# Secure Access Environment

## Privacy Impact Assessment

June 2021

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.



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. *Secure Access Environment Privacy Impact Assessment*. Ottawa, ON: CIHI; 2021.

Cette publication est aussi disponible en français sous le titre *Évaluation des incidences sur la vie privée de l'environnement d'accès sécurisé*.

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

- *Secure Access Environment Privacy Impact Assessment*

Approved by

Brent Diverty
Vice President, Data Strategies and Statistics

Rhonda Wing
Executive Director, Chief Privacy Officer
and General Counsel

Ottawa June 2021

# Table of contents

# Quick facts about CIHI's Secure Access Environment

Historically, the Canadian Institute for Health Information (CIHI) has provided researchers and other approved users with access to de-identified data from our data holdings by extracting the relevant data into files and sending the files to the users. Many leading data institutes and research organizations have moved away from this approach and are now using secure access environments (SAEs) similar to CIHI's SAE, which is described here.

Here are some key facts about CIHI's SAE:

- CIHI's SAE is an encrypted, secure environment hosted in CIHI's data centre.
- Consistent with CIHI's existing policies and procedures, only approved researchers or analysts have access to the SAE (for purposes of this privacy impact assessment, these users are all subsequently referred to as "researchers").
- Researchers' access is limited to folders containing data extracts that have been prepared and vetted by CIHI staff for an approved research project.
- Access is through secure, encrypted, approved user accounts, which have strong password protection and two-factor authentication.
- Only aggregate results can be extracted from the SAE, in accordance with CIHI's existing policies and procedures.
- Approved users are subject to stringent agreement terms.

# 1 Introduction

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

The purpose of this privacy impact assessment (PIA) is to examine the privacy, confidentiality and security risks associated with CIHI's Secure Access Environment (SAE), which is used by third-party data requestors of record-level CIHI data for research purposes. This PIA has been completed in compliance with our *Privacy Impact Assessment Policy* and our *Privacy and Security Risk Management Framework*.

# 2 Background

## 2.1 Introduction to the SAE

Through CIHI's data request process, CIHI makes analysis-ready files available to third parties for research, always subject to our privacy policies and jurisdictional data-sharing agreements. Before CIHI established the SAE, we released record-level data directly to third parties either on an encrypted and password-protected CD/DVD or via the Data Dissemination Tool. CIHI's SAE is intended to further strengthen CIHI's disclosure process by addressing the following challenges:

- Monitoring compliance with information security requirements and authorized access;
- Streamlining the lengthy data destruction/follow-up process; and
- Enabling collaborative research (where researchers from multiple institutions may want to access the same data sets).

To advance our data disclosure processes and infrastructure, CIHI initiated a project to create the SAE, which provides controlled remote access to CIHI data via secure and encrypted sessions. The SAE eliminates risks of losing data in transit, enables us to more easily monitor compliance with information security requirements, and supports collaborative research by enabling researchers from different institutions to access the same data in the SAE.

For many years, CIHI has been a trusted source of support for approved researchers, decision-makers and health system managers, providing them with aggregate or record-level data from 1 or more of our databases through our third-party data request process (see Make a data request), which is governed by our privacy policies:

- *Privacy Policy on the Collection, Use, Disclosure and Retention of Personal Health Information and De-Identified Data*
- *Privacy Policy on the Collection, Use, Disclosure and Retention of Health Workforce Personal Information and De-Identified Data*

Through our third-party data request process, we disclose data at the highest degree of de-identification while still meeting approved research or analytical purposes. Once a project is approved, CIHI staff work with the requesters to prepare de-identified, customized, analysis-ready data sets that include only those data elements necessary to meet the identified research or analytical purposes.

For years, we have disclosed data sets by securely sending copies to users. Thanks to technological developments such as cloud services and encryption, more and more data holders are creating SAEs in which to conduct research or analysis using data. This prevents data from leaving the SAE, as users are restricted to accessing data remotely and working with it inside the environment.

Like other such programs, CIHI's SAE provides secure and controlled remote access to customized record-level data sets and analytical tools to authorized users. In its initial roll-out, the SAE will provide access to de-identified record-level CIHI data only. While most users will access only de-identified data in the SAE, some may be permitted access to personal health information under Section 44 of Ontario's *Personal Health Information Protection Act* or by informed consent. At such time as authorized access to personal health information or health workforce personal information is permitted through the SAE, this PIA will be updated.

The SAE is hosted on and operated from servers located in Canada. This complies with all relevant requirements under agreements with our data providers.

Access to the SAE is controlled using secure and encrypted remote desktop connection and two-factor authentication. In other words, access to the SAE requires multi-factor authentication, which ensures the security of connections and prevents unauthorized access. The SAE is protected by a firewall. No internet access is permitted from within the SAE. The SAE provides secure storage and back-up for authorized project data.

The safety and security of data accessed through the SAE are also ensured by user agreements and terms of use specific to the SAE.

The SAE provides central administration of project and user accounts. Approved project team members can collaborate with each other and view each other's results in the SAE. Research is facilitated in the SAE by enabling access to different analytical utilities such as SAS and Microsoft Office.

Record-level data cannot be copied or removed from the SAE. Only aggregate outputs that have been reviewed by CIHI staff can leave the SAE, to prevent inadvertent disclosure of confidential personal health information or health workforce personal information.

## 2.2 No new data collection

The SAE does not involve data collection by CIHI. It replaces our traditional method of disclosing to third-party requestors data from our existing data holdings in a de-identified form or, where permitted, under Section 44 of Ontario's *Personal Health Information Protection Act* or by consent of the individual. However, the SAE will permit authorized users to upload their own data into the SAE, for analysis in the SAE in relation to CIHI data files that have been prepared and made available for their project. CIHI has administrative and technical controls in place to ensure that only users who are authorized to upload data can do so, and CIHI will review the data prior to it being uploaded into the SAE.

Because no new data collection by CIHI is involved, this PIA does not follow the standard format of other PIAs published by CIHI. Its focus is to assess implementation of required administrative and technical controls to ensure the privacy, confidentiality and security of the data accessed by third-party data requestors in the SAE.

The next section describes CIHI's Privacy and Security Risk Management Program, which has played an integral role in the development and implementation of measures to support the privacy and security of CIHI's SAE.

# 3 Privacy and security 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. 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.

As a result of this PSRM process, 13 privacy/security risks were identified. These risks were added to CIHI's Privacy and Security Risk Register and were assessed and addressed in accordance with CIHI's PSRM methodology. These risks have been sufficiently mitigated to meet CIHI's privacy and security risk tolerance level of low.

# 3.2 Authorities governing SAE data

## General

As noted earlier, the SAE does not involve CIHI collecting data that it does not already hold. The SAE provides a more secure method for enabling authorized users of data to access and use approved data files. As with all of our other relevant activities, CIHI adheres to our *Privacy Policy, 2010* and to any applicable privacy legislation and/or legal agreements.

Authorized researchers will be allowed, in certain approved and controlled circumstances, to upload data for purposes of linkage to CIHI data. CIHI will, in addressing requests to upload data, assess privacy compliance issues associated with the proposal and either decline permission or implement appropriate privacy measures.

## Accountability and governance of the SAE

The following table identifies key internal senior positions with responsibilities in terms of PSRM for the SAE:

**Table** Key positions and responsibilities

| Position/group | Role/responsibilities |
|---|---|
| Vice President, Data Strategies and Statistics | Responsible for the overall strategic direction of the SAE |
| Director, Acute and AmbulatoryCare Information Services | Responsible for the overall operations and strategic business decisions of the SAE |
| Manager, Decision Support, Corporate Data Request Program and Trauma | Responsible for the ongoing management, development and deployment of the SAE. The manager makes operational decisions about the SAE and manages consultation with internal and external stakeholders for the SAE as appropriate. |
| Chief Information Security Officer | Responsible for the strategic direction and overall implementation ofCIHI's Information Security Program |
| Chief Privacy Officer | Responsible for the strategic direction and overall implementation of CIHI's Privacy Program |

# SAE privacy and security–related processes and safeguards

## Identity and access management

Only researchers whose projects are approved in accordance with CIHI's existing policies and procedures may access the SAE. Researchers will be required to provide the following information as part of the access request process:

- Name
- Position
- Organization
- Address
- Organizational email address
- Research ethics board approval for the proposed study

This information must be provided for the principal researcher and all researchers proposed to be authorized to access the SAE for the research project.

The responsible CIHI program area then confirms the status of the researchers through an online search and further inquiries if warranted. Any request for a change by an SAE user triggers a re-engagement with the user.

Our Secure Access Environment Agreement must be signed by an individual with authorized signing authority for the organization with which the research is affiliated, and also by the individual who is leading the research project and who is accountable for all researchers working on the project in the SAE. The agreement binds both the organization and the individual who is leading the research project to terms specific to the SAE and its use. In addition, each researcher with access to the SAE must sign the Secure Access Environment Terms of Use.

Approved users are also supported by our *SAE User Guide*. This guide includes instructions on the SAE's technical safeguards and related requirements. These include using only computers provided by the user's employer or institution, installing and using SFTP capabilities, and using two-factor authentication through Cisco's Duo app.

The *SAE User Guide* sets out step-by-step instructions on how to access and use the SAE. It also details how users can interact with our technical staff, to better support users' compliance with our privacy and security requirements.

A key contractual condition for all users is that they will be prohibited from accessing the SAE from outside Canada.

## Authorized projects

Use of the SAE is restricted to users whose projects are approved in accordance with CIHI's existing policies and procedures. When a request is received, CIHI assesses the intended use of data and approves the project only if it is consistent with CIHI's mandate and core functions (as described in Section 37 of CIHI's *Privacy Policy, 2010*), as well as any other applicable legislation. In addition, for all authorized projects, CIHI ensures that requestors enter into legally binding agreements with CIHI for the appropriate use and protection of the data, and that only data elements necessary to meet the identified purposes are disclosed.

## Data linkage

Approved third-party projects may include requirements for data linkages between data files held by CIHI (e.g., between data files for the Discharge Abstract Database and the National Ambulatory Care Reporting System), as well as for linkages between CIHI data files and researcher-provided data files.

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. All third-party requests for data linkage are subject to an internal review and approval process. When carrying out data linkages, CIHI uses consistently encrypted health care numbers. The linked data in any case remains subject to CIHI's *Privacy Policy, 2010*.

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

The individuals whose personal health information is used for data linkage have consented to the data linkage (Section 23) or the following criteria have been met (Section 24):

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 of CIHI's *Privacy Policy, 2010*; 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 of CIHI's *Privacy Policy, 2010*; and
f. The data linkage has demonstrable savings over other alternatives or is the only practical alternative.

## Data disclosure/de-identification in the SAE

Access to data files in the SAE is a disclosure and must be authorized in accordance with CIHI's *Privacy Policy, 2010*. While most users will access only de-identified data in the SAE, some may be permitted access to personal health information under Section 44 of Ontario's *Personal Health Information Protection Act* or by informed consent. In the initial phase, the scope of the SAE is limited to access to de-identified data. An update to this PIA will be undertaken if access to personally identifiable information is permitted in the future.

Record-level de-identified data files are vetted through CIHI's Privacy Analytics Eclipse data de-identification tool before they are released into the SAE, where applicable. A compliance report is included as part of the documentation to approve release into the SAE. Record-level de-identified data files that are not run through the Privacy Analytics Eclipse data de-identification tool must be screened by a senior methodologist in CIHI's Methodology Unit before they are released into the SAE.

## Access to the SAE from outside of Canada

Access to the SAE from outside of Canada is prohibited; this is a contractual condition for all users. CIHI has implemented technical and administrative controls to address this requirement.

## Outputs

To prevent inadvertent disclosure of confidential personal health information or health workforce personal information, only aggregate outputs that have been reviewed by CIHI staff can leave the SAE. Contractual controls in the Secure Access Environment Agreement and Secure Access Environment Terms of Use stipulate that the user can export only aggregate outputs that have been reviewed by CIHI, and explicitly prohibit the user from copying, exporting or otherwise reproducing the CIHI data (including taking photos). CIHI has also implemented technical controls to prevent copying data using copy and paste tools. As well, CIHI staff manually review all output files and source codes requested for removal from the SAE and through that process will detect any attempts to copy data into document management applications or files.

## Auditing and monitoring

Access to the SAE is provided through a centralized SAE user access process. This process enables CIHI to control user access and to on-board and off-board users to and from the SAE. Approved users are subject to an annual audit to verify active users and their access. Access is revoked and accounts are closed for any user accounts identified as dormant through this annual audit process.

# 4 Conclusion

All of the risks identified through the PSRM assessment of the SAE have been sufficiently mitigated to meet CIHI's privacy and security risk tolerance level of low.

This PIA will be updated or renewed in compliance with our *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

24695-0721