



# PRIVACY POLICY

Policy Section Name	Policy Category	Policy Number	Supersedes
Privacy	Privacy	800PR-PR-001	NA
Organizational Scope	IPC (Yes/No)	Effective Date	Next Review Date
ICES-Network (no site-specific procedures)	Yes	January 2014	May 2021
Authority (Title)		Owner (Title)	
Chief Privacy and Legal Officer		Chief Privacy and Legal Officer	
Required Reviewers			
Chief Executive Officer		Local Privacy & Security Officers	

## GLOSSARY OF TERMS

Please refer to the [glossary](#) for terms and definitions.

List of terms: **Agent; De-Identified Data; Direct Personal Identifier; ICES Analytic Staff; ICES Data; ICES Employee; ICES Scientist; ICES Student; Knowledge User; Personally Identifiable Information; Prescribed Entity; Prescribed Registry; Privacy Complaint; Privacy Information; Privacy Inquiry; Privacy Impact Assessment; Privacy Incident; Research; Risk-Reduced Coded Data; Security Incident; Third Party Researchers**

### 1. PURPOSE

The purpose of this policy is to provide an overarching description of ICES' collection, use and disclosure of Personally Identifiable Information and ICES' approach to its protection.

### 2. POLICY SCOPE

This policy applies to all activities of ICES involving Personally Identifiable Information collected by ICES, and any derivatives of that information.

#### 3a. POLICY STATEMENT

ICES relies on its ability to collect and use information that is subject to privacy laws, and is committed to its protection in accordance with applicable law, Research Ethics Board (REB) approvals and contractual obligations.

#### 3b. POLICY DETAIL

##### Prescribed Entity

ICES is a Prescribed Entity under s. 18(1) of O. Reg. 329/04 under Ontario's *Personal Health Information Protection Act* (PHIPA), and is committed to protecting the Personal Health Information (PHI) it collects in accordance with PHIPA and its regulation. ICES implements the privacy and security policies, procedures and practices required to protect PHI, which are subject to review and approval by the Information and Privacy Commissioner of Ontario every three years. ICES is responsible for its employees' and agents'



# PRIVACY POLICY

compliance with those policies, procedures and practices, and enables this through mandatory training and agreements.

## The Information ICES Collects and Why

A high proportion of ICES' scientific programs and services involve the collection or use of information that is subject to privacy law (collectively, "Personally Identifiable Information"). Such programs and services include

- Health system analysis and evaluation conducted by ICES, independently or on behalf of policy-makers and health care providers;
- Health-related Research conducted by ICES; and
- Augmenting information collected by Third Party Researchers in accordance with applicable law and REB approvals.

ICES also collects Personally Identifiable Information as needed to manage the day-to-day activities of the institute.

The types of Personally Identifiable Information ICES collects include

- PHI collected by health information custodians, like hospitals;
- PHI collected by other Prescribed Entities and Prescribed Registries;
- PHI and other personal information collected Third Party Researchers;
- Personal information collected by other organizations in the public and private sectors; and
- Personal information ICES collects to manage its relationships with employees, affiliated individuals and others who interact with ICES.

## How ICES Protects Privacy

ICES recognizes that Personally Identifiable Information is inherently sensitive, and is responsible for ensuring it is protected in accordance with its policies and procedures as a Prescribed Entity, PHIPA and its regulation, other applicable law, REB approvals and contractual obligations. ICES has therefore adopted the following key principles, which guide its handling of Personally Identifiable Information:

1. ICES collects Personally Identifiable Information only in accordance with applicable law and REB approvals.
2. ICES collects no more Personally Identifiable Information than is reasonably necessary and only when other information will not serve the purpose.
3. ICES implements a range of administrative, technical and physical safeguards to protect Personally Identifiable Information. These include removal of Direct Personal Identifiers and assignment of a confidential ICES Identifier or code before making it available to ICES Analytic Staff, ICES Employees and Agents who conduct health systems analysis and evaluation or health-related Research use this Coded Data. Third Party Researchers are permitted to access Risk-reduced Coded Data on ICES-controlled systems. Subject to section 5, only De-identified Data is released to



# PRIVACY POLICY

Third Party Researchers or Knowledge Users or for publication. Disclosure of Personally Identifiable Information to any Knowledge User is strictly prohibited.

ICES also takes steps to transfer, retain and destroy Personally Identifiable Information securely. These include an encrypted file transfer system that protects both inbound and outbound electronic files, and a prohibition against transferring paper with Direct Personal Identifiers. Personally Identifiable Information with Direct Personal Identifiers is retained only temporarily. It is isolated in secure network folders and cabinets until data quality issues have been resolved, and is then securely destroyed by an ICES-approved method such as cross-cut shredding for paper or secure wiping or physical destruction for media and devices.

4. ICES subjects all requests to conduct health system evaluation or Research to a Privacy Impact Assessment to verify compliance with ICES policies and procedures and applicable law and REB approvals. In addition, each year ICES submits a report of its activities to the Research Ethics Board of Sunnybrook Hospital for modified expedited review.
5. ICES does not disclose Personally Identifiable Information, subject to the following exceptions:
  - a. To Prescribed Entities and Prescribed Registries for their prescribed purposes, as permitted by sections 45 and 39(1)(c) of PHIPA and a contract, and verified through a Privacy Impact Assessment.
  - b. To define cohorts for Third Party Researchers for the purposes of publicly funded research that cannot be reasonably conducted within ICES, as permitted by section 44 of PHIPA and a contract, and verified through a Privacy Impact Assessment.

In such cases, ICES discloses Personally Identifiable Information only where other information will not serve the purpose and only to the extent reasonably required for the purpose.

## **Privacy Information, Privacy Inquiries and Privacy Complaints**

ICES strives to be transparent, and enables individuals to make Privacy Inquiries and Privacy Complaints about its privacy policies, procedures and practices. To this end, the Chief Privacy and Legal Officer (CPLO) is responsible for ensuring that a list of ICES Data Holdings, together with information about ICES' privacy practices and information about how to make Privacy Inquiries and Privacy Complaints (collectively Privacy Information), are published on ICES' website. The Privacy Information shall inform individuals that they may make Privacy Inquiries and Privacy Complaints directly to the CPLO, verbally and in writing, at

Institute for Clinical Evaluative Sciences  
G-106 - 2075 Bayview Avenue  
Toronto, Ontario M4N 3M5

Telephone: 416-480-4055  
Fax: 416-480-6048  
Email: [privacy@ices.on.ca](mailto:privacy@ices.on.ca)



# PRIVACY POLICY

The Privacy Information shall also state that individuals may direct Privacy Complaints regarding ICES' compliance with its duties as a Prescribed Entity to the Information and Privacy Commissioner of Ontario at

Office of the Information and Privacy Commissioner of Ontario  
1400 – 2 Bloor Street East  
Toronto, Ontario M4W 1A8

Telephone: 416-326-3333 / 1-800-387-0073  
Fax: 416-325-9195  
Email: [info@ipc.on.ca](mailto:info@ipc.on.ca)

## Accountability

ICES' Chief Executive Officer (CEO) is responsible for ensuring that ICES defines and implements the policies, procedures and practices that are necessary to achieve the objectives of this Privacy Policy. At a minimum, this shall include

- Seeking and implementing the policies, procedures and practices necessary to maintain the designation of Prescribed Entity under s. 18(1) of O. Reg. 329/04, and comply with PHIPA and its regulation, as amended from time to time;
- Appointing and overseeing a CPLO with combined responsibility for privacy and security, whose role it is to design and oversee a control environment that is appropriate, taking into account ICES' obligations as a Prescribed Entity, which include responsibility for the development, revision, approval, communication and implementation of required policies and procedures and processes for the effective prevention, detection and response of Privacy Incidents and Security Incidents;
- Ensuring the necessary budgets and agreements are in place to maintain a team of privacy officers, reporting to the CPLO and located at ICES Central and across the ICES network, for the day-to-day management of privacy across ICES; and
- Taking the steps necessary to ensure reporting of privacy breaches and complaints and an annual written update on the status of ICES' program to the Audit and Risk Committee of the ICES Board of Directors, which addresses privacy training, the development and implementation of privacy policies and procedures, privacy audits and Privacy Impact Assessments, and associated recommendations and their status.

## 4. RELATED PROCEDURES

[ICES Privacy Policies & Procedures Log](#)

## 5. TRAINING AND COMMUNICATION

This policy and its administrative procedures are to be communicated to all ICES Employees, ICES Scientists and ICES Students across the network, and addressed in the ICES Privacy Orientation.



# PRIVACY POLICY

Policies are available on the ICES Intranet. Employees and contractors are made aware of applicable policies during onboarding. Policy awareness is supported and promoted by the Policy Owner.

## 6. COMPLIANCE AND ENFORCEMENT

Compliance to all ICES policies and procedures is subject to audit and review.

Suspected violations of policies should be reported to the appropriate authorities. The information will be reviewed by the appropriate authorities, including Human Resources, as required.

Policy violations due to human error or operational procedure gaps/deficiencies will be addressed through training and/or modifications to procedures as required.

All other violations may be subject to a range of disciplinary actions including warning, temporary or permanent loss of access privileges, legal sanctions and/or termination of employment or contract with ICES.

## 7. CROSS REFERENCES / RELATED DOCUMENTATION

## 8. ADDITIONAL INFORMATION

*IPC Manual for the Review and Approval of Prescribed Persons and Prescribed Entities*, s. 1(1), 1(10),1(12), 4(1)

## 9. CHANGE TRACKING TABLE

Review Date	Change Description	Changed By	Reviewed By	Policy Status
January 2014		CPO		Archived
October 2014	Edits	CPO		Archived
October 2016	Updated to reflect: (1) CPCO responsibility for security; (2) correct characterization of data provided to third party researchers; (3) cohort disclosure; (4) decommissioning of hosting services.		CEO, LPSOs	Archived
March 2018	Names removed under required reviewers; titles updated; formatting changes	Corporate PM	Privacy	Archived
May 2019	Updated role title, new template; changed information about ICES as a PE to s. 18(1) of O. Reg. 329/04, as ICES is not prescribed as a PE under s. 45 of PHIPA	Manager, Privacy & Compliance	N/A	Archived



# PRIVACY POLICY

May 2020	N/A (annual review)	N/A	Manager, Privacy & Compliance	In Effect
----------	---------------------	-----	-------------------------------	-----------