Privacy Policy

Department	Document Number	Organizational Scope	ICES Site	IPC Scope
PLO	PO.005	ICES Network Policy	ICES Network	All Acts
Original Date (month yyyy)	**Last Review Date** (month yyyy)	**Frequency of review** (month yyyy)	**Next Review Due Date** (month yyyy)	**Supersedes (if applicable)**
January 2014	September 2022	Triennially	September 2025	800PR-PR-001

Authority (Title)	Policy Owner (Title)
Chief Privacy and Legal Officer	Director, PLO

Required Reviewers (Titles)		
N/A		

Please refer to the **glossary** for terms and definitions.

1.0 PURPOSE

1.1 This **Policy** provides the general principles that form the lawful basis for ICES' collection, use, disclosure, and handling practices of **Personal Health Information (PHI)** and **Personal Information (PI)**.

1.2 This **Policy** supports a clear mandate for ICES' robust compliance regime in relation to **PHI/PI**.

1.3 This **Policy** identifies the primary roles and responsibilities for ICES' privacy program.

1.4 This **Policy** sets out ICES' approach to protection **of PHI/PI**.

2.0 SCOPE

2.1 This **Policy** applies to all activities of ICES involving **ICES Data** collected, used, disclosed or otherwise handled by ICES, and any derivatives of that **ICES Data**.

3.0 ROLES AND RESPONSIBILITIES

3.1 ICES **Chief Executive Officer ("CEO")** is responsible for ensuring that ICES defines and implements the **Policies**, **Procedures,** and **Practices** that are necessary for compliance with this **Policy**, applicable laws and other legal requirements, including the requirements under the *Personal Health Information Protection Act* **("PHIPA"),** the *Coroners Act,* and their regulations applicable to **Prescribed Entities ("PE")**. At a minimum, this shall include:

3.1.1 Seeking and implementing the **Policies**, **Procedures** and **Practices** necessary to maintain the designation of **Prescribed Entity** under **PHIPA** and the *Coroners Act*, and complying with such statutes and their applicable regulations, as amended from time to time.

3.1.2 Appointing and overseeing an ICES **Chief Privacy and Legal Officer** ("**CPLO**").

3.1.3 Ensuring the necessary budgets and agreements are in place to maintain a team of ICES Privacy **Subject Matter Experts ("SMEs")**, reporting to the ICES **CPLO** or their delegate, and located across the **ICES Network**.

3.1.4 Taking the steps necessary to ensure reporting of **Privacy Incidents** and **Privacy Complaints**.

3.1.5 Final signing-off approval on **Privacy Audits**.

3.1.6 Ensuring there are written updates on the status of ICES' privacy program to the ICES **Finance, Audit & Risk Committee** ("**FAR**") of the ICES **Board of Directors,** which may include privacy training, the development and implementation of privacy **Policies** and **Procedures**, **Privacy Audits** and **Privacy Impact Assessments (PIAs),** associated recommendations, and the status of these recommendations.

3.1.7 Fostering a privacy-minded culture and promoting awareness of and compliance with ICES **Policies**, **Procedures**, and **Practices**.

3.1.8 The ICES **CPLO** reports directly to the ICES **CEO** and is delegated day-to-day authority to manage ICES' privacy and security programs, including:

a. Tthe design and oversight of ICES' **Key Control** environment, with consideration of ICES' obligations as a **Prescribed Entity**, and including responsibility for the development, revision, approval, communication and implementation of required **Policies**, **Procedures**, and **Practices** for the effective prevention, detection, and response to **Privacy Incidents** and **Security Incidents**;

b. The oversight of a team of ICES Privacy **SMEs**, distributed across the **ICES Network**, responsible for ensuring compliance with ICES' **Policies**, **Procedures** and **Practices**, and delivering a range of privacy services, including but not limited to privacy awareness; privacy training; conducting **PIAs**; supporting the development of **Data Sharing Agreements ("DSAs")**; handling **Privacy Incidents** and **Privacy Breaches**; performing or supporting **Privacy Audits**; and responding to a variety of privacy-related consultations; and

c. Ensuring all ICES committees involving discussion, decision, or actions in relation to **PHI/PI** include representation of ICES Privacy **SMEs**. The current list of all ICES committees that include ICES Privacy **SME** representation is set out in ICES' *Privacy and Security Governance and Accountability Policy*.

4.0 DETAILS

4.1 Legal Authorities

4.1.1 ICES is a **Prescribed Entity** under s.18(1) of O. Reg. 329/04 under Ontario's *Personal Health Information Protection Act* **("PHIPA")** for the purposes of s.45 of **PHIPA** and, as such, ICES has the legal authority to collect and use **PHI** for the purpose of analysis or compiling statistical information with respect to the management of, evaluation or monitoring of, or the allocation of resources to or planning for all or part of the health system, including the delivery of services. ICES is committed to complying with the provisions of **PHIPA** and its regulation applicable to **Prescribed Entities**.

4.1.2 ICES is designated a **Prescribed Entity** under s.2 of O. Reg. 523/18 to the *Coroners Act,* for the purposes of s.52.1 of the *Coroners Act* and, as such, ICES has legal authority to collect and use **PI** as defined under the *Coroners Act* for the purpose of analysis or compiling statistical information related to the health or safety of the public, or any segment of the public. ICES is committed to complying with the provisions of the *Coroners Act* and its regulation applicable to **Prescribed Entities**.

4.1.3 ICES is a not-for-profit corporation incorporated in 1992 under the laws of Ontario and has legal authority to collect and use **PHI/PI** pursuant to its **Corporate Objects**, but only if ICES' **Corporate Objects** align with the intended purposes for the collection and use of **PHI/PI** set out in **PHIPA**, the *Coroners Act*, and their applicable regulations.

4.1.4 ICES respects the principle of **Indigenous Data Sovereignty** and aims to incorporate the principle in ICES' approach to data governance, including the collection, use, and disclosure of **Indigenous Data**. The First Nations principles of ownership, control, access, and possession (**OCAP**) also form part of ICES' approach to data handling practices.

4.1.5 ICES enters into **DSAs** with respect to the collection, use, and disclosure of **PHI/PI** and such **DSAs** outline the terms and conditions for ICES lawfully collecting, using, and/or disclosing the **PHI/PI** governed by the **DSAs**.

4.1.6 To rely on a **Research** legal authority for the collection, use, and disclosure of **PHI/PI,** ICES must be specifically named in a written research plan approved by a **Research Ethics Board ("REB")**, and such research plan must clearly articulate ICES' role in the planned **Research**.

4.1.7 In instances where ICES is not a designated **Prescribed Entity** in legislation or regulation relied on by the **Data Provider** for lawful disclosure of **PHI/PI** to ICES then ICES must ensure that it has lawful authority to collect and use the **PHI/PI** being disclosed.

4.1.8 From time to time, ICES may collect **Non-PHI/PI**. Such **Non-PHI/PI** also may be subject to the requirements and obligations set out in this **Policy**.

4.2 Compliance

4.2.1 ICES implements privacy and security **Policies**, **Procedures,** and **Practices** required to protect the privacy of individuals whose **PHI**/PI it receives and to maintain the confidentiality of that **PHI/PI**.

4.2.2 ICES is committed to complying with the provisions of *PHIPA*, the *Coroners Act,* and their regulations applicable to **Prescribed Entities**.

4.2.3 ICES' **Policies**, **Procedures,** and **Practices** are prepared in accordance with the **Information and Privacy Commissioner of Ontario ("IPC")** *Manual for The Review and Approval of Prescribed Persons And Prescribed Entities* and the **IPC's** *Coroners Act Addendum,* and ICES is subject to review by the **IPC** every three years.

4.2.4 ICES is responsible for the **PHI/PI** collected, used, and disclosed by **ICES Agents**.

4.2.5 ICES is responsible for **ICES Agents'** compliance with ICES' **Policies**, **Procedures,** and **Practices**.

4.2.6 ICES ensures compliance by **ICES Agents** with **PHIPA** and the *Coroners Act* through ICES' **Policies, Procedures, Practices,** privacy awareness, training, and agreements.

4.3 The information ICES collects and uses

4.3.1 Most ICES' scientific programs and services involve the collection and use of **PHI/PI** that is subject to privacy law, including **PI** received from the Chief Coroner and from service providers under the *Coroners Act*.

4.3.2 ICES collects and uses **PHI/PI** such that **ICES Agents** may conduct:

a. Health system analysis and evaluation for ICES Purposes (called **Statistical Analysis** or **Analytics** interchangeably); and/or

b. Health-related **Research**.

4.3.3 ICES may only collect and use **PHI/PI** that is permitted by law and aligns with its **Corporate Objects**.

4.3.4 The types of **PHI/PI** collected by ICES includes:

a. **PHI** originally collected by **Health Information Custodians ("HIC") and Prescribed Entities** or **Prescribed Registries**;

b. **PHI** and other personal information as defined under the relevant legislative regime collected by **Third Party Researchers ("TPRs")**;

c. Identifying information about individuals that was originally collected by other organizations in the public and private sectors;

d. **PI** collected from the Chief Coroner under the *Coroners Act*; and

e. Other information ICES collects to manage its relationships with employees, affiliated individuals, and others who interact with ICES.

4.3.5 ICES recognizes that **PHI/PI** is inherently sensitive and ICES is responsible for ensuring that **PHI/PI** is protected in accordance with ICES' **Policies** and **Procedures** as a **Prescribed Entity**, **PHIPA,** the *Coroners Act*, and their applicable regulations, other applicable law, contractual obligations, and **REB** approvals. ICES has therefore adopted the following key principles, which guide its handling of **PHI/PI**:

a. ICES must only collect and use **PHI/PI** permitted by **PHIPA** and/or the *Coroners Act*, and their applicable regulations, and only in accordance with applicable law and, when necessary, **REB** approvals;

b. ICES must not collect and use **PHI/PI** if other less identifiable information will serve the purpose;

c. ICES must not collect and use more **PHI/PI** than is reasonably necessary for the purposes identified;

d. ICES must implement **Policies**, **Procedures** and **Practices** to ensure that both the amount and the type of **PHI/PI** collected and used is limited to that which is reasonably necessary for its purposes;

e. ICES must ensure that upon collection of **PHI/PI**, ICES assigns a confidential **ICES Identifier** to individual-level **PHI/PI** and removes the **Direct Personal Identifiers ("DPI")** before making available for use by **ICES Agents**;

f. ICES must implement a list of the data holdings of **PHI/PI**; and

g. ICES' **Data Dictionary** sets out the purposes, data elements, and data sources for each data holding of **PHI/PI**.

4.3.6 ICES must distinguish in each **PIA** if the purpose for the use of the **PHI/PI** is for **Statistical Analysis** or for **Research**.

4.3.7 All requests to conduct **Statistical Analysis** or **Research** require a **PIA** by ICES to ascertain legal authority and compliance with ICES **Policies**, **Procedures**, and **Practices**, **Corporate Objects**, **DSAs**, and **REB** approvals.

a. **PIAs** must set out **Risks** and recommendations, if applicable, associated with the requests outlined in the **PIAs**;

b. **PIAs** must be conducted by an appropriate ICES Privacy **SME**;

c. **PIAs** must clearly distinguish between the use of **PHI/PI** and the use of **De-Identified Data,** either in the form of **Aggregate Data (Summary Output)** or of **Publishable Data**;

d. **PIAs** must ensure that each use of **PHI/PI** is consistent with the uses of **PHI/PI** permitted by **PHIPA** and its regulation (for **PHI**) or the *Coroners Act* and its regulation (for **PI**), and/or any other statute, as applicable; and

e. All **PIAs** must articulate a commitment that the use of **PHI/PI** by **ICES Agents** is only for ICES' purposes.

4.3.8 ICES remains responsible for the **PHI/PI** used by any **ICES Agents** as set out in ICES' **ICES Agent and Confidentiality Agreement ("ICES Agent CA")**.

4.3.9 **ICES Agents** must only collect, use, disclose, retain, and destroy PHI/PI in compliance with **PHIPA** (for **PHI**) and the *Coroners Act* (for **PI**), and their applicable regulations, and in compliance with the privacy and security **Policies**, **Procedures**, and **Practices** implemented by ICES and as set out in **ICES Agent CA** and the *ICES Agent Policy*.

4.4 The information ICES discloses

4.4.1 ICES must not disclose **PHI**, subject to the following exceptions:

a. Disclosure of **PHI** to **Prescribed Entities** and **Prescribed Registries** for their prescribed purposes, as permitted by s.18(4) of O. Reg 329/04 to **PHIPA,** with respect to s.39 (1)(c) and s.45 of **PHIPA,** and verified through a **PIA**;

b. Disclosure of **PHI** to **TPRs** in the form of **Risk Reduced Coded Data ("RRCD")** on ICES-controlled systems, for the purposes of publicly or privately funded research, as permitted by s.18(4) of O. Reg 329/04 to **PHIPA**, with respect to s.44 of **PHIPA,** and verified through a **PIA**; and

c. Disclosure of **PHI** to **TPRs** in the form of a **Cohort List**, for the purposes of publicly funded research that cannot be reasonably conducted within ICES, as permitted by s.44 of ***PHIPA*** and verified through a **PIA**.

4.4.2 ICES must not disclose **PHI/PI** if other information, such as **De-Identified Data,** will serve the purpose.

4.4.3 ICES must not disclose more **PHI/PI** than is reasonably necessary to meet the purpose.

4.4.4 **TPRs** are only permitted to access **RRCD** on ICES-controlled systems.

4.4.5 Only **De-identified Data** is released to **TPRs** or **Knowledge Users**.

4.4.6 ICES prohibits the disclosure of **PHI/PI** to any **Knowledge User**.

4.4.7 Prior to release of **De-Identified Data**, ICES must review to ensure that it is not reasonably foreseeable in the circumstances that any **De-identified Data** could be used, either alone or with other information, to identify an individual.

4.5 **PHI/PI** transfer

4.5.1 ICES must takes steps to transfer **PHI/PI** securely as set out in ICES' *Secure Transfer of PHI/PI Procedure*.

4.5.2 ICES must ensure that an encrypted file transfer system is enabled to protect both inbound and outbound electronic files.

4.5.3 ICES prohibits the transfer of paper records that include **PHI/P**.

4.6 Secure retention and destruction of records of **PHI/PI**

4.6.1 **PHI/PI** with **DPI** (called **Fully Identifiable Data**)is retained for as long as specified in the associated **DSA** with the **Data Provider** and as otherwise specified in ICES' *Record Retention Standard*.

4.6.2 **Fully Identifiable Data** must be isolated in secure network folders and cabinets until data quality issues, if any, are resolved, and after which the **PHI/PI with DPI** must be securely destroyed in accordance with ICES' *Destruction of ICES Data Procedure.*

4.7 Implementation of administrative, technical, and physical safeguards

4.7.1 ICES must implement a range of administrative, technical, and physical safeguards to protect **PHI/PII**.

4.7.2 ICES assesses the range of administrative, technical, and physical safeguards in **PIAs** and **Threat Risk Assessments** ("**TRAs**").

4.7.3 The administrative, technical, and physical safeguards implemented by ICES are set out in ICES' privacy and security **Policies**, **Procedures**, and **Practices**.

4.8 Transparency, Privacy Inquiries, and Privacy Complaints

4.8.1 ICES strives for transparency and enables individuals to make **Privacy Inquiries** and **Privacy Complaints** about ICES' privacy **Policies**, **Procedures,** and Practices.

4.8.2 The ICES **CPLO** is responsible for ensuring the following privacy information is published on ICES' website:

a. The list of ICES' **Data Holdings**;

b. Information about ICES' **Privacy Policies, Procedures,** and **Practices**; and

c. Information about how individuals can make **Privacy Inquiries** and **Privacy Complaints**.

4.8.3 Individuals can make **Privacy Inquiries** and **Privacy Complaints** directly to the ICES **CPLO**, either verbally or in writing using the contact details below, regarding ICES' privacy **Policies**, **Procedures,** and **Practices**, and/or ICES' compliance with **PHIPA** and the ***Coroners Act***:

a. Institute for Clinical Evaluative Sciences
Attn: Chief Legal and Privacy Officer
G-106 - 2075 Bayview Avenue
Toronto, Ontario M4N 3M5
Telephone: 416-480-4055
Fax: 416-480-6048
Email: privacy@ices.on.ca

b. Individuals may also direct **Privacy Complaints** about ICES' **PHI/PI** practices under **PHIPA** and the *Coroners Act*, to the **IPC** using the contact details below:
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

5.0 RELATED DOCUMENTATION

5.1 *Ongoing Review of Privacy and Security Policies, Procedures, Practices, and Exceptions Policy*

5.2 *Change Management Policy*

5.3 *Discipline and Corrective Action in Relation to ICES Data Policy*

5.4 *Termination or Cessation of Employment or Contractual Relationship in Relation to ICES Data Policy*

5.5 *Destruction of ICES Data Proceure*

5.6 *Record Retention Standard*

5.7 *Secure Transfer of PHI/PI Procedure*

5.8 *ICES Agent Policy*

5.9 *Privacy and Security Governance and Accountability Policy*

6.0 TRAINING AND COMMUNICATION

6.1 **Policies** and **Procedures** are available on the **ICES Intranet**.

6.2 This **Policy** and any administrative **Procedures** are communicated to all **ICES Agents** across the **ICES Network** during onboarding and on a yearly basis. **Policy** awareness is also supported and promoted by the **Policy Owner**.

6.3 Once new **Policies** are published to the **ICES Intranet**, they are communicated to **ICES Employees** in ICES OnTap, the weekly email with the organization's internal updates.

7.0 COMPLIANCE AND ENFORCEMENT

7.1 **ICES Agents** must comply with all applicable ICES **Policies** and **Procedures**.

7.2 **ICES Agents** must notify an ICES Privacy **Subject Matter Expert ("SME")** or ICES Security **SME** at the first reasonable opportunity if they breach or believe there has been a breach of ICES' privacy and security **Policies** or **Procedures**, in accordance with ICES' *Privacy and Security Incident Breach Management Policy* and associated **Procedures**, as set out in the framework posted on the ICES **PLO**/Cybersecurity site on the **ICES Intranet**.

7.3 All other violations under ICES privacy and security **Policies** and **Procedures** 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 for cause, or contract with ICES pursuant to *ICES' Discipline and Corrective Action in Relation to ICES Data Policy* and ICES' *Termination or Cessation of Employment or Contractual Relationship in Relation to ICES Data Policy* and associated **Procedures**.

7.4 Compliance is subject to annual audit by an ICES Privacy **SME** or ICES Risk & Compliance Analyst pursuant to the **Annual Audit Schedule** established under ICES' *Privacy and Security Audit Policy*.

8.0 EXCEPTIONS

8.1 Any exceptions requested pursuant to this **Policy** must be in accordance with ICES' *Ongoing Review of Privacy and Security Policies, Procedures, Practices, and Exceptions Policy* and ICES' *Change Management Policy*.