ICES is an independent, not-for-profit research institute made up of a community of research, data and clinical experts. We work with Ontario's health-related data and aim to inform health system policy and planning to improve the health of all Ontarians. Our organization receives core funding from the Ontario Ministry of Health.

PRIVACY & CYBERSECURITY

Since 1992, the Ontario government has entrusted ICES with securing its administrative data to evaluate and improve Ontario's health system. We have a vital role in the health care system and are accountable to the public, the provincial government, and the Information and Privacy Commissioner of Ontario to use data appropriately. The Information and Privacy Commissioner oversees the *Freedom of Information and Protection of Privacy Act*, the *Municipal Freedom of Information and Protection of Privacy Act* and the *Personal Health Information Protection Act*.

Learn more about the different kinds of data that ICES holds.

We are able to collect and use data through:

- **Federal and Provincial Legislation.** ICES is a Prescribed Entity under PHIPA regulations. This designation enables ICES to compile and analyze statistics about the management and effectiveness of health care in Ontario.

- **Contracts**. Agreements with data providers define the way ICES uses and safeguards data.

How we protect data

Policies and processes

Data security is foundational to our work. All data handling processes are built on the privacy and security policies required by the Information and Privacy Commissioner of Ontario.

Cybersecurity

Within our internet-connected work environment, we maintain cybersecurity best practices to protect ICES hardware, software and data from information disclosure, theft or damage. ICES uses complex passcodes and encryption and applies the framework set by the National Institute of Standards and Technology to manage cybersecurity-related risk.

Data desensitization

A restricted group of ICES staff removes direct personal information, such as name and health card number, and replaces it with a unique, anonymous ICES identifier. ICES prohibits unauthorized reidentification of individuals. We use methods such as coding techniques, data quality and destruction procedures, and re-identification risk assessments to ensure that individuals cannot be identified during the data linkage process or at any research stage.

Data collection and access

We limit data collection to what is necessary and lawful. Data access is administered on a project-by-project basis, and scientists must apply for and justify the use of all requested data. Researchers can access health data on individuals on our secure servers only after the data has been desensitized and its quality confirmed.

Learn more about ICES privacy and cybersecurity.

STAY CONNECTED