



Clinical Administrative Databases

Privacy Impact Assessment

August 2019



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.

All rights reserved.

The contents of this publication may be reproduced unaltered, in whole or in part and by any means, solely for non-commercial purposes, provided that the Canadian Institute for Health Information is properly and fully acknowledged as the copyright owner. Any reproduction or use of this publication or its contents for any commercial purpose requires the prior written authorization of the Canadian Institute for Health Information. Reproduction or use that suggests endorsement by, or affiliation with, the Canadian Institute for Health Information is prohibited.

For permission or information, please contact CIHI:

Canadian Institute for Health Information

495 Richmond Road, Suite 600

Ottawa, Ontario K2A 4H6

Phone: 613-241-7860

Fax: 613-241-8120

cihi.ca

copyright@cihi.ca

© 2019 Canadian Institute for Health Information

How to cite this document:


Canadian Institute for Health Information. *Clinical Administrative Databases Privacy Impact Assessment, August 2019*. Ottawa, ON: CIHI; 209.

Cette publication est aussi disponible en français sous le titre *Bases de données clinico-administratives : évaluation des incidences sur la vie privée, août 2019*.


The Canadian Institute for Health Information (CIHI) is pleased to publish the following privacy impact assessment in accordance with its *Privacy Impact Assessment Policy*:

- Clinical Administrative Databases

Approved by:



Brent Diverty
Vice President, Programs



Rhonda Wing
Chief Privacy Officer & General Counsel

Ottawa – August 2019

Table of contents

Quick facts about the Clinical Administrative Databases	5
1 Introduction	6
2 Background	6
2.1 Introduction to clinical administrative health services data and the CAD	6
2.2 Data collection	8
2.3 Access management, data submission and flow for DAD-HMDB and NACRS	17
3 Privacy analysis	19
3.1 Privacy and Security Risk Management Program	19
3.2 Authorities governing CAD data	20
3.3 Principle 1: Accountability for personal health information	21
3.4 Principle 2: Identifying purposes for personal health information	22
3.5 Principle 3: Consent for the collection, use or disclosure of personal health information	22
3.6 Principle 4: Limiting collection of personal health information	22
3.7 Principle 5: Limiting use, disclosure and retention of personal health information	23
3.8 Principle 6: Accuracy of personal health information	29
3.9 Principle 7: Safeguards for personal health information	30
3.10 Principle 8: Openness about the management of personal health information	31
3.11 Principle 9: Individual access to, and amendment of, personal health information	31
3.12 Principle 10: Complaints about CIHI's handling of personal health information	32
4 Conclusion	32
Appendix: Text alternative for figure	32

Quick facts about the Clinical Administrative Databases

1. The Clinical Administrative Databases (CAD) consist of 2 separate databases: the Discharge Abstract Database–Hospital Morbidity Database (DAD-HMDB) and the National Ambulatory Care Reporting System (NACRS).
2. Data supplied to the CAD is based on that which is collected from admission to discharge for inpatient acute visits, emergency department visits and outpatient (ambulatory care) visits (such as those in clinics or day surgery settings).
3. Prior to 2001, the HMDB was maintained separately from the DAD. Starting with 2001–2002 data, the 2 data holdings were merged.
4. The DAD was originally developed in 1963 to collect data on acute inpatient visits in Ontario.
5. The HMDB was developed by the Dominion Bureau of Statistics (now Statistics Canada) and was maintained by that organization until 1995, when responsibility was transferred to the Canadian Institute for Health Information (CIHI).
6. NACRS received its first full year of usable data in 2001–2002. Some data elements are specific to emergency activity, while others are specific to day surgery and/or clinic visits.
7. Special Project fields are used to collect supplemental information required to meet specific jurisdiction and/or facility needs; these data elements are not routinely collected in the DAD-HMDB and NACRS.
8. Limited data about long-term care, rehabilitation and mental health events is also collected from some hospitals and other health care facilities.
9. As of 2012, data is being collected for all acute inpatient and day surgery visits in all provinces and territories.
10. As of 2018–2019, Canadian Joint Replacement Registry (CJRR) data can be captured in the DAD-HMDB.
11. In 2017–2018, the most recent year for which data is complete, 3,427,247 records were submitted to the DAD and 22,245,338 records were submitted to NACRS. Approximately 1.2 million records have been included in the HMDB from Quebec for 2017–2018.

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 Clinical Administrative Databases (CAD). This PIA, which replaces the 2012 version, includes a review of the 10 privacy principles set out in the Canadian Standards Association's *Model Code for the Protection of Personal Information*, and how the principles apply to the CAD, 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, August 2017](#).

2 Background

2.1 Introduction to clinical administrative health services data and the CAD

The CAD consist of 2 separate databases: the Discharge Abstract Database–Hospital Morbidity Database (DAD-HMDB) and the National Ambulatory Care Reporting System (NACRS). They were created in response to a need for standardized clinical administrative health services data that permits comparisons across the country. Governments (e.g., ministries of health, regional health authorities) use CAD data for funding, system planning and evaluation. Hospitals and other health care providers use the data to evaluate performance indicators and to support facility-specific operational and utilization management decisions and administrative analysis. Academics and others also use the CAD for research purposes.

The DAD-HMDB and NACRS are related in that each is a repository of clinical, demographic and administrative data that was originally collected by hospitals and other health care facilities that deliver acute and ambulatory care. Each record submitted to the CAD is commonly referred to as an abstract. Each abstract contains health care and administrative information about a patient during the normal course of a single inpatient, emergency or outpatient (ambulatory care) visit.

DAD-HMDB

Discharge abstract data

The DAD was originally developed in 1963 to collect data on acute inpatient separations in Ontario. Since then, coverage has expanded to include data for all acute care separations from all provinces and territories except Quebec. Day surgery data is also collected in the DAD. Limited data about long-term care, rehabilitation and mental health events is also collected from some facilities. The data collected on each record includes diagnostic, intervention and patient demographic and administrative information.

Hospital morbidity data

The HMDB is a national data holding that contains data about all acute inpatient separations from all provinces and territories. It was developed by the Dominion Bureau of Statistics (now Statistics Canada) and was maintained by that organization until 1995, when responsibility was transferred to CIHI. Statistics Canada continues to hold the data from 1960 to 1993–1994.

Approximately 76% of the acute care records included in the HMDB data set are collected via the DAD; the remaining records are received directly from the ministère de la Santé et des Services sociaux du Québec in a single annual data submission following the closure of its provincial database, MED-ÉCHO, at the end of the fiscal year. The HMDB data file contains demographic, clinical and administrative data for acute inpatient care and day surgery separations, as well as data from some rehabilitation, chronic and psychiatric facilities, captured in MED-ÉCHO. The HMDB file format is not the same as the DAD file format; however, many of the data elements are the same. The HMDB contains a subset of the data elements in the DAD. To enable national reporting and provincial comparisons, CIHI, with the input of the Quebec ministry, maps the available MED-ÉCHO data elements to the DAD data elements where definitions and concepts are similar. This mapping allowed the 2 data holdings to be merged in 2001–2002, and the system was renamed the DAD-HMDB.

NACRS

Emergency and ambulatory care activity has grown significantly in recent years to become one of the largest-volume patient activities in Canadian health care. This increasing activity was the original reason for creating NACRS, which captures clinical, administrative and demographic information from all facility- and community-based emergency and ambulatory care: emergency departments, day surgery settings and outpatient clinics, such as those for diagnostic imaging, cardiac catheterization, renal dialysis and oncology. NACRS received its first full year of usable data in 2001–2002. Some data elements are specific to emergency activity, while others are specific to day surgery and/or clinic visits. NACRS currently collects data on emergency events from all facilities in Ontario, Quebec, Alberta and Yukon, and from some facilities in Newfoundland and Labrador, Prince Edward Island, Nova Scotia, Manitoba, Saskatchewan and British Columbia. CIHI is actively working on expanding NACRS data coverage to 100% across all provinces and territories, with implementations planned in Nova Scotia, New Brunswick and Saskatchewan.

2.2 Data collection

Data for the DAD-HMDB and NACRS is received directly from submitting facilities in participating provinces and territories, with the exception of Quebec, Manitoba and Alberta. In Manitoba and Alberta, hospitals submit their data to the provincial ministry of health, which then, in its role as a custodian or trustee, submits the data to CIHI. As Quebec does not participate in the DAD, its ministry of health submits 1 data file annually to CIHI specifically for the HMDB.

The CAD hold patient demographic, diagnostic, intervention and administrative information. A hospital or clinic chart (e.g., patient history, discharge summary, operative report, diagnostic test results report) contains patient-specific information that hospitals are required to collect, which reflects the normal course of patient care and administration for individual patients resulting from a hospital or clinic visit. The data supplied to the CAD is based on information that is collected between a patient's admission and separation, be it

- An inpatient acute visit (where a patient stay in hospital is usually longer than 24 hours);
- An emergency department visit; or
- An outpatient (ambulatory care) visit (such as in a clinic or day surgery setting), where a patient stay in hospital or other health care facility is usually less than 24 hours.

Health records personnel in hospitals and other health care facilities use CIHI's coding standards and the DAD-HMDB or NACRS abstracting/data collection manuals to capture specific data elements from the facility's records. Some data is captured in an automated, electronic method from hospital information systems (e.g., a registration system or emergency department information system), and other data is manually entered into software applications specifically developed for DAD-HMDB and NACRS data submissions. Commonly referred to as an abstract, each record submitted represents a single inpatient, emergency or outpatient visit. One of CIHI's strategic goals is to reduce the burden of data collection and submission. To accomplish this goal, CIHI continues to examine and implement opportunities to collect digitized data in more automated ways and from data sources that result in minimal burden to the health systems.

Data collected in designated fields is either mandatory or optional. A mandatory field is one that all provinces collect and includes information, such as date of birth or gender, that is core to analyses or permits the categorization of patients into clinically cohesive groups. Optional fields are those that are not collected in all provinces or facilities. There are also fields that individual provinces, hospitals or other health care facilities may mandate for collection.

Provinces, hospitals or other health care facilities also have the option of capturing information in Special Project fields to support specific initiatives. Special Project fields are used to collect supplemental information required for specific jurisdictional and/or facility needs; these data elements are not routinely collected in the DAD-HMDB and NACRS. These fields enable the capture of data in the form of alpha and/or numeric values that are meaningful only to the data provider (e.g., the data collected in Special Project fields from organizations participating in the project is meaningful only to those organizations). Prior to using Special Project fields, data providers are required to submit to CIHI for review and approval the codes and values they intend to submit. The abstracting/data collection manuals available to users inform data providers that Special Project fields are not to be used to record personal identifiable or confidential information (e.g., health care [card] numbers, chart numbers, provider numbers). Monthly, the CAD team audits Special Project fields to determine whether health care numbers have been submitted in non-health care number fields.

Data is being collected for all acute inpatient and day surgery visits in all provinces and territories. Data for emergency department and ambulatory care separations is also being collected in some provinces and territories, with varying levels of coverage.

Limited data about long-term care, rehabilitation and mental health events is also collected from some hospitals and other health care facilities. In 2017–2018, the most recent year for which data is complete, 3,427,247 records were submitted to the DAD and 22,245,338 records were submitted to NACRS. Approximately 1.2 million records have been included in the HMDB from Quebec for 2017–2018.

Table 1 summarizes the coverage of the DAD-HMDB and NACRS as of 2017–2018:

Table 1 Summary of 2017–2018 coverage, by event type and province/territory, for the CAD

Event type	N.L.	P.E.I.	N.S.	N.B.	Que.	Ont.	Man.	Sask.	Alta.	B.C.	Y.T.	N.W.T.	Nun.
Acute care	D/H	D/H	D/H	D/H	H	D/H	D/H	D/H	D/H	D/H	D/H	D/H	D/H
Day surgery	D	D	N	D	H†	N	D	D	N	D	D	D	D
Emergency department (Levels 1 and 2 data‡)	n/a	n/a	N*	n/a	N	N	N*	N*	N	N	n/a	n/a	n/a
Emergency department (Level 3 data‡)	n/a	N*	N*	n/a	n/a	N	n/a	n/a	N	n/a	N	n/a	n/a
Ambulatory clinics	n/a	N*	n/a	n/a	n/a	N	n/a	n/a	N	n/a	n/a	n/a	n/a
Clinic Lite	N*	n/a	N*	n/a	n/a	N*	n/a	N*	n/a	n/a	n/a	n/a	n/a
Rehabilitation	n/a	n/a	D*	D*	H*	n/a	n/a	n/a	D*	D*	n/a	n/a	n/a
Special rehabilitation	n/a	n/a	D*	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Chronic care	D*	n/a	n/a	D*	H*	D*	D*	D*	n/a	D*	n/a	D*	n/a
Psychiatric	n/a	n/a	D*	D*	H†	n/a	D*	n/a	D*	n/a	n/a	n/a	n/a
Home for the aged	n/a	n/a	n/a	n/a	n/a	n/a	D*	n/a	n/a	n/a	n/a	n/a	n/a

Notes

* Submissions from a limited number of facilities only.

† Quebec day surgery and psychiatric data is housed in the DAD-HMDB data tables but is not part of the DAD or HMDB populations.

‡ For NACRS, various data submission options are available. For Emergency Department (ED) data submissions, 3 different levels of submissions — Level 1, Level 2 and Level 3 — are available. NACRS ED Level 1 includes 30 mandatory data elements required for the calculation of ED wait time indicators. Level 2 data submission contains the same mandatory and optional data elements as Level 1, and the completion of at least one of the NACRS pick-lists (Presenting Complaint or ED Discharge Diagnoses). Level 3 data submission includes all mandatory and optional data elements collected in NACRS. Day Surgery records and ambulatory clinic records are also submitted at Level 3. Level 0 is used by data providers to submit basic but essential clinic data via the NACRS Clinic Lite option (explained further in the next section).

D: Discharge Abstract Database (DAD).

H: Hospital Morbidity Database (HMDB).

N: National Ambulatory Care Reporting System (NACRS).

n/a: Not applicable.

The CAD contain data elements that could alone, or in combination with other information, lead to the identification of an individual. These elements include the original Health Care Number, full Postal Code, Date of Birth and Gender. Below is a list of data elements collected in the CAD that are particularly sensitive.

Facility-assigned identifiers

- **Chart Number** (DAD, HMDB, NACRS): Health care numbers from Prince Edward Island and the Eastern Health regional health authority of Newfoundland and Labrador are submitted to CIHI in the Chart Number field.
- **Register Number** (DAD, NACRS): This is not collected in all provinces.
- **Second Chart/Register Number/Sequence Number** (DAD, NACRS): This was not collected in all facilities. As noted above, health care numbers from P.E.I. and the Eastern Health regional health authority of Newfoundland and Labrador are submitted to CIHI in the Chart Number field. Second Chart/Register Number/Sequence Number was retired as of 2018–2019 (see [Section 3.1](#) for privacy and security risk identified).ⁱ
- **Maternal/Newborn Chart or Register Number** (DAD, HMDB).

Emergency services–assigned identifiers

- **Ambulance Call Number** (NACRS): This is not collected in all facilities. This data element was retired in 2018–2019 (see [Section 3.1](#) for privacy and security risk identified).ⁱ

Personal attributes/identifiers

- **Health Care Number** (DAD, HMDB, NACRS): Health care (card) numbers from Manitoba and Quebec are encrypted by Manitoba Health and the ministère de la Santé et des Services sociaux du Québec, respectively, prior to submission to CIHI.
- **Date of Birth** (DAD, HMDB, NACRS): Quebec submissions to the HMDB include the age of the patient in lieu of Date of Birth; age is derived at the Quebec health ministry using CIHI's methodology.
- **Living Arrangement** (NACRS): Examples include living with family or living in an institution. This is not collected in all facilities. This data element was retired as of 2018–2019 (see [Section 3.1](#) for privacy and security risk identified).ⁱ
- **Residence Type** (NACRS): Examples include living in a private dwelling or homeless. This is not collected in all facilities. This data element was retired as of 2018–2019 (see [Section 3.1](#) for privacy and security risk identified).ⁱ
- **Highest Level of Education** (NACRS): This is not collected in all facilities.

i. Effective 2019–2020, CAD treatment of retired data elements includes the following:

- Release of information pertaining to the official retirement of data elements in Vendor Specifications;
- Removal of retired data elements from submission records, production database schemas and production systems; and
- Removal of retired data elements, or replacement with filler, in file layouts, data cuts (e.g., SAS analytical environment), and ceasing the population of datamarts and analytical sources-of-truth that supply data to CIHI public and restricted access products.

Geographic attributes of the patient

- **Postal Code** (DAD, HMDB, NACRS): All provinces submit full patient postal codes to the DAD-HMDB, with the exception of Quebec. Patient geographic information submitted by Quebec consists of a mini-postal code (a 2-letter code identifying the Canadian province/territory of residence) and a ministry-assigned administrative (health) region code for Quebec residents and Quebec facilities.

Clinical attributes

- **Diagnoses and Interventions** (DAD, HMDB, NACRS): The main clinical information in the CAD is related to diseases or health problems (diagnoses) and the procedures or treatments applied (interventions). Diagnosis information is captured using the *International Statistical Classification of Diseases and Related Health Problems, 10th Revision, Canada* (ICD-10-CA); the *International Statistical Classification of Diseases and Related Health Problems* is an international standard for reporting clinical diagnoses developed by the World Health Organization, and the ICD-10-CA is an enhanced version developed by CIHI for morbidity classification in Canada. ICD-10-CA classifies diseases, injuries and causes of death, as well as external causes of injury and poisoning. Intervention information is captured using the *Canadian Classification of Health Interventions* (CCI), which was developed by CIHI to accompany ICD-10-CA. Diagnostic and intervention information may also be collected in NACRS via pick-lists (Presenting Complaint List, ED Discharge Diagnosis and ED intervention). Pick-lists are a condensed but structured list of codes/terms that can be used by clinicians to capture common diagnoses and interventions.
- **Supplemental Information for Reproductive Care** (DAD, NACRS): This is not collected in all provinces.

[Section 3.7](#) and [Section 3.9](#) describe CIHI's disclosure avoidance measures and security safeguards, respectively.

Details on all CAD data elements can be found on the following CIHI web pages:

[DAD metadata](#), [HMDB metadata](#) and [NACRS metadata](#).

Changes to the DAD-HMDB and/or NACRS since the 2012 PIA

DAD-HMDB and/or NACRS data

While there have been no major changes to data collected by the DAD-HMDB since the last PIA was conducted in 2012, the data set has been modified to capture the following information:

- Special Project fields have been expanded from 5 to 25 occurrences in both the DAD-HMDB and NACRS as of 2015–2016. All fields are subject to the monthly health care number (HCN) audit described later in this section.
- In summer 2017, CIHI initiated a project to facilitate submission of ED data, including discharge diagnosis, from Quebec — submission of data to CIHI began in 2018–2019. The project enabled the submission of Système d'information de gestion des urgences (SIGDU) data to CIHI via CIHI's electronic Data Submission Services (eDSS) and provided a way to integrate Quebec ED data into NACRS as the single source for ED data at CIHI. The collection of Quebec ED data addresses various data gaps and increases national coverage to 82%. In addition, the provision of SIGDU data to CIHI provides opportunities for Quebec data to be reflected in various CIHI value-added products such as the ED Wait Times comparative reports and CIHI's Shared Health Priorities initiative.
- Beginning in 2018–2019, DAD-HMDB collection was modified to allow the submission of hip and knee prosthesis information for patients receiving joint replacements. This is not a new collection by CIHI but an alternative means of collecting the same information previously collected exclusively via the [Canadian Joint Replacement Registry \(CJRR\)](#) electronic file system and the now retired CJRR Web-Based Data Submission and Reports Tool. To create CJRR, authorized CIHI staff outside of the CAD area append hip and knee prosthesis information collected in the DAD-HMDB to joint replacement data collected elsewhere by CIHI.
- In 2018–2019, CIHI began collection of
 - Additional and revised Mental Health and Blood Transfusion Products data elements in both the DAD-HMDB and NACRS;
 - New Weight (for adults) and Height data elements in the DAD-HMDB; and
 - New ED Intervention Pick-List and ED Investigative Technology data elements in NACRS to enable assignment of Case Mix Group and Resource Intensity Weights for ED Level 2 submissions.

Data supply modernization

NACRS Clinic Lite

NACRS has introduced substantial changes to data collection efforts. As noted in [Section 2.1](#), the volume of emergency and ambulatory care activity has become one of the largest-volume patient activities in Canadian health care. As care shifts from inpatient to ambulatory care and from hospital clinics to community clinics, there is a need to collect key relevant clinical, quality and resource utilization information at the patient level. In response, CIHI introduced NACRS Clinic Lite as a new level of collecting and reporting basic but essential clinic data in a timely and flexible manner.

CIHI recognized the need to provide an alternative means of data submission to smaller data providers (facilities, mostly ambulatory care clinics) that do not have adequate resources and/or infrastructure to submit NACRS data via CIHI's eDSS. As a result, in 2015, CIHI developed and implemented a webentry tool that would allow data providers to submit NACRS Clinic Lite records that contain fewer mandatory data fields than those currently being submitted to NACRS.

The NACRS Clinic Lite Web-Entry Tool is a secure web-based tool that allows users to enter, save, edit/update/delete, access and retrieve saved or submitted records. The tool includes

- Customizable data capture functionality;
- Basic data edits and validations (e.g., entry of mandatory data, data types, permissible values, data lengths), which are displayed for users and enforced prior to data transmission;
- The ability for users to create and trigger submission files for processing; and
- An embedded in-application user guide and help modules.

The NACRS Clinic Lite option — Level 0 — is used by data providers to submit basic but essential clinic data. NACRS Clinic Lite uses Special Project fields to collect supplemental information that is not routinely collected in NACRS. The use of Special Project fields to collect NACRS Clinic Lite data opens the door for any data provider or group of providers who may not have submitted data to CIHI in the past to provide CIHI with data that complies with its standards.

The major differences between the data submitted to the full Level 3 NACRS Clinic option and the data submitted as NACRS Clinic Lite are as follows:

- There are fewer mandatory data elements; and
- Clinic Lite data providers can select the optional data they want to collect and submit to meet the information needs of a particular clinic type (e.g., rehabilitation, cataract, gastrointestinal).

[Details on NACRS Clinic Lite data elements](#) are available on CIHI's website.

As of the date of this update, 2 projects have been initiated to submit data via the web-entry tool: Children's Healthcare Canada (formerly the Canadian Association of Paediatric Health Centres [CAPHC]) Paediatric Rehabilitation Project, also known as the Paediatric Rehabilitation Reporting System (PRRS), and the Ontario Bundled Care Outpatient Rehabilitation Project. Additional projects are expected to begin as interest in submitting data at the NACRS Clinic Lite level grows.

Demonstration projects

As part of this work to modernize data collection, CIHI is also completing a series of demonstration projects to collect existing DAD-HMDB and/or NACRS data elements from digital health systems that have been implemented within hospitals or (in future) provincial electronic health records. A data supply demonstration project is a collaboration between CIHI and a leading hospital or ministry to identify and act on opportunities both for streamlining data reporting for secondary purposes and for reducing data collection and submission burden. Projects focus on sourcing data created at the point of care from hospital information systems rather than relying on manually coded and abstracted data.

The current demonstration projects do not represent a new data collection for CIHI, and all future demonstration project activities will continue to comply with CIHI's [Privacy Policy, 2010](#), including Section 1 and related procedures requiring CIHI's Executive Committee approval of new collections of personal health information and de-identified record-level data.

Automated auditing of HCN in non–health care number fields

Several data elements in the DAD-HMDB and NACRS abstracts allow for the inadvertent capture and submission of a valid HCN in non–health care number fields (e.g., Chart Number field). If CIHI is unaware that an HCN is being submitted in any of these fields, it increases privacy/security risk (e.g., unauthorized disclosure of personal health information). As of 2013, an HCN audit process has been implemented to identify inappropriate capture of HCNs in the DAD-HMDB and NACRS databases. This audit looks for an exact match of numbers/patterns found in the DAD-HMDB and NACRS HCN fields compared with the non-HCN data element fields that are large enough (with length equal to or over 8 characters) to contain HCNs. The process is automatically initiated on a monthly or on-demand basis at the point that extracts of the DAD-HMDB and NACRS production systems are taken to populate internal SAS data cuts. When an exact match is found, the non-HCN data element fields affected are blanked out in the SAS data cut. The audit result is also captured in a report that is sent to the CAD program area, which then notifies data submitters for corrections, if necessary.

Linkage of DAD, NACRS, OMHRS datasets to the Canadian Vital Statistics Death Database

CIHI's DAD, NACRS and Ontario Mental Health Reporting System (OMHRS) data sets already capture deaths occurring in hospital. However, information on patients who have died following their discharge from an acute care hospital or an emergency room was not available to CIHI. Addressing this information gap enhances CIHI's ability to develop and validate health care indicators and performance measures, as well as to perform survival and outcome analyses on acute inpatient data while considering such elements as efficiency, continuum of care, outcomes and disparities in health and longevity.

In 2017, with authorization from provincial/territorial vital statistics agencies, and under a Statistics Canada–CIHI agreement, CIHI began receiving from Statistics Canada death information on individuals who have been discharged from an acute care facility, same-day surgery, ED or acute care mental health facility. Statistics Canada linked data from the DAD, NACRS and OMHRS to the Canadian Vital Statistics Death Database (CVSD), providing CIHI with an initial linked file containing records from the CVSD for reference years 2000 to 2012. In 2019, CIHI received a refresh of the 12 years of linked data and an additional 5 years of linked data. This represents records from reference years 2000 to 2017.

Statistics Canada removes all direct identifiers from the linked file CIHI receives. Statistics Canada does not have Quebec hospitalization data as part of its data holdings and thus Quebec data is not included in the linked data supplied to CIHI. As of 2019, Yukon Vital Statistics had not provided authorization, and as such, Yukon data is not available.

The agreement between Statistics Canada and CIHI imposes restrictions on CIHI's use and disclosure of the data beyond those specified in CIHI's [Privacy Policy, 2010](#). For example,

- CIHI is prohibited from performing additional matching (data linkage) with the data file CIHI receives from Statistics Canada; and
- CIHI may only disclose or publish outputs from the linked data at an aggregate, non-confidential level.

The changes noted above in this section do not introduce any new privacy and security risk, beyond that already present in the CAD.

2.3 Access management, data submission and flow for DAD-HMDB and NACRS

Access to CIHI's secure applications is subject to CIHI's role-based access management process, which is managed by CIHI's Client Support Applications (CSA) department. CSA manages access to CIHI's secure applications using established access management system (AMS) processes for granting and revoking access.

The AMS Listener is an optional notification feature developed to further reduce the risk of unauthorized access to CIHI's restricted services. Manual audits are triggered when access is being granted to a new user. This is achieved by having program area staff monitor the alerting mechanism within the AMS application. If staff suspect or identify that an incorrect type of access was granted, they immediately alert CSA to disable access and send an email to incident@cihi.ca in compliance with CIHI's [Privacy and Security Incident Management Protocol](#). Within the CAD, the AMS Listener feature has been implemented for access to the NACRS Clinic Lite Web-Entry Tool.

Once authenticated through CIHI's AMS, CAD data providers submit to CIHI record-level data from facilities that is electronically captured using specialized software, through CIHI's secure web-based eDSS or the web-entry tool (NACRS Clinic Lite). One jurisdiction, Manitoba, transmits data to CIHI's IT Common Services directly via an approved server-to-server application.

At the time of processing, all submitted CAD data automatically undergoes validation and a data quality check for errors and inconsistencies against specifications outlined in documents prepared and maintained by CIHI, including coding standards, abstracting/data collection and submission manuals, and the *Acute and Ambulatory Care Data Content Standard*. These documents are used to specify validity/edit checks on the data transmitted from facilities to identify duplicate records, missing and/or invalid data, and inconsistencies in data transmissions. The data processing system is internal to CIHI, with no external connection.

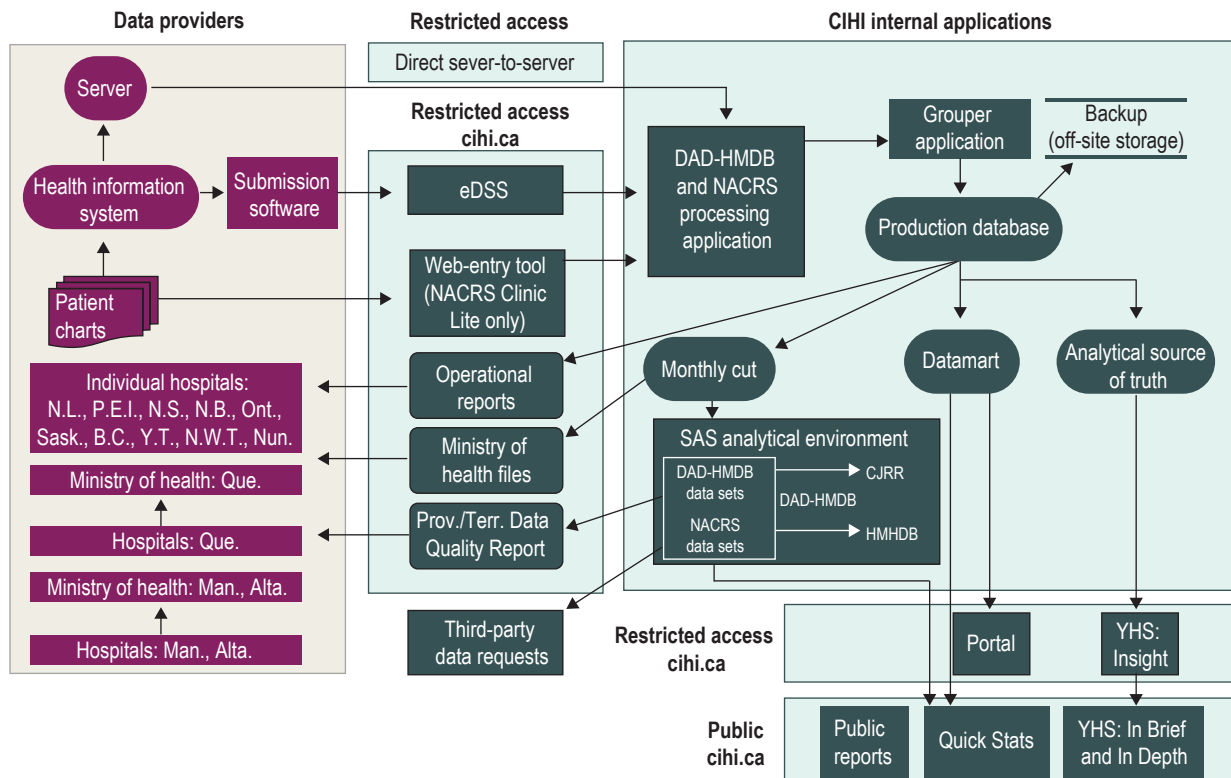
Error and validation reports generated at the time of processing are made available to the respective data providers via the Common Document Dissemination Service (CDDS) in compliance with CIHI's *Secure Information Transfer Standard*. These reports (i.e., operational reports) identify recordsⁱⁱ with errors; specify the number of records a data provider has successfully submitted; indicate the reason records were rejected or the relevant warning message; and permit the data provider to correct errors in the records and submit corrected records, delete duplicates or submit additional records missing at the time of initial submission. However, in the case of the NACRS Clinic Lite data submitted via the web-entry tool, users can access, view and edit the data (including HCNs) in any record that has been submitted by them or someone else at their facility.

ii. Operational reports usually use all of the following key identifier fields (5 in the DAD-HMDB and 4 in NACRS) as record identifiers; however, in some cases, Chart Numbers may be used: in the DAD-HMDB — Institution Number, Fiscal Year, Fiscal Period, Batch Number, Abstract ID; and in NACRS — Facility Number, Fiscal Year, Fiscal Period and Abstract ID.

Once the iterative error correction process is completed, final summary reports of file processing results are returned to data providers via the CDDS. A complete copy of the DAD-HMDB or NACRS data set is then uploaded to the production database, and a de-identified copy of the same data is uploaded to CIHI's SAS analytical environment where it is made available to approved CIHI staff for CIHI purposes. Also, the DAD-HMDB is a source of data used internally by CIHI to create the Hospital Mental Health Database (HMHDB) and CJRR. CIHI returns CAD data to the data provider that originally supplied the data, as well as to the respective ministry of health via the restricted access portion of CIHI's website. CIHI also discloses aggregate and record-level data to third-party requestors and aggregate data to the public. The figure presents a high-level illustration of the data flows for the CAD.

Staff access to the SAS analytical environment is provided through CIHI's centralized SAS Data Access process. The process ensures that all requests for access, including access to CAD data, are traceable and authorized. The SAS Data Access system 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 CAD data.

Figure DAD-HMDB and NACRS data flows showing internal and external systems and outputs



3 Privacy analysis

3.1 Privacy and Security Risk Management Program

Privacy and security risk management (PSRM) 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](#). CIHI's chief privacy officer 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, for example. 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 Senior Management Committee on behalf of the corporation.

The following privacy and security risk was identified during this PIA:

Privacy and security risk identified: The collection of data that is no longer required results in non-compliance with CIHI's privacy and security policies, procedures and standards governing personal health information.

Background: During this PIA, retirement of the following data elements was reported: Ambulance Call Number (NACRS); Second Chart/Register Number/Sequence Number (DAD, NACRS); Living Arrangement (NACRS); and Residence Type (NACRS).

When data elements are retired, for example due to lack of usefulness or to reduce collection burden, standard CIHI practice is that the data elements become a “filler” in the data submission layout used by all data providers, and changes are implemented to internal data processing systems to ensure the data is no longer accepted by CIHI systems. However, to address specific circumstances at the time, the decision was taken to adopt the approach of non-supported collection. This approach relied on various communication efforts directed at data providers advising them to stop submitting the data elements; but data providers were not asked to modify their submission layouts, and no change was made to CIHI systems that would reject/remove the unwanted data.

PSRM process: The privacy and security risk identified above has been added to CIHI’s Privacy and Security Risk Register, and will be assessed in accordance with PSRM methodology.

3.2 Authorities governing CAD 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 the health system, including statistical analysis and reporting. Data providers are responsible for meeting the statutory requirements in their respective jurisdictions, where applicable, at the time the data is collected.

The following provinces 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 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, CAD 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, a Governance and Privacy Committee of its Board of Directors, and an external chief privacy advisor.

Organization and governance

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

Table 2 Key positions and responsibilities

Position/group	Role/responsibilities
Vice president, Programs	Responsible for the overall strategic direction of the CAD
Director, Acute and Ambulatory Care Information Services	Responsible for the overall operations and strategic business decisions of the CAD
Manager, Clinical Administrative Databases Development/Expansion	Responsible for CAD development and expansion, including CAD-supported reporting and production systems
Manager, Clinical Administrative Databases Operations	Responsible for other CAD operations, including client support, education, data quality and analytics
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, Information Integration and Intelligence Products	Responsible for ensuring the availability of technical resources and solutions for ongoing operations and enhancements of CAD data

3.4 Principle 2: Identifying purposes for personal health information

Personal health information is collected for the CAD for the following purposes:

- To analyze acute inpatient separations and ambulatory care events;
- To support management decision-making at the facility, regional and provincial/territorial levels, as well as management report cards;
- To facilitate provincial and national comparative reporting, including health system performance and longitudinal analysis;
- To support the development and use of analytical tools, such as case grouping methods, length of stay analysis and resource utilization analysis;
- To support administrative research, system planning and evaluation, as well as funding decisions;
- To support quality and risk management; and
- To streamline data collection and reduce duplication between provinces.

The intended purposes and scope of the CAD are clearly identified in this PIA, on CIHI's website and in relevant publications.

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 the health care systems.

The data elements collected and their purpose have been identified in consultation with appropriate stakeholders, including CIHI's Steering Committee for National Clinical Administrative Databases.

CIHI's Steering Committee for National Clinical Administrative Databases guides the ongoing maintenance and enhancements of the CAD. The committee is engaged for operational and strategic recommendations to CIHI related to DAD-HMDB and NACRS data collection and use. Each province or territory appoints a member to this committee, with the requirement that the member be able to provide input representing the province's or territory's position on matters related to the CAD and bring back relevant information for discussion. In addition, there is 1 representative from each of Statistics Canada, Health Canada and the Public Health Agency of Canada.

The CAD also contain data collected in Special Project fields found in the DAD-HMDB and NACRS records. This data is used by data providers to capture supplemental information not routinely captured in the DAD-HMDB and NACRS abstracts for all jurisdictions. A range of Special Project fields is reserved for the use of CIHI and/or specific jurisdictions (e.g., fields for wait time and stroke information). Data related to these reserved projects is stored within the DAD-HMDB and NACRS and routinely returned to data providers as part of CIHI's data quality processing, which includes error/warning notifications. CIHI may use and report on this project information, where appropriate.

For unreserved project fields — those not developed for use by CIHI and/or specific provinces/territories — undefined data in the form of alpha and/or numeric values may be submitted to CIHI. These values are meaningful only to the data provider. The DAD-HMDB and NACRS abstracting/data collection manuals inform data providers to not use Special Project fields to record personal identifiable or confidential information (e.g., health care [card] numbers, chart numbers, provider numbers).

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

Limiting use

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

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.

Data sets used for internal CIHI analysis purposes do not contain names or direct identifiers, such as unencrypted HCNs. They are removed from records before being moved to CAD's analytical environment (see [Section 2.3](#)). HCNs in an unencrypted form are available to CIHI staff on an exceptional, need-to-know basis only, subject to approval processes as set out in CIHI's internal Privacy (2010) policy and procedures.

As noted previously, subsets of CAD data are extracted and appended to other information collected by CIHI to create the HMHDB and CJRR. A [privacy impact assessment of HMHDB](#) and [CJRR](#) are available on CIHI's website.

CAD data is used to create case-mix methodologies including Case Mix Group+ (CMG+),ⁱⁱⁱ Comprehensive Ambulatory Classification System (CACCS) and Resource Intensity Weight (RIW)^{iv} methodologies, which are used by hospitals and ministries to study health system utilization and resource allocation. CAD data is also used broadly by all analytical areas across CIHI to conduct analyses, create reports, undertake special studies and populate reporting/analytical tools.

Data linkage

Data linkages are performed between the CAD data and other CIHI data sources. While this potentially causes greater risk of identification of an individual, CIHI undertakes mitigating steps to reduce the risks.

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](#).

iii. This is the new acute care inpatient ICD-10-CA/CCI grouping methodology.

iv. This is the resource indicator used with CMG+.

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

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 HCN, and the province/territory that issued the HCN. For the linkage of 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

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 of health for data quality purposes and for purposes consistent with their mandate (e.g., for health services and population health management, including planning, evaluation and resource allocation). The return of own data is considered a use and not a disclosure.

Through CIHI's restricted access web-based services, authorized users have access to CAD data and reports in the following ways:

- Reports on the outcome of their data submissions, including details of records that contain errors, are returned to data providers so these organizations can investigate and, where necessary, correct and resubmit data (i.e., operational reports).
- Following a specified schedule, CIHI returns data to data providers in standardized reports, including value-added data elements (such as case mix–related data elements, including CMGs and RIWs) consistent with the purpose of the CAD. In accordance with CIHI's [Privacy Policy, 2010](#), personal health information returned to an original data provider shall not contain additional identifying information to that originally provided.
- Your Health System (YHS): Insight is a web-based tool that serves as a complement to CIHI's public interactive web tool, YHS: In Depth and YHS: In Brief. YHS: Insight is an analytical web-based tool in a secured private environment, providing authorized users with a deeper look at various standardized indicators and summary measures on health system performance; it is not publicly accessible. YHS: Insight contains clinical and administrative data from CIHI's DAD-HMDB and NACRS. The aggregate data contained in YHS: Insight includes indicators and measures from the acute care setting that are reported at the facility level (by name), as well as at the regional, provincial and national levels, and that are available to all designated users.

A key feature of YHS: Insight is the automated return of record-level information, which is the contributing data used to build a particular indicator. This feature allows authorized designated users of clients that are data providers to reconcile their indicator results with their own locally held data, and to use the data to identify underlying factors that may be driving their results. For a given indicator, the user can view or export record-level data (only own data from their own facility) that provides enough detail to permit the user to locate the patient records in their own system that contributed to

the indicator. The record-level data does not include HCNs and does not contain the full/complete list of fields from the DAD-HMDB or NACRS. Rather, a subset of fields tailored to each indicator are returned that include Chart Number, Institution Number, Register Number, Admission Date, Discharge Date and other fields necessary to permit the user to better understand the YHS indicator being reported.

A [privacy impact assessment of YHS: Insight](#) is available on CIHI's website.

Limiting disclosure

Disclosures to data provider community

Via restricted access web-based services, YHS: Insight and CIHI Portal, CIHI makes comparative reports containing facility-identifiable, aggregate CAD information available to the data provider community:

- As of June 2017, the CAD have made aggregate data accessible to registered users (i.e., organizations that submit data to the DAD-HMDB and NACRS and their respective provincial or territorial ministries of health) through CIHI's YHS: Insight. This information was previously accessed only through CIHI's eDAD and eNACRS products (both products were retired in September 2017, with eDAD/eNACRS users transitioned to Insight). YHS: Insight provides indicator results and contextual measures reported at the facility level (by name), as well as at the provincial and national levels, that are available to all users, including but not limited to rates (e.g., adjusted rate, crude rate) and numerator and denominator counts that may include small cell counts. As many as 15 different factors (e.g., age group, sex, triage level, Case Mix Group, main patient service) can be explored, which can include breakdowns by age and sex. A [privacy impact assessment of YHS: Insight](#) is available on CIHI's website.
- Subsets of de-identified data from the DAD-HMDB and NACRS are also included in CIHI Portal, an analytical web-based tool for health care data that was designed by CIHI to provide clients, such as hospitals, regional health authorities and ministries of health, with online access to pan-Canadian health care data in a secure environment that safeguards privacy and confidentiality. The tool allows clients to create reports on clinical administration, resourcing, service provision, cost-efficiencies and population demographics for planning and research purposes. CIHI Portal does not allow direct access to individual records. Queries to create reports may return rows with individual record counts, but users cannot see or request the extraction of individual records. A [privacy impact assessment of CIHI Portal](#) is available on CIHI's website.

Query and report results include aggregate information on patient demographics, clinical outcomes, service utilization, and quality and performance indicators. Organization-specific results, and results that present comparable information across organizations, do not

contain any person-identifying information (e.g., they exclude HCNs, dates of birth and full postal codes). Results obtained may contain de-identified data in the form of small cell sizes (defined as 5 or fewer occurrences) that are not suppressed in the results produced by users.

Before being provided with access to CAD data, users must sign a service agreement that includes rules regarding health facility–identifiable information and the suppression of small cell size data.

Third-party data requests

Customized record-level and/or aggregate data from the CAD may be requested by a variety of third parties.

CIHI administers a third-party data request program that 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 and in a manner consistent with its mandate and core functions, and CIHI 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 has adopted a complete life cycle approach for record-level third-party data requests. As part of that life cycle, the Privacy and Legal Services branch 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, the Privacy and Legal Services branch contacts third-party data recipients on an annual basis to certify that they continue to comply with their obligations as set out in the data request form and data protection agreement signed with CIHI.

Public release

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 tools such as YHS: In Brief and YHS: In Depth.

Limiting retention

The CAD form 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, the CAD are 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 CAD data.

3.9 Principle 7: Safeguards for personal health information

CIHI's Privacy and Security Framework

CIHI has developed a [Privacy and Security Framework](#) to provide a comprehensive approach to 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 CAD 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 de-identified record-level data, where the HCN has been removed or encrypted upon first receipt. In exceptional instances, staff will require access to original HCNs. CIHI's internal Privacy (2010) policy and procedures, 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 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 at 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, who may direct an inquiry or complaint to the privacy commissioner of the jurisdiction of the person making the inquiry or complaint.

4 Conclusion

CIHI's assessment of the CAD identified 1 privacy/security risk (see [Section 3.1](#)).

Any recommendations resulting from a PIA, including those arising from PSRM assessments initiated because of a PIA, are tracked in the Corporate Action Plan Master Log of Recommendations, and monitoring and follow-up action is taken accordingly to ensure implementation.

This PIA will be updated or renewed in compliance with CIHI's [Privacy Impact Assessment Policy, August 2017](#).

Appendix: Text alternative for figure

Data collection by CIHI: Once authenticated through CIHI's access management system processes for granting and revoking access, CAD data providers submit record-level data to CIHI through CIHI's secure web-based electronic Data Submission Services.

Internal data processing following collection by CIHI: All data submitted to CIHI undergoes data processing and a data quality check for errors and inconsistencies before being integrated into the respective database within CIHI's production database. Error and validation reports generated at the time of processing are made available to the respective data providers via the Common Document Dissemination Service in compliance with CIHI's *Secure Information Transfer Standard*.

CIHI return, disclosure and use of data: CIHI staff access data within the SAS analytical environment on a need-to-know basis, to return data to original data provider, to fulfill third-party data requests, and to release aggregate statistics and analyses to the public.



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

20832-1019

