

# CIHI's Secure Access Environment (SAE)

Presentation to the Health Analytics Community

Canadian Institute for Health Information

# Presentation Outline



1. About CIHI
2. SAE at-a-glance
3. Identity and Access Management
4. SAE Outputs
5. Questions and Discussion

# About CIHI

CIHI is an independent, not-for-profit organization that provides essential information and insight on Canada's health system and the health of Canadians. [CIHI - What we do - YouTube](#)

## Vision

**Better data.  
Better decisions.  
Healthier Canadians.**

## Mandate

Deliver comparable and actionable information to accelerate improvements in health care, health system performance and population health across the continuum of care.

## Values

Respect • Integrity • Collaboration • Excellence • Innovation

**Better data, better decisions, healthier Canadians:**

powered by a shared sense of purpose, the highest standards of excellence and trust.

# CIHI's Health and Health System Data & Information



## Types of care

- Hospital and emergency
- Mental health
- Home care
- Long-term care
- Rehabilitation
- Pharmaceuticals
- Clinical registries: organ transplant/renal, hip and knee replacements; trauma
- More



## Patient-reported data

- Patient-reported outcome measures (PROMs)
- Patient-reported experience measures (PREMs)



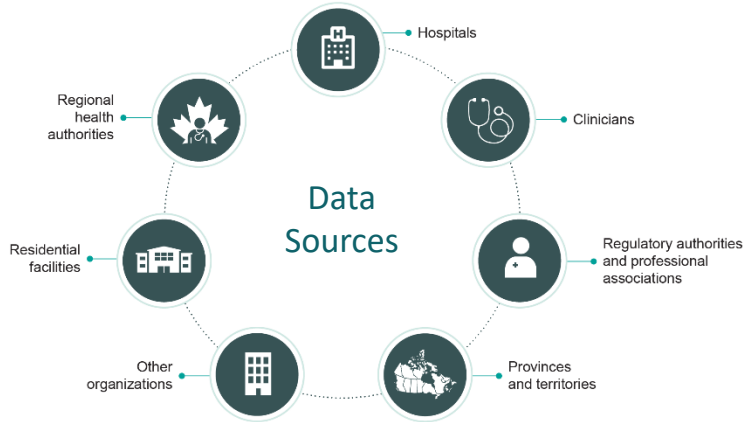
## Health spending

- Patient costing data
- Hospital and regional health authority financial accounts
- Physician billing
- System-wide health expenditures



## Health workforce

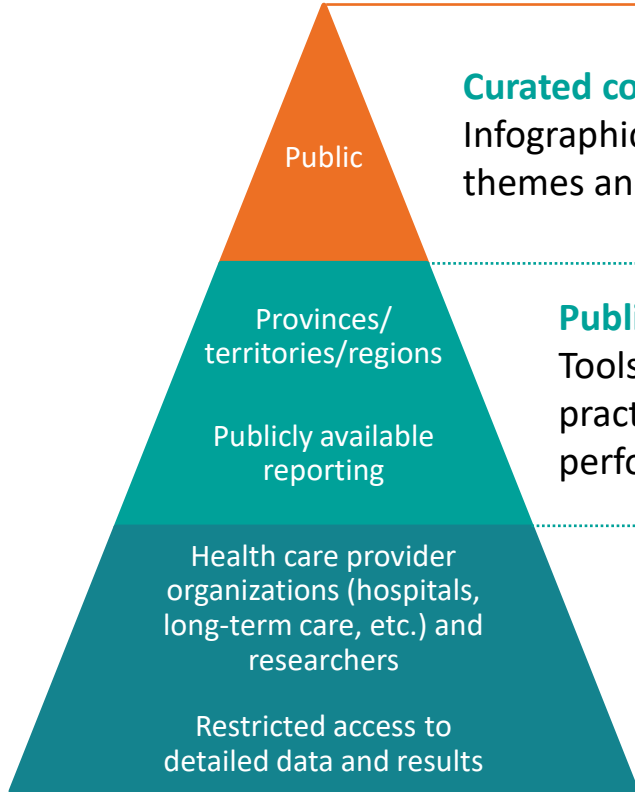
- Physicians
- Nurses
- Occupational therapists
- Pharmacists
- Physiotherapists
- Allied health professionals
- More



**CIHI strives to provide high quality, standardized data, and information to help with pan-Canadian, and international comparisons**

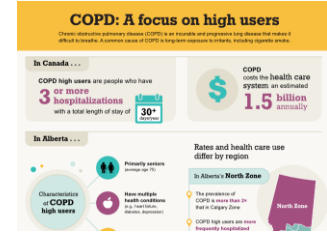
**CIHI data and information is used by health ministries, regional health authorities, hospital administrators, clinicians, researchers, journalist and students**

# Making CIHI data available



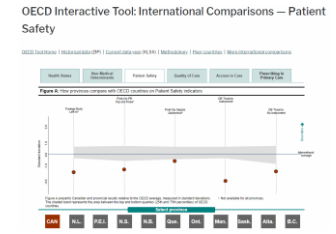
## Curated content

Infographics on emerging issues, priority themes and populations



## Public data hub

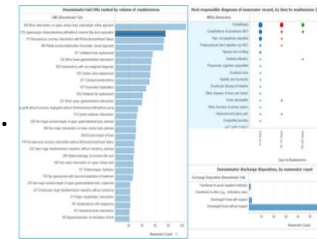
Tools with aggregated results to support best practices, knowledge sharing and performance improvement



## Secured data access

Tools to support exploring and understanding performance results, as well as data validation.

CIHI's **Secure Access Environment** makes data more accessible for custom use.



# Custom Data Requests at CIHI - Overview

	Aggregate Data Requests	Record-Level Data Requests
Types of data	Tabulations and data summaries (e.g. counts, means, median) Indicator/rate calculations	De-identified records on health care events / patients
Output Format	Data tables (typically in Excel)	SAS, or comma-delimited text files
Documentation required for requesting data	Aggregate Data Request Form and Non-Disclosure/ Confidentiality Agreement	Record-level Data Request Form and Non-Disclosure/Confidentiality Agreement
		<del>Information Security Form</del> SAE Agreement and Terms of Use
		REB Approval and Study Protocol
Types of requestors	Researchers from academic institutions, research organizations, clinician groups, graduate students, for-profit	Researchers from academic institutions, research organizations, clinician groups, graduate students

# Secure Access Environment for 3<sup>rd</sup> Party Data Requests



## What is CIHI's Secure Access Environment (SAE)?

- CIHI's SAE is a secure environment hosted in CIHI's Cloud environment
- Only approved researchers or analysts have access to the SAE, in accordance with CIHI's existing policies and procedures
- 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, with 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

# CIHI's Secure Access Environment (SAE)

Operational as  
of January 2022



## What data can be accessed via the SAE?

- De-identified, record-level CIHI data for custom data requests; linkable with approved research cohort data

## What tools are available in the SAE?

- SAS 9.4M7 and SAS EG 8.3
- R
- Python
- MS Word, Excel, PowerPoint

## What are the Benefits for the SAE users?

- **Remote access** from any institution-issued device; compatible with any operating system
- Access to **metadata** within SAE
- Can share data/code amongst authorized project team members to **collaborate/view** results
- Relieve user of security requirements for on-site data management

SAE Access fee: \$2,500 per year for up to 3 users per project  
Each additional user: \$1,500 per year

# SAE Identity and Access Management



1. Researcher signs SAE Agreement & Terms of Use

2. CIHI adds new user(s) and grant access to SAE project

3. CIHI uploads CIHI Datasets and Researchers Datasets to SAE

4. Authorized users access the environment

- User is reminded of *Terms of Use* at each login
- *Terms of Use* available for download at any time
- CIHI authenticates users (organizational credentials; ethics review and approval)
- CIHI datasets are de-identified
- Researcher cannot upload files into SAE; CIHI reviews and uploads all files to the SAE
- 2-factor authentication to validate authorized users
- Complex password requirement
- User access is removed once project is closed or when CIHI receives request to remove user

# SAE Folder Setup



**SAE authorized users can only access their own data for the authorized project, and data shared within the same authorized project. Sharing of data across projects is not possible.**

- Authorized users have read-only access to the original data provided by CIHI and stored in the unique DATA folder
- Research project team members with active SAE accounts (i.e. authorized users) can collaborate and view results in the SHARED folder
- Each user has access to their own PERSONAL folder. This is a private folder that cannot be accessed by any other user.
- Aggregate level outputs and other research materials have to be saved in the VETTING folder prior to making a request to remove them from the SAE
- Metadata documentation and a copy of the *Terms of Use* is available

# SAE Terms of Use



**SAE Terms of Use prohibit users from the following:**

- Disclose the information accessed through the SAE to anyone or in any way
- Copy, export, print, share, or otherwise reproduce outside of the SAE the information accessed
- Share user credentials or log in using someone else's user credentials
- Access the SAE from outside of Canada
- Access the SAE and the information disclosed for any purpose other than the research project identified in the Terms of Use
- Access more than one research project within the SAE at a time, or move/reproduce any information to another research project location within the SAE
- Attempt to use the information disclosed to identify or contact any individual or health facility
- Merge, link or otherwise combine the information disclosed with any other information beyond what has been identified in the request form

# SAE Output Review



## All outputs to be removed from the SAE must be reviewed and approved by CIHI staff

- Absolutely no record-level data can be included in any documents and/or files to be removed from the SAE
- SAS datasets (.sas7bdat) cannot be removed from SAE
- Outputs and analyses must minimize the risk of re-identifying of individuals
- **SAE User Guide** provides guidance re: handling geography, counts/rates and statistics, and recommends techniques such as suppression, aggregation, rounding, etc.
- Users need to create a “Read Me” file describing the outputs to be vetted to support CIHI review

# SAE Project Closure and Audit



5. CIHI removes existing user(s) and revokes access at end of project

6. CIHI completes data backup and archiving

## Annual audit

- CIHI deletes user accounts, duo accounts, Amazon Web Services (AWS) WorkSpaces, etc.
- CIHI deactivates access by users to project folders
- CIHI deletes all project folders from the SAE
- CIHI backs up project data folder for 6 months, based on CIHI backup policy
- CIHI verifies active users and their access
- CIHI revokes access and closes accounts if user accounts identified as dormant

# SAE Project Closure and Audit



5. CIHI removes existing user(s) and revokes access at end of project

6. CIHI completes data backup and archiving

## Annual audit

- CIHI deletes user accounts, duo accounts, Amazon Web Services (AWS) WorkSpaces, etc.
- CIHI deactivates access by users to project folders
- CIHI deletes all project folders from the SAE
- CIHI backs up project data folder for 6 months, based on CIHI backup policy
- CIHI verifies active users and their access
- CIHI revokes access and closes accounts if user accounts identified as dormant

# Make a data request

## ACCESS DATA AND REPORTS

Topics

Indicators +

Reports and releases

Data tables

Tools

Data holdings -

Using Provisional Data

Make a Data Request

## CIHI's Secure Access Environment (SAE)

### What is CIHI's SAE?

The SAE gives authorized individuals secure and controlled remote access to customized record-level data sets and analytical tools. It is hosted in CIHI's cloud-based environment. Access to the SAE is facilitated via secure and encrypted remote desktop connection and use of multi-factor authentication.

### What type of data can be accessed via the SAE?

Currently, the SAE provides access to de-identified record-level CIHI data only. Disclosures of personal health information (PHI) by CIHI are subject to the specific jurisdictional legislation and agreements under which the data was originally collected and shared with CIHI. The SAE does not currently support access to PHI.

### What security features does the SAE have?

- The SAE is protected by a firewall. No internet access is permitted from within the SAE.
- The SAE provides central administration of project and user accounts.
- Access to the SAE requires multi-factor authentication, which ensures the privacy of the connection and prevents unauthorized access.
- Through contractual obligations, users are prohibited from accessing the SAE from outside Canada.
- Only aggregate outputs that adhere to CIHI's vetting rules may leave the SAE. This prevents inadvertent disclosure of confidential personal health information.
- Record-level data cannot be copied or removed from the SAE.
- The SAE provides secure storage and back-up for authorized project data.

### What user features does the SAE have?

Project team members can

- Share data and code
- Collaborate and view each other's results
- Access SAS and Microsoft Office utilities

# For more information:

CIHI's [Make A Data Request](#) page

# Questions and Discussion





Canadian Institute for Health Information

**Better data. Better decisions. Healthier Canadians.**



cihi.ca