Approved by:

Brent Diverty
Vice President, Programs

Anne-Mari Phillips
Chief Privacy Officer & General Counsel

Ottawa – June 2017
Table of contents

Quick facts about the Canadian Organ Replacement Register (CORR) ...................................... 6
Definitions ................................................................................................................................... 7

1 Introduction ................................................................................................................................... 8

2 Background ................................................................................................................................... 8
   2.1 Introduction to CORR ................................................................................................ 8
   2.2 Data collection ........................................................................................................... 9
   2.3 Data flow ................................................................................................................. 11
   2.4 Access management ............................................................................................... 15

3 Privacy analysis .......................................................................................................................... 16
   3.1 Privacy and Security Risk Management Program .................................................... 16
   3.2 Authorities governing CIHI and CORR ................................................................. 17
   3.3 Principle 1: Accountability for personal health information ....................................... 19
   3.4 Principle 2: Identifying purposes for personal health information .............................. 20
   3.5 Principle 3: Consent for the collection, use or disclosure of personal health information .......................................................................................................................... 20
   3.6 Principle 4: Limiting collection of personal health information ................................. 21
   3.7 Principle 5: Limiting use, disclosure and retention of personal health information ....... 21
   3.8 Principle 6: Accuracy of personal health information ................................................ 26
   3.9 Principle 7: Safeguards for personal health information ........................................... 27
   3.10 Principle 8: Openness about the management of personal health information ......... 28
   3.11 Principle 9: Individual access to, and amendment of, personal health information ... 29
   3.12 Principle 10: Complaints about CIHI’s handling of personal health information ...... 29

4 Conclusion ................................................................................................................................... 29
Quick facts about the Canadian Organ Replacement Register (CORR)

- CORR, which is maintained by the Canadian Institute for Health Information (CIHI), is a national register of patients treated for end-stage renal and extra-renal organ failure and transplantation, as well as organ donors, in Canada. It is a longitudinal database that follows a patient from his or her first treatment for end-stage organ failure (dialysis or transplantation) until the patient dies or is lost to follow-up.

- CORR collects data directly from participating dialysis centres (hospital-based satellite facilities, independent stand-alone health care facilities or provincial renal agencies), transplant centres and organ procurement organizations.

- CORR collects identifiable record-level data (personal health information) on 4 types of individuals: patients with end-stage kidney disease on dialysis; organ transplant recipients (kidney, liver, heart, lung/heart–lung, pancreas and islets, and intestinal); living organ donors; and deceased organ donors.

- While the CORR data holding is managed by CIHI, it receives strategic advice from the external, independent CORR board of directors. The board has representation from the Canadian Society of Transplantation, the Canadian Society of Nephrology, Canadian Blood Services and the Kidney Foundation of Canada.

- In 2015, CORR was enhanced to accept data electronically through the CORR Web-Entry Data Form. As of the 2015 data year, CORR is fully electronic and no longer receives any paper forms for any jurisdiction.
Definitions

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

**Aggregate data**: Data that has been compiled from record-level data related to records of individuals that have been compiled to a level of aggregation that ensures that the identity of the individuals cannot be determined by reasonably foreseeable methods.

**Data provider**: Any Canadian government ministry, department or agency, regional health authority, health care facility, public or private institution, or organization submitting data to CORR.

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

**Own data**: The CORR data was originally provided to CIHI by a data provider.

**Record-level data**: Data in which each record is related to a single individual (also referred to as “micro data”).

**Canadian Organ Replacement Register data**: All record-level data related to records of individuals contained within CORR and any aggregate data generated by CORR.
1 Introduction

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

The purpose of this privacy impact assessment (PIA) is to examine the privacy, confidentiality and security risks associated with CIHI’s Canadian Organ Replacement Register (CORR). This PIA updates the previous PIA report published in September 2010, and includes a review of the status of a recommendation made in the report about CORR’s retention and disposal practices of paper questionnaires. The PIA includes a review of the 10 privacy principles set out in the Canadian Standards Association’s Model Code for the Protection of Personal Information, as the principles apply to CORR. The primary driver for this PIA is compliance with CIHI’s Privacy Impact Assessment Policy.

2 Background

2.1 Introduction to CORR

CORR is maintained by CIHI. It is a national register of patients treated for end-stage renal and extra-renal organ failure and transplantation, as well as organ donors, in Canada. It is a longitudinal database that follows a patient from his or her first treatment for end-stage organ failure (dialysis or transplantation) until the patient dies or is lost to follow-up. Through CORR, CIHI provides pan-Canadian information on vital organ replacement therapy in Canada, with the goal of enhancing research, treatment and patient care.

The first renal failure register in Canada was started in 1972 under the leadership of Dr. Arthur Shimizu. In 1973, the register was transferred to Statistics Canada, with the collaboration of the Kidney Foundation of Canada. In 1987, with the support of the Federal/Provincial Advisory Committee on Institutional and Medical Services, the register was expanded to include data on extra-renal organ transplants. The expanded register was originally maintained by the Hospital Medical Records Institute. In 1995, responsibility for CORR transferred to CIHI.
The number of solid organ transplants performed in Canada continues to grow and, since 1972, there has been tremendous innovation in technique as well as pre- and post-surgical care. CORR’s wealth of current and historical data has, over time, increased its research potential. As a result, CORR has also seen an increased demand for data access on the part of data providers and third-party researchers in Canada.

2.2  Data collection

CORR collects identifiable record-level data (personal health information) on 4 types of individuals: patients on dialysis; organ transplant recipients; living organ donors; and deceased organ donors. Data is collected for recipients of kidney, liver, heart, lung/heart-lung, pancreas and islet, and intestinal transplants, as well as for end-stage renal failure patients receiving dialysis.

Presently, CORR does not receive individual patient data for those wait-listed for transplant. Aggregate counts of patients waiting for solid organ transplants, including the number of patients who died while waiting for a solid organ transplant, as well as the number of organ donors, are provided on a semi-annual basis by the organ procurement organizations responsible for maintaining wait lists. This supplemental information is maintained separately from the CORR database, and is used by CORR to achieve enhanced reporting of transplant and donor information. Table 1 summarizes the CORR data elements that are collected relating to information about individuals.

Facility-identifiable (facility profile) information is collected by CORR as supplemental data, and similar to the aggregate data, is maintained separately from the CORR database.
<table>
<thead>
<tr>
<th>Data element</th>
<th>Patients on dialysis</th>
<th>Organ transplant recipients</th>
<th>Living organ donors</th>
<th>Deceased organ donors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Y (full name)</td>
<td>Y (full name)</td>
<td>Y (partial name)</td>
<td>Y (partial name)</td>
</tr>
<tr>
<td>Province of Residence</td>
<td></td>
<td>Y</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Postal Code</td>
<td></td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Birthdate</td>
<td></td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Sex</td>
<td></td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Provincial Health Card Number</td>
<td></td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Blood Type</td>
<td></td>
<td>N</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Race</td>
<td></td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Height</td>
<td></td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Weight</td>
<td></td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Death</td>
<td></td>
<td>Cause of death</td>
<td>Not applicable</td>
<td>Province of death</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cause of death</td>
<td></td>
<td>Cause of death</td>
</tr>
<tr>
<td>Clinical Information</td>
<td></td>
<td>Pre-dialysis information</td>
<td>Transplant information</td>
<td>Hospital information</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Diagnosis</td>
<td>Diagnosis</td>
<td>Serology</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Treatment</td>
<td>Wait time</td>
<td>Risk factors</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Risk factors</td>
<td>Risk factors</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Treatment withdrawal</td>
<td>Serology status</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>information</td>
<td>Outcome</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Follow-up information</td>
<td>Post-transplant</td>
<td>Serology</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>follow-up information</td>
<td>Risk factors</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Organ-specific</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>information</td>
</tr>
</tbody>
</table>

Notes
Y: Yes, information is collected, partially collected or converted.
N: No, information is not collected.
Unique identifiers

Record identifiers

When submitting records, a data provider–generated record identification number (Record ID) is assigned to uniquely identify records. Record IDs are used to identify records for correction. Patients can have multiple Record IDs.

Recipient identifiers

As a longitudinal database, CORR assigns a Recipient ID and a Recipient Treatment ID at the time of registration. When subsequent records are added, CORR uses these unique identifiers, as follows:

- Recipient ID: Used to uniquely identify recipients by matching patient name, health card number and date of birth
- Recipient Treatment ID: Used in conjunction with Recipient ID to link treatments associated with each unique recipient

2.3 Data flow

The figure illustrates the high-level flow of data for CORR.

CIHI is a secondary data collector and collects data directly from participating dialysis centres (hospital-based satellite facilities, or independent stand-alone health care facilities or provincial renal agencies), transplant centres and organ procurement organizations. (For a list of CORR participating centres, see the 2016 Canadian Organ Replacement Register Methodological Notes and Supplementary Information.)

As a secondary data collector and user of CORR data, CIHI relies on the submission of data from participating centres (“data providers”). All CORR data flows in and out of CIHI through secure web-based applications. To access any of these applications, users must be authorized through CIHI’s Central Client Services (see Section 2.4 Access management). Staff in participating centres abstract the necessary patient information contained in records held in their local centres. They have the option of collecting and submitting the required information electronically via CIHI’s electronic Data Submission Services (eDSS) or using CORR’s standardized electronic web forms (i.e., CORR Web-Entry Data Form).
Submitted raw data files that contain personal health information are grouped as being either compliant with technical specifications of the CORR eFile application or non-compliant.

- **Non-compliant CORR data files must**
  - Be manually entered by CORR staff; and
  - Undergo a 2-step data quality process, which involves both a visual online data quality review and a mandatory automated edit check against prescribed specifications (as outlined in the CORR instruction manuals for dialysis and transplant records) for errors, omissions or inconsistencies.

- **Compliant data is subject to mandatory automated data quality checking only.**

When data quality issues are discovered in submitted compliant data files, they are identified in a Submission Report and returned to the appropriate data provider. When data quality issues are discovered in non-compliant data files, a system-generated submission summary of the required information is returned to the data provider, as well as a list of errors, including incomplete records.

Corrections made by data providers are resubmitted to CORR. Records that pass all edit checks undergo data-processing activities, as the records are entered into the production environment. Personal identifiers such as names and health card numbers are removed from records before being moved into the CORR analytical environment.

As a longitudinal database, CORR tracks patients from their first treatment for end-stage organ failure (dialysis or transplantation) and as they are treated in various facilities or treatment options, through to their death, unless they become lost to follow-up. This means that a kidney transplant record, for example, will be added to an existing patient’s records if the patient has been receiving dialysis treatment prior to the transplant. Follow-up information for dialysis patients is collected annually. For transplant patients, follow-up information is designed to capture information on outcomes, including patient status (e.g., transfer, graft failure, death, lost to follow-up). Follow-up records are added and linked to existing records by matching Recipient IDs.
Paper form submission

In April 2012, CIHI ceased collection of personal health information in paper format from data providers in Ontario. In 2015, CORR was enhanced to accept data electronically through the CORR Web-Entry Data Form. As of the 2015 data year (i.e., data for treatments and/or transplants that occurred in 2015), submission of paper forms is no longer accepted by CORR for any jurisdiction.

Electronic submission

Electronic Data Submission Services

In fall 2010, CORR was enhanced to accept data electronically via CIHI’s secure web-based electronic Data Submission Services (eDSS). Through eDSS, providers can submit data electronically in a variety of file formats. For CORR, participating centres can submit data files in a format that is compliant with technical specifications of the CORR eFile application, or in a file format that is not compliant.

Upon receipt, submitted non-compliant files are stored securely with access limited to authorized staff. Selected non-compliant files are printed in preparation for manual data entry. Non-compliant files, including printed hardcopies, are retained in compliance with CIHI’s Secure Information Storage Standard. Non-compliant files are entered into the CORR system by authorized CORR staff. Once entered, records undergo a 2-step data quality process.

Submitted compliant files are automatically received and processed for data quality within the CORR system.

Personal identifiers such as names and health card numbers are removed from records before being moved into the CORR analytical environment.

CORR Web-Entry Data Form

In winter 2015, CIHI released the CORR Web-Entry Data Form, a secure web environment that allows data providers to enter data online and submit it directly to CIHI. Data providers using the web-entry data tool can enter and save complete or partially complete records. Authorized users have the option to print a copy of the records entered in the web-entry form at the time of submission. Once records have been submitted, users are unable to view them, with the exception of records that were flagged with error(s) and sent back to the data provider for correction. Authorized users are unable to view partially saved records submitted by any other user, even a user within the same facility.

---

i. Data submitted by providers complies with CIHI’s Data Collection Standard.
Through the CORR Web-Entry Data Form, users submit single records, where each record undergoes a visual online data quality check by CORR staff in the CORR Web-Entry Data Form application. Dialysis records that pass all data quality checks are then moved into CORR’s eFile application, whereas transplant and donor record types are manually entered into the CORR system. Once moved into the CORR system, all record types undergo mandatory data-quality processing. Personal identifiers such as names and health card numbers are removed from records before being moved into the CORR analytical environment.

**Note**
Data collection using paper forms is no longer accepted.
2.4 Access management

CIHI’s Central Client Services (CCS) department is mandated to provide first-tier support to individualsii who want to access CIHI’s electronic products and services. Prior to granting access, CIHI determines whether it needs to enter into an agreement with the client. The criteria for determining whether an agreement is needed are based, in part, on the following:

- The applications themselves that need to be accessed and the nature of the activity;
- The sensitivity of the data being accessed;
- The volume of personal health information being returned; and
- Whether health facility–identifiable information by name is being disclosed.

As previously indicated, data providers have 2 options to electronically submit the required information to CORR: via CIHI’s eDSS or using CORR’s standardized electronic web forms (see Section 2.3).

2.4.1 Access to CIHI’s eDSS

Authorized users are required to set up a CIHI profile. Once the profile has been authenticated, users can log in on CIHI’s website and, from the My Services page, access the applications they are authorized to access, such as eDSS.

2.4.2 Access to the CORR Web-Entry Data Form

Access permissions are managed by CIHI’s CCS through the established Access Management System (AMS) processes for granting and revoking access. The process of granting access permissions to the CORR web-entry tool is a coordinated effort between data providers ("clients"), the CORR team and CCS. The approach used to restrict access to authorized users is role-based access control. CORR has 1 external user role, which allows only users to submit and modify their own data.

---

ii. This group includes customers in health service organizations, ministries/departments of health (federal/provincial/territorial) and staff in CIHI’s program areas.
The key components of the AMS process include the following:

1. Clients
   - Entering into a service agreement with CIHI;\textsuperscript{iii}
   - Assigning a designated organization contact; and
   - Identifying designated users through the organization contact.

2. CCS
   - Authenticating 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 obtaining approval from the organization contact; and
     - Granting the appropriate access privileges following authentication.

3. Privacy analysis

3.1 Privacy and Security Risk Management Program

Privacy and security risk management is a formal, repeatable process for identifying, assessing, treating and monitoring risks in order to minimize the probability of such risks materializing and/or their impact should they occur. In 2015, CIHI approved its Privacy and Security Risk Management Framework, and implemented the associated Policy on Privacy and Security Risk Management, Privacy and Security Risk Management Methodology and (an updated) Privacy and Security Risk Register. CIHI’s chief privacy officer and chief information security officer, in collaboration with senior managers, are responsible for identifying, assessing, treating, and monitoring and reviewing risk privacy and security risks.

\textsuperscript{iii} CORR clients are not required to sign CIHI’s Secure Electronic Reporting Services Agreement because the tool is designed for submission, not the return of own data (i.e., sensitive personal health information).
Privacy and security risks may be identified from a variety of sources, including for example, PIAs. Once identified, risks are entered into the Privacy and Security Risk Register and categorized as high, medium or low based on the likelihood and impact of a risk event.

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

The likelihood and impact of the identified risk are used to create a risk score. The risk assessment score (low, medium or high) defines how serious a risk is. A higher risk ranking indicates a more serious threat and a greater imperative for treatment. Once an initial risk treatment is applied, the residual risk (the new calculation of the likelihood and impact of the risk given the treatment) is assessed and compared against CIHI’s privacy and security risk tolerance statement, which indicates that CIHI’s privacy and security risk tolerance is low. If the risk score for the residual risk is still greater than low, additional risk treatment is necessary until the risk is assessed as low or the untreated/residual risk is accepted by CIHI’s Senior Management Committee on behalf of the corporation.

### 3.2 Authorities governing CIHI and CORR

#### 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 systems, including statistical analysis and reporting. Data providers are responsible for meeting the statutory requirements in their respective jurisdictions, where applicable, at the time the data is collected.
The following provinces and territories have enacted health information–specific privacy legislation: Newfoundland and Labrador, Prince Edward Island, Nova Scotia, New Brunswick, Ontario, Manitoba, Saskatchewan, Alberta, Yukon and the Northwest Territories. Health information–specific privacy legislation authorizes facilities to disclose personal health information without patient consent for purposes of health system use, provided that certain requirements are met. For example, CIHI is recognized as a prescribed entity under the Ontario's *Personal Health Information Protection Act*, so health information custodians in Ontario may disclose personal health information to CIHI without patient consent pursuant to Section 29 as permitted by Section 45(1) of the act.

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

**Agreements**

At CIHI, CORR data is governed by CIHI’s *Privacy Policy, 2010*, legislation in the jurisdictions and existing data-sharing agreements with the provinces and territories. CIHI has in place 2 types of agreements related to CORR:

**Memorandum of agreement**

CIHI entered into an agreement with the Canadian Organ Replacement Register Inc., a not-for-profit incorporated corporation. This agreement includes the constitution and bylaws that govern CORR Inc., and CIHI’s responsibility for ongoing management of the CORR data holding.

**Data-sharing agreements**

As indicated in Section 2.3, data flows directly from data providers that are responsible for the delivery and/or administration of health services. The data-sharing agreements that CIHI has with the provinces and territories 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.
3.3 Principle 1: Accountability for personal health information

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

Organization and governance

Table 2 identifies key internal positions with responsibilities for CORR 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>The vice president is responsible for providing overall leadership and oversight regarding the acquisition, management and reporting of CORR data.</td>
</tr>
<tr>
<td>Director, Acute and Ambulatory Care Information Services</td>
<td>The director is responsible for strategic and operational decisions about CORR, ensuring its continued successful development and managing the strategic relationship with the CORR board of directors and other stakeholders.</td>
</tr>
<tr>
<td>Manager, Decision Support, CORR and Trauma Registry</td>
<td>The manager is responsible for ongoing management, development and dissemination of CORR. The manager makes operational decisions about CORR, supports the CORR board of directors and consults both internally and with CORR clients as appropriate.</td>
</tr>
<tr>
<td>Program Lead, CORR</td>
<td>The program lead is responsible for coordinating operational and analytical activities related to the functioning of CORR and serves as the main day-to-day contact for stakeholders. He or she ensures the timely delivery of results and services that satisfy business and user requirements.</td>
</tr>
<tr>
<td>Chief Information Security Officer</td>
<td>The chief information security officer is responsible for the strategic direction and overall implementation of CIHI’s Information Security Program.</td>
</tr>
<tr>
<td>Chief Privacy Officer</td>
<td>The chief privacy officer is responsible for the strategic direction and overall implementation of CIHI’s Privacy Program.</td>
</tr>
<tr>
<td>Manager, ITS Health Information Applications</td>
<td>The manager is responsible for ensuring the availability of technical resources and solutions for ongoing operations and enhancements of CORR data.</td>
</tr>
<tr>
<td>Manager, Central Client Services</td>
<td>The manager is responsible for managing access to CIHI’s web-based applications, such as CORR.</td>
</tr>
</tbody>
</table>
**CORR board of directors**

Although CIHI manages the CORR data holding, it receives strategic advice from the external, independent CORR board of directors. The board is constituted to provide strategic guidance and advice on the register such as which data elements need to be collected. It includes representation from the Canadian Society of Transplantation, the Canadian Society of Nephrology, Canadian Blood Services and the Kidney Foundation of Canada.

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

CIHI collects only personal health information required for achieving the goals of CORR, which are to enhance research, treatment and patient care. More specifically, the purposes of CORR are to

- Provide a pan-Canadian view of end-stage organ failure statistics for comparative analyses and research;
- Increase the availability of comparative data to facilitate better treatment decisions;
- Provide statistics that track long-term trends for organ transplantation, organ donation and dialysis activities that can be used for planning and optimizing programs;
- Enable feedback to centres as a quality assurance function for treatment; and
- Provide statistics to the health care community to support decision-making.

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

CIHI is a secondary collector of data and does not have direct contact with patients. CIHI relies on data providers to abide by and meet their data collection, use and disclosure rules and responsibilities, including those related to consent and notification, as outlined in jurisdiction-applicable laws, regulations and policies.
3.6 Principle 4: Limiting collection of personal health information

CIHI is committed to the principle of data minimization. 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. In accordance with this principle, CORR only collects the information necessary to achieve the goals and purposes of CORR, as outlined above in Section 3.4.

Only information relevant to the goals of CORR is gathered. Instruction manuals for CORR list data elements that are collected. These documents are publically available on CIHI’s website.

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

Limiting use

CIHI limits the use of CORR data to authorized purposes, as described in Section 3.4. These include conducting comparative analyses within and among jurisdictions; trend analyses to assess/monitor the impact of differences in policy, practices and service delivery; production of statistics to support planning, management and quality improvement. CIHI staff is permitted to access and use data on a need-to-know basis only, including for data processing and quality management, producing statistics and data files, and conducting analyses. All CIHI staff is required to sign a confidentiality agreement at the commencement of employment, and they are subsequently required to renew their commitment to privacy yearly.

CORR data sets used for internal CIHI analysis purposes do not contain direct identifiers, such as names or unencrypted health card numbers. They are removed from records before being moved to CORR’s analytical environment (see Section 2.3 Data flow). Health card numbers in an unencrypted form and other direct identifiers 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

Linkages of records are performed within CORR, as it is a longitudinal database. When follow-up records for patients in CORR are added to the database, they are linked to existing records by matching unique recipient identification numbers, which are generated by CORR by matching patient name, health card number and date of birth.

Data linkages are also performed between CORR data and other CIHI data holdings. While this potentially causes greater risk of identification of an individual, CIHI will undertake 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 consistently encrypted health card numbers. The linked data remain subject to the use and disclosure provisions in the Privacy Policy, 2010.

Criteria for approval of data linkages are set out in sections 23 and 24 of CIHI’s Privacy Policy, 2010, as follows:

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.
   f. The data linkage has demonstrable savings over other alternatives or is the only practical alternative.
Client linkage standard

In 2015, CIHI implemented a corporate-wide client linkage standard to be used for the linkage of records created in 2010–2011 or later, where the records include the following data elements: encrypted health care number, the province/territory which issued the health care number and birthdate. For the linkage of records which do not satisfy these criteria, the linkage mechanism is determined on a case-by-case basis.

Destruction of linked data

Section 28 of CIHI’s Privacy Policy, 2010 sets out the requirement that CIHI 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 time-limited specific projects, the secure destruction of linked data will occur within one 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 an ongoing program of work, secure destruction will occur when the linked data are 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.

Return of own data

Section 34 of CIHI’s Privacy Policy, 2010 establishes the return of data to the data provider that originally provided it to CIHI or the relevant ministry of health for data quality purposes and for purposes consistent with their mandate, for example, for health services and population health management, including planning, evaluation and resource allocation. This return of data (own data) is not considered a disclosure; rather, it is considered a use.

CORR returns data to submitting facilities in the form of Submission Reports for purposes of data quality and correction (see Section 2.3). These reports, which indicate how many records a participating centre has successfully submitted and the reason why records were rejected, are disseminated to the participating centres in manner that complies with CIHI’s Secure Information Transfer Standard. These reports permit the centres to correct errors in the records and resubmit them to CORR. In order to identify the records which contain errors, the report refers to the record identification number, which is assigned to each patient record by data providers. The Submission Report does not contain original health card numbers.
In addition to Submission Reports, CORR returns data in the form of system-generated (error) reports, which are customized reports used for data verification of new patients by year, deaths by year, and prevalent patients by year for the purposes of accurate reporting in annual/ad hoc/centre specific reports.

Limiting disclosure

Public release of CORR data

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

The availability of small cell sizes is considered vital to providing clinical information needed by the participating centres. For example, the small cell information on pediatric patients is particularly important as these patients have different diagnoses, comorbid conditions and outcomes. Small cells also arise in relation to infrequent transplantation procedures such as combination transplants. The incidence of these procedures is important because of their rarity. If Canadian practitioners cannot obtain Canadian information from CORR, they have to rely on sources from the United States, which have less clinical relevance. In addition, it may be possible to identify hospitals where there are small cell sizes or where only one hospital or physician provides a given procedure in a province.

Because of the nature of the material being reported by CORR, there are instances when cells with fewer than 5 observations are reported. It is recognized that there is a small risk of re-identification from reporting small cell sizes, if they were to be matched with other external sources of information. Small cells are typically reported at a provincial level and more often at a national level to reduce this risk.

Prior to finalizing this PIA, the Methodology Unit conducted an assessment for the risk of re-identification and residual disclosure for past publications. The Methodology Unit indicated the risk was negligible.
Third-party data requests

Customized de-identified record-level and/or aggregated data from CORR 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 aggregated data is not sufficiently detailed for the intended purpose, record-level data that has been de-identified may be disclosed to the recipient on a case-by-case basis, when the recipient has entered into a data protection agreement or other legally binding instrument with CIHI. Only those data elements necessary to meet the intended purpose may be disclosed.

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

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

- Secure destruction requirements;
- CIHI’s right to audit;
- 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.

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 confirm 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

As indicated in Section 2.3, CORR is no longer accepting the submission of data using paper forms. The paper records previously submitted by data providers and paper printouts of non-compliant data in preparation for manual data entry are stored in locked cabinets within CIHI’s secure premises in compliance with CIHI’s Secure Information Storage Standard.

In the September 2010 CORR PIA, the following risk was identified and recommendation made:

**Risk:** There are no guidelines in place for retaining paper questionnaires that contain personal information. Paper questionnaires stored over a long period of time increase the risk of improper access to personal information.

**Recommendation:** CORR should review the practices around retaining paper questionnaires and, in consultation with Records Management, establish a retention and disposal schedule that takes into account any legal requirements or restrictions and redress mechanisms. CORR should dispose of documents that no longer have a specific purpose in a way that prevents improper or unauthorized use, access, copying, modification or disclosure and that is in accordance with CIHI’s policies and procedures.

This recommendation was accepted and a decision was made to retain CORR paper records for 5 years. Paper questionnaires that are older than 5 years have been destroyed in accordance with CIHI’s Secure Destruction Policy and Information Destruction Standard, and will continue to be destroyed on an ongoing basis. In addition, non-compliant electronic raw data files older than 5 years have been destroyed in accordance with CIHI’s Secure Destruction Policy and Information Destruction Standard, and will continue to be destroyed on an ongoing basis.

3.8 Principle 6: Accuracy of personal health information

CIHI has a comprehensive data quality program. Any known data quality issues are addressed with the data provider and/or documented in data limitations documentation that is made available to all users. For more information, please see the Data Quality Documentation for Users: Canadian Organ Replacement Register, which is posted on CIHI’s external web page.

Similar to other CIHI data holdings, CORR is 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 CORR data.
3.9  Principle 7: Safeguards for personal health information

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 CORR data are highlighted below.

System security

CIHI recognizes that information is secure only if it is secure throughout its entire life cycle: creation and collection, access, retention and storage, use, disclosure and destruction. Accordingly, CIHI has a comprehensive suite of policies that 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 upon first receipt. 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 that access is approved at the appropriate level and in the appropriate circumstances, and that the principle of data minimization is adhered to at all times. CIHI logs access to data as follows:

- Access to health card numbers and patient names (rarely collected) within CIHI’s operational production databases;
- Access to data files containing personal health information extracted from CIHI’s operational production databases and made available to the internal analytical community on an exceptional basis; and
- Changes to permissions in access to operational production databases.
CIHI’s employees are made aware of the importance of maintaining the confidentiality of personal health information and other sensitive information through a mandatory privacy and security training program and through ongoing communications about CIHI’s privacy and security policies and procedures. Employees attempting to access a CIHI information system must confirm, prior to each logon attempt, their understanding that they may not access or use the computer system without CIHI’s express prior authority or in excess of that authority.

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

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

3.10 Principle 8: Openness about the management of personal health information

CIHI makes information available about its privacy policies, data practices and programs relating to the management of personal health information. Specifically, CIHI’s Privacy and Security Framework and Privacy Policy, 2010 are available to the public on its corporate website (www.cihi.ca).
3.11 Principle 9: Individual access to, and amendment of, personal health information

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

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

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

4 Conclusion

This PIA summarizes CIHI’s assessment of the privacy implications of CORR. No privacy risks were identified in this assessment. This PIA will be updated or renewed in compliance with CIHI’s Privacy Impact Assessment Policy.