for Heal

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.

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

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

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

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*
-

3 Privacy and security analysis

3.1 Privacy and Security Risk Management Program

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

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*

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

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