Transparency of Privacy and Security Policies, Procedures, and Practices Policy

Department	Document Number	Organizational Scope	ICES Site	IPC Scope
PLO	PO.006	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)**
September 2022	N/A	Triennially	September 2025	N/A

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

Required Reviewers (Titles)		
Director, Cybersecurity		

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

1.0 PURPOSE

1.1 The purpose of this **Policy** is to:

1.1.1 Identify the information made available to the public and other stakeholders relating to ICES' privacy **Policies**, **Procedures,** and **Practices**.

1.1.2 Identify the means by which such information is made available.

2.0 SCOPE

2.1 This policy applies to all privacy **Policies**, **Procedures,** and **Practices** implemented by ICES.

3.0 ROLES AND RESPONSIBILITIES

4.0 DETAILS

4.1 ICES **Chief Privacy and Legal Officer ("CPLO")** is responsible for ensuring **ICES Privacy Information** is created and made available on ICES' public website and by other means.

4.2 At a minimum, **ICES Privacy Information** shall include the following:

4.2.1 ICES' *Privacy Policy*.

4.3 Frequently asked questions related to:

a. Description of ICES' status as a **Prescribed Entity** under Ontario's *Personal Health Information Protection Act* **("PHIPA")** and under Ontario's *Coroners Act*;

b. the duties and responsibilities arising from these statuses;

c. the **Policies**, **Procedures**, and **Practices** implemented with respect to **Personal Health Information ("PHI")** and **Personal Information ("PI")**, including:

   i. For **PHI**:

      A. The types of **PHI** collected and the persons or organizations from which this **PHI** is typically collected;

      B. The purposes for which **PHI** is collected;

      C. The purposes for which **PHI** is used and if **PHI** is not used then the nature of the information that is used; and

      D. The circumstances in which and purposes for which ICES discloses **PHI,** and the persons or organizations to whom **PHI** is typically disclosed,

   ii. For **PI**:

      A. The types of **PI** collected from the Chief Coroner;

      B. The specific purposes for which **PI** is collected;

      C. The specific purposes for which **PI** is used and if **PI** is not used then the nature of the information that used;

      D. The **Record Linkages** of the **PI**, including:

         (1) The specific purposes for which **PI** is linked;

         (2) The **PI** used for linking; and

         (3) The processes used to link the **PI**, and

      E. The circumstances in which and the specific purposes for which the **PI** is disclosed and the persons or organizations to whom **PI** is typically disclosed.

d. A summary overview of key administrative, technical, and physical safeguards used to protect the privacy of **PHI/PI**, including the steps taken to protect **PHI/PI** against theft, loss, and unauthorized use or disclosure and to protect records of **PHI/PI** against unauthorized copying, modification, or disposal; and

e. The name and/or title, mailing address, and contact information of the **ICES Agent** to whom inquiries, concerns or complaints regarding compliance with the privacy **Policies**, **Procedures,** and **Practices** implemented and regarding compliance with **PHIPA** and the *Coroners Act* may be directed.

4.3.2 Documentation related to ICES' most recent review under s.45(3) of ***PHIPA*** and most recent review under s.52.1(3) of the *Coroners Act* by the **Information and Privacy Commissioner of Ontario ("IPC")**.

4.3.3 Documentary evidence of the **IPC's** designation of ICES as a **Prescribed Entity** under **PHIPA** and under the *Coroners Act*.

4.3.4 A list of **ICES Data Holdings** of **PHI/PI** maintained by ICES.

4.3.5 Instructions, including the title, mailing address and contact information, for making inquiries and complaints about ICES' privacy **Policies, Procedures and Practices**, and compliance with **PHIPA**, the *Coroners Act*, and their applicable regulations.

4.3.6 **Privacy Impact Assessments ("PIAs")** or a summary of **PIAs**.

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 *Privacy and Security Audit Policy*

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

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

5.6 *Privacy and Security Incident Breach Management Policy*

5.7 *Privacy 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*.