Canadian Organ Replacement Register

Privacy Impact Assessment

September 2023

Canadian Institute for Health Information
Institut canadien d'information sur la santé

Production of this document is made possible by financial contributions from Health Canada and provincial and territorial governments. The views expressed herein do not necessarily represent the views of Health Canada or any provincial or territorial government.

Unless otherwise indicated, this product uses data provided by Canada's provinces and territories.

Canadian Institute for Health Information
495 Richmond Road, Suite 600
Ottawa, Ontario K2A 4H6
Phone: 613-241-7860
Fax: 613-241-8120
cihi.ca
copyright@cihi.ca

How to cite this document:
Canadian Institute for Health Information. *Canadian Organ Replacement Register Privacy Impact Assessment, September 2023*. Ottawa, ON: CIHI; 2023.

Cette publication est aussi disponible en français sous le titre *Registre canadien des insuffisances et des transplantations d'organes : évaluation des incidences sur la vie privée, septembre 2023*.

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 Organ Replacement Register Privacy Impact Assessment, September 2023*

Approved by

Brent Diverty
Vice President, Data Strategies and Statistics

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

Ottawa, September 2023

Table of contents

Quick facts about the Canadian Organ Replacement Register

- The Canadian Organ Replacement Register (CORR), which is maintained by the Canadian Institute for Health Information (CIHI), is a pan-Canadian register of patients receiving treatment for end-stage organ failure (dialysis or transplantation) and deceased and living organ donors in Canada. CORR began as a renal failure registry in 1972, and its first report was produced in 1974. Its scope was expanded in 1988 to include data on extra-renal organ transplants. It is a longitudinal database that follows a patient from first treatment for end-stage organ failure until the patient dies or, in rare instances, is lost to follow-up.
- The goals of CORR are to provide national data on vital organ replacement therapy in Canada to enhance treatment and patient care, and to enable research.
- CORR contains record-level data — including patient personal identifiers and 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 intestines); living organ donors; and deceased organ donors.
- CORR receives data directly from 335 participating dialysis centres, 25 transplant centres and 12 organ donation organizations (as of August 2022).
- CORR is managed by CIHI, which receives strategic advice and guidance from the external, independent CORR board of directors, both directly and through working groups. The board has representation from the Canadian Society of Transplantation, the Canadian Society of Nephrology, Canadian Blood Services and the Kidney Foundation of Canada.

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 and aggregated to a level that ensures that the identity of individuals cannot be determined by reasonably foreseeable methods. Aggregate data with units of observation less than 5 may constitute either de-identified data or personal health information.

Canadian Organ Replacement Register data: Any record-level data or aggregate data collected through and stored in the CORR system

data provider: Any Canadian government ministry, department or agency, regional health authority, health care facility, public or private institution, or organization that submits data

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

own data: The CORR data that was originally provided to CIHI by a data provider

record-level data: Data where each record is related to a single individual (also referred to as “micro data”)

1 Introduction

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

The purpose of this privacy impact assessment (PIA) is to examine the privacy, confidentiality and security risks associated with the Canadian Organ Replacement Register (CORR). This PIA, which replaces the July 2017 version, includes both a review of the 10 privacy principles set out in the Canadian Standards Association's *Model Code for the Protection of Personal Information* and how the principles apply to CORR, as well as a look at the application of CIHI's *Privacy and Security Risk Management Framework*.

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

2 Background

2.1 Introduction to CORR

CORR is maintained by CIHI. It is a pan-Canadian database of patients receiving treatment for end-stage organ failure (dialysis or transplantation) and deceased and living organ donors in Canada. It is a longitudinal database that follows a patient from first treatment for end-stage organ failure until the patient dies or, in rare instances, is lost to follow-up. Through CORR, CIHI provides national information on vital organ replacement therapy in Canada, with the goals of enhancing treatment and patient care and of supporting research.

CORR began as the first renal failure database in Canada in 1972 under the leadership of Dr. Arthur Shimizu. In 1973, the database 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 database was expanded to include extra-renal organ transplants. The expanded database was originally maintained by the Hospital Medical Records Institute (HMRI). In 1995, HMRI became part of CIHI and therefore responsibility for CORR transferred to CIHI.

The number of solid organ transplants performed in Canada continues to grow and, since the database's inception, there has been tremendous innovation in technique as well as in pre- and post-surgical care. There has been increased demand for access to CORR data on the part of policy-makers, health system managers and researchers in Canada.

2.2 Data collection

Each record submitted to CORR reflects the minimum data set and includes personal identifiers/demographic information, health characteristics, administrative information and health facility identifiers. Additional information about the data elements included in the CORR minimum data set can be found on CIHI's website.

CORR contains record-level data — including patient personal identifiers and 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 intestines); living organ donors; and deceased organ donors.

Currently, CORR does not receive individual patient data for those on a wait-list for a transplant. Aggregate counts of patients waiting for organ transplants (including the number of patients who died while waiting for an organ transplant) and of the number of organ donors are provided annually by organ donation organizations. This supplemental information is maintained separately from CORR and is used to achieve enhanced reporting of transplant and donor information.

Table 1 summarizes the CORR data elements relating to information about individuals. The purpose of collecting these data elements, including direct identifiers and personal health information, can be found in Section 3.4. The secure flow of data into CIHI and its subsequent handling within the organization can be found in Section 2.3.

Table 1 Data elements collected about individuals, by type of individual

Data element	Type of individual			
	Patients on dialysis	Organ transplant recipients	Living organ donors	Deceased organ donors
Province of Residence	Y	Y	Y	Y
Postal Code	Y	Y	N	N
Birthdate	Y	Y	N (age only)	N (age only)
Sex	Y	Y	Y	Y
Name	Y (full name)	Y (full name)	Y (partial name)	Y (partial name)
Provincial Health Card Number	Y	Y	N	N
Blood Type	N	Y	Y	Y
Race	Y	Y	Y	Y
Height	Y	Y	Y	Y
Weight	Y	Y	Y	Y
Death	• Cause of death	• Cause of death	• Not applicable	• Province of death • Cause of death
Clinical Information	• Pre-dialysis information • Diagnosis • Treatment • Risk factors • Treatment withdrawal information • Follow-up information	• Transplant information • Diagnosis • Wait time • Risk factors • Serology status • Outcome • Post-transplant follow-up information • Tumour information (liver only)	• Hospital information • Serology • Risk factors • Organ-specific information	• Serology • Risk factors • Organ-specific information

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

2.3 Access management and data flow for CORR

Data providers can use 2 methods to securely submit electronic data to CORR: CIHI's electronic Data Submission Services (eDSS) and the CORR Web-Entry Data Form. Both systems are housed in CIHI's secure environment, and all users must be authenticated through CIHI's access management system (AMS) process.

There is 1 exception to CORR's data submission methods — a single facility in Nova Scotia has granted permission to CORR staff to create a user profile in order to access the facility's secure environment. Similar to CIHI's eDSS method of data submission, access to the facility's secure environment requires CORR staff to log in by entering a username and password in order to be authenticated and then to retrieve the CORR records prepared by the facility in a PDF format. After retrieving the records, CORR staff enter the data as single records, as described below under CORR Web-Entry Data Form.

Access management

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

Once authenticated through CIHI's AMS, CORR data providers submit record-level data from facilities that is electronically captured using specialized software, through CIHI's secure web-based eDSS or server-to-server (SFTP) application.

Access to the CORR Web-Entry Data Form

Access permissions are managed by CIHI's PMCE through the established 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 PMCE. Role-based access control is used to restrict access to authorized users. CORR has 1 external user role, which allows users to submit and modify their own data only.

Data flow

CIHI is a secondary data collector and relies on the submission of data from participating dialysis centres and provincial renal agencies, transplant centres and organ donation organizations (for a list of CORR participating centres, see the Canadian Organ Replacement Register Directory).

electronic Data Submission Services

CORR accepts data electronically via CIHI's secure web-based 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 complies with technical specifications of the CORR eFile application or in a file format that is not compliant (Microsoft Excel file). Compliant files submitted via eDSS are automatically received by CORR's eFile application and then forwarded to the CORR system in the production environment. Non-compliant files are stored securely on CIHI's network in compliance with CIHI's *Secure Information Storage Standard*, where access is limited to authorized staff approved by the manager of CORR and the director of CIHI's Acute and Ambulatory Care Information Services (AACIS) branch. Non-compliant files are manually entered by authorized CORR staff into the CORR system in the production environment. Non-compliant files are retained for 5 years, at which point they are destroyed in compliance with CIHI's *Secure Destruction Standard.*

CORR Web-Entry Data Form

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

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. **Donor and transplant records** that pass the visual data quality check are manually entered by CORR staff into the CORR system in the production environment. **Dialysis records** that pass the visual data quality check are batched together, processed into CORR's eFile application and then added to the CORR system in the production environment.

Processing in production environment

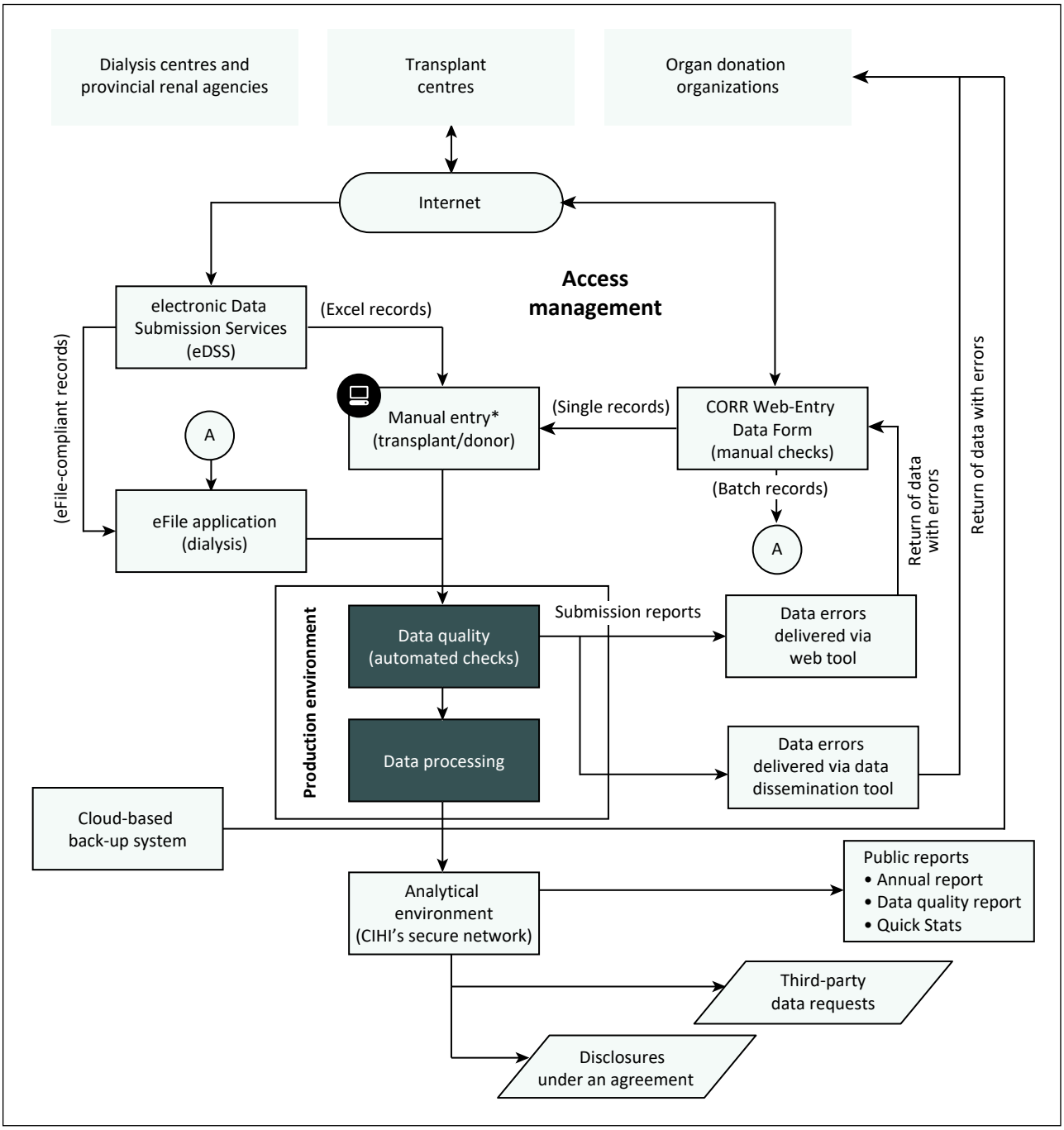
CORR records that pass into the CORR system in the production environment undergo automated 2-step data processing activities before being moved into CORR's analytical environment. The first step involves identifying data quality issues, where errors, omissions, inconsistencies or incomplete records are flagged. A submission report is automatically generated by the CORR system and returned to the data provider for correction and resubmission. If additional follow-up activities are required to complete the error correction process, CORR staff may do so in accordance with CIHI's *Secure Information Transfer Standard* (e.g., via phone calls, emails or use of CIHI's secure data dissemination tool).

The second step of data processing involves removing personal identifiers from records, including names and unencrypted health care numbers (HCNs). These identifiers are maintained in a separate restricted folder in the CORR analytical environment, not in the main CORR database. Access to both the main database and the restricted folders is granted to authorized CIHI staff on an approved, need-to-know basis only. This access is time-limited and can be granted only with documented approval from both the manager of CORR and the director of AACIS.

Copies of CORR data are retained in a cloud-based back-up system.

The following figure illustrates CORR data flows.

Figure CORR data flow



Notes

* For 1 facility in Nova Scotia, a CORR staff member logs in to the facility's secure environment to retrieve records electronically in PDF format. The records are then manually entered into the CORR system.

A: Dialysis records entered in the CORR Web-Entry Form undergo manual checks and are then batched together and processed into CORR's eFile application.

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. CIHI has implemented its *Privacy and Security Risk Management Framework* and the associated *Policy on Privacy and Security Risk Management*. CIHI's chief privacy officer and general counsel, and chief information security officer, in collaboration with senior managers, are responsible for identifying, assessing, treating, monitoring and reviewing privacy and security risks.

Privacy and security risks may be identified from a variety of sources, including PIAs. Once identified, risks are entered into the Privacy and Security Risk Register and categorized as **high**, **medium** or **low**, based on the likelihood and impact of a risk event:

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

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

No privacy and security risks were identified as a result of this PIA.

3.2 Authorities governing CORR data

General

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

Privacy legislation

CIHI is a secondary data collector of health information, specifically for the planning and management of Canada's 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, the Yukon and the Northwest Territories. Health information–specific privacy legislation authorizes facilities to disclose personal health information without patient consent for the purposes of health system use, provided that certain requirements are met. For example, CIHI is recognized as a prescribed entity under the *Personal Health Information Protection Act* of Ontario, so health information custodians in Ontario may disclose personal health information to CIHI without patient consent pursuant to Section 29 as permitted by Section 45(1) of the act.

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

Agreements

At CIHI, CORR data is governed by CIHI's *Privacy Policy, 2010*, by legislation in the jurisdictions and by data-sharing agreements with the provinces and territories. The data-sharing agreements set out the purpose, use, disclosure, retention and disposal requirements of personal health information provided to CIHI, as well as any subsequent disclosures that may be permitted. The agreements also describe the legislative authority under which personal health information is disclosed to CIHI.

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 Committee, and a Governance and Privacy Committee of its Board of Directors.

Organization and governance

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

Table 2 Key positions and responsibilities

Position/group	Roles/responsibilities
Vice president, Data Strategies and Statistics	Responsible for providing overall leadership and oversight regarding the acquisition, management and reporting of CORR data.
Director, Acute and Ambulatory Care Information Services	Responsible for making 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.
Manager, Organ Donation and Transplantation (ODT) Project and CORR	Responsible for ongoing management, development and dissemination of CORR. Makes operational decisions about CORR, supports the CORR board of directors and consults both internally and with CORR clients as appropriate.
Program Lead, CORR	Responsible for coordinating operational and analytical activities related to the functioning of CORR and serves as the main day-to-day contact for stakeholders. Ensures the timely delivery of results and services that satisfy business and user requirements.
Chief information security officer	Responsible for the strategic direction and overall implementation of CIHI's Information Security Program.
Chief privacy officer	Responsible for the strategic direction and overall implementation of CIHI's Privacy Program.
Manager, ITS Health Information Applications	Responsible for ensuring the availability of technical resources and solutions for ongoing operations and enhancements of CORR data.
Manager, Product Management and Client Experience	Responsible for managing access to CIHI's web-based applications, such as CORR.

CORR board of directors

CIHI manages the CORR data holding and receives strategic advice from the external, independent CORR board of directors. The board is constituted to provide strategic guidance and advice on the database, 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's 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. In order to fulfill its mandate, CIHI collects the following types of data in CORR for the purposes set out in Section 2.1.

Unique identifiers

As a longitudinal database, CORR performs data linkages using the following unique identifiers, which are either generated by data providers' health information systems and then submitted to CORR or generated by the CORR system. These linkages are undertaken for purposes such as adding records to existing patients' data, for example, to follow the patients from their first treatment for end-stage organ failure (dialysis or transplantation) through to their death.

Record identifiers

Records submitted using eFile each have a unique record ID generated by the data providers. Records submitted using the CORR Web-Entry Data Form each have a unique record ID automatically generated by the online tool. 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, HCN and date of birth
- Recipient Treatment ID: Used in conjunction with Recipient ID to link treatments associated with each unique recipient

Patient personal identifiers

Includes identifiers that allow CIHI to link records describing the different types of care provided to the individual at different times by different facilities. Examples include HCN and recovery program donor number. Due to the unique need for long-term follow-up of patient care in CORR and the mobility of patients across the country, having patient name, HCN and birthdate maximizes the linkability of records belonging to the same individual. CIHI uses this information to develop a complete picture of the care provided to the individual. In order to perform these linkages, CIHI needs to know which records pertain to the individual. Although this is not a normal practice for CIHI, individual names (full or partial) are collected for this specific and unique purpose in CORR, together with HCN and other identifiers. These data elements are stored, accessed and used by CIHI staff on a need-to-know basis as described in CIHI's *Privacy Policy, 2010*. As noted elsewhere in this PIA, access to these data elements is highly restricted at CIHI.

Patient demographic information

Examples include birthdate, postal code, sex and Indigenous identifiers. As mentioned in Section 2.3, access to these sensitive variables can be granted only with documented approval from both the manager of CORR and the director of AACIS. Within CORR, the computation of patient age is based on a count of months between birthdate and treatment date, which is then divided by 12. This calculation yields a number that is rounded to a whole number in years. For donors, age is collected in terms of a code (i.e., newborn, days, months, years) and unit (e.g., 2, 12, 35), as birthdate is not part of the donor data set. CIHI uses geographic information derived from postal code and sex for demographic analysis of health care services and outcomes.

Patient health characteristics

Examples include diagnoses and related comorbidities. CORR uses this information to analyze diagnoses and risk factors.

Administrative information

Examples include dates when the patient first began dialysis, was first placed on the transplant wait-list, was moved to final list status and received a transplant. CIHI uses this information to report on health system journeys for patients with end-stage organ failure and donors.

Health facility identifiers

Examples include the names of the hospital where the transplant occurred and of the treatment facility for dialysis. CIHI uses this information to generate operational reports and return own data to the respective health facilities.

Free (open) text fields

An example of the type of information that is entered into free-text fields in CORR is other patient health characteristics that may be identified, such as cause of death or other primary diagnosis. This information is used to capture information critical to the register but is not released externally to third parties. Users could potentially enter personal health information or other sensitive information in these fields. Free-text fields identified as potential privacy risks by CORR staff are held in a restricted-access folder in CIHI's environment, separate from other data, to ensure that access is provided on an approved, need-to-know basis only. On a regular basis, CORR reviews data captured in free-text fields to check for the presence of personal health information or other sensitive information. Additionally, on an annual basis, prior to database closure, CORR staff review and re-categorize responses captured in free-text fields using the existing listed diagnosis and cause of death codes where possible. For example, if diagnoses or causes of death are submitted using free text for the code of "other" instead of the listed numeric codes, these are re-coded to the numeric code wherever applicable.

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. Under sections 1 and 2 of CIHI's *Privacy Policy, 2010*, CIHI collects from data providers only the information that is reasonably required for health system uses, including statistical analysis and reporting, in support of the management, evaluation or monitoring of health care systems.

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

Limiting use

Clients

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

CIHI staff

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

Staff access to CIHI's secure analytical environment is provided through CIHI's centralized data access process. This environment is a separate, secure space for analytical data files, including general use data (GUD) files, where staff are required to conduct and store the outputs from their analytical work.

The GUD files are pre-processed files that are designed specifically to support internal analytical users' needs. Pre-processing includes removing the original HCN (and replacing it with an encrypted HCN) and the full date of birth and full postal code (and replacing them with a set of standard derived variables).

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

Data linkage

As CORR is a longitudinal database, data linkages are routinely performed within it. CORR follows patients from their first treatment for end-stage organ failure (dialysis or transplantation) through to their death, unless they become lost to follow-up. This means, for example, that a kidney transplant record will be added to an existing patient's records in CORR if the patient received dialysis treatment prior to the transplant. 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 using an automatic algorithm by matching patient name, HCN and date of birth. Follow-up information for dialysis patients is collected annually. For transplant patients, outcome information is collected for patients including patient status (e.g., transfer, graft failure, death, loss to follow-up).

CORR also performs internal linkages to link donors and transplant recipients by matching on organ donation organization and donor identifiers, partial donor last name, donor age or date of birth, and donor cross-clamp date/time.

Data linkages are also performed between CORR and other CIHI data sources using encrypted HCN, province of HCN and year of birth. While this potentially causes greater risk of identifying an individual, CIHI undertakes mitigating steps to reduce the risks (e.g., assigning meaningless transaction numbers).

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 HCNs. 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 sections 23 and 24 of CIHI's *Privacy Policy, 2010*, as follows:

Section 23 The individuals whose personal health information is used for data linkage have consented to the data linkage; or

Section 24 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.

Client linkage standard

CIHI has implemented a corporate-wide client linkage standard to be used to link records created in 2010–2011 or later, where the records include the following data elements: encrypted HCN and the province/territory that issued the HCN. When linking records that 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 1 year after publication of the resulting analysis or 3 years after the linkage, whichever is sooner, in a manner consistent with CIHI's *Secure Destruction Standard*. For linked data resulting from an 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 *Secure Destruction Standard*. These requirements apply to data linkages both for CIHI's own purposes and for third-party data requests.

Return of own data

A submitting facility/organization can access secure web-based submission reports that indicate how many records it has successfully submitted to CORR. These reports also indicate which records were not submitted successfully and the reason why (e.g., the records were missing information). The reports permit the facility/organization to identify errors in the records so that it may correct and resubmit them. In order to identify the records that contain errors, the report refers to the record identifier that the facility/organization assigns to each patient; the report contains no HCNs.

In addition to returning data to submitting facilities, Section 34 of CIHI's *Privacy Policy, 2010* establishes that CIHI may return records to the relevant ministry for data quality purposes and for purposes consistent with its mandate (e.g., for health services and population health management, including planning, evaluation and resource allocation) or as directed in the data-sharing agreement or other legal instrument. The return of own data is considered a use and not a disclosure.

Limiting disclosure

Third-party data requests

Customized record-level and/or aggregated data from CORR may be requested by a variety of third parties.

CIHI administers its Third-Party Data Request Program, which establishes privacy and security controls that must be met by the recipient organization. Furthermore, as set out in sections 37 to 57 of CIHI's *Privacy Policy, 2010*, CIHI discloses health information in a manner consistent with its mandate and core functions, and 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 de-identified data or personal health information (in limited circumstances, for example, with individual consent) 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.

CIHI uses a secure access environment (SAE) as the preferred means of providing record-level data access to third-party data requestors (the SAE is separate from CIHI's secure analytical environment that CIHI staff access, as described in Section 3.7). CIHI's SAE is an encrypted, secure environment hosted in CIHI's data centre. Consistent with CIHI's existing policies and procedures, approved researchers — who are subject to stringent agreement terms — access data extracts that have been prepared and vetted by CIHI staff for an approved research project. Record-level data cannot be copied or removed from the SAE; only aggregate results can be extracted from the SAE. Further information about CIHI's SAE is available on CIHI's website on the Make a data request web page and in the *SAE Privacy Impact Assessment*.

CIHI has adopted a complete life cycle approach to record-level data that it has extracted into files and sent to researchers and other approved users. 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. 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 requesters are required to complete and submit a data 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 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 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, PLS contacts third-party data recipients annually 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.

As noted in Section 3.4, CORR collects a pan-Indigenous identifier. The disclosure of this identifier is governed by CIHI's *Policy on the Release and Disclosure of Indigenous-Identifiable Data*, which requires that any request for Indigenous-identifiable data at CIHI be accompanied by approvals from appropriate Indigenous authorities. For more information, see *A Path Forward: Toward Respectful Governance of First Nations, Inuit and Métis Data Housed at CIHI*.

Disclosures (e.g., third-party data request disclosures) of CORR data are derived from annual data cuts that have undergone data quality checks. As noted in Section 3.4, CIHI collects information in free-text fields; data from free-text fields is released externally only in own-data requests back to the original data providers.

Public release of CORR data

As part of its mandate, CIHI publicly releases aggregated data only in a manner designed to minimize any risk of re-identification and residual disclosure. This generally requires a minimum of 5 observations per cell in accordance with Section 33 of CIHI's *Privacy Policy, 2010*. Aggregated statistics and analyses are made available in publications and on CIHI's website through products such as the annual statistics and summary statistics.

The availability of small cell sizes in tables generated from CORR 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 international sources.

Because of the nature of the material being reported by CORR, there are instances when cells with fewer than 5 observations are reported. Prior to any public release, CORR data is assessed for the risk of re-identification and residual disclosure. For the 2022 products (summary statistics, annual statistics and centre-specific reports), the risk was determined to be negligible.

Limiting retention

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

3.8 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, CORR is subject to a data quality assessment on a regular basis, based on *CIHI's Information Quality Framework*. The process of completing the framework includes numerous activities to assess the various dimensions of quality, including the accuracy of CORR data.

3.9 Principle 7: Safeguards for personal health information

CIHI's Privacy and Security Framework

CIHI's *Privacy and Security Framework* provides a comprehensive approach to enterprise privacy and security management. Based on best practices from across the public, private and health sectors, the framework is designed to coordinate CIHI's privacy and security policies and to provide an integrated view of the organization's information management practices. Key aspects of CIHI's system security with respect to the 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 specify the necessary controls

for the protection of information in both physical and electronic formats, up to and including robust encryption and secure destruction. This suite of policies and the associated standards, guidelines and operating procedures reflect best practices in privacy, information security and records management for the protection of the confidentiality, integrity and availability of CIHI's information assets.

System control and audit logs are an integral component of CIHI's Information Security Program. CIHI's system control and audit logs are immutable. Analysis at CIHI is generally conducted with the use of risk-reduced record-level data, where the HCN has been encrypted upon first receipt. In exceptional instances, staff will require access to original HCNs. CIHI's internal *Privacy Policy and Procedures, 2010* sets out strict controls to ensure that access is approved at the appropriate level and in the appropriate circumstances, and that the principle of data minimization is adhered to at all times. CIHI logs access to data as follows:

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

CIHI's employees are made aware of the importance of maintaining the confidentiality of personal health information and other sensitive information through the mandatory Privacy and Security Training Program and through ongoing communications about CIHI's privacy and security policies and procedures. Employees attempting to access a CIHI information system must confirm, prior to each attempt to log in, 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 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*, questions, concerns or complaints about CIHI's handling of information are investigated by the chief privacy officer and general counsel, who may direct an inquiry or complaint to the Information and Privacy Commissioner of the jurisdiction of the person making the inquiry or complaint.

4 Conclusion

CIHI's assessment of CORR did not identify any privacy or security risks that have not already been addressed.

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

help@cihi.ca

CIHI Ottawa
495 Richmond Road
Suite 600
Ottawa, Ont.
K2A 4H6
613-241-7860

CIHI Toronto
4110 Yonge Street
Suite 300
Toronto, Ont.
M2P 2B7
416-481-2002

CIHI Victoria
880 Douglas Street
Suite 600
Victoria, B.C.
V8W 2B7
250-220-4100

CIHI Montréal
1010 Sherbrooke Street West
Suite 602
Montréal, Que.
H3A 2R7
514-842-2226

cihi.ca

43417-1123