Privacy and Security Governance and Accountability Policy

Department	Document Number	Organizational Scope	ICES Site	IPC Scope
PLO	PO.001	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)**
March 2022	September 2022	Triennially	September 2025	300CO-CO-001; 1100SE-CO-07

Authority (Title)	Policy Owner (Title)
CEO	Chief Privacy and Legal Officer

Required Reviewers (Titles)		
Director, Cybersecurity	Director, PLO	

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

1.0 PURPOSE

1.1 ICES is a prescribed entity pursuant to the *Personal Health Information Protection Act, 2004* ("**PHIPA**") and its regulation O. Reg 329/04. **PHIPA** is a consent-based statute in that a **Health Information Custodian" ("HIC")** may collect, use, and disclose **Personal Health Information ("PHI")** only with the consent of the individual to whom the **PHI** relates, subject to limited exceptions where **PHIPA** permits or requires the collection, use, or disclosure to be made without consent.

1.2 One such disclosure that is permitted without consent is the disclosure of **PHI** by **HICs** to **Prescribed Entities ("PEs")** for the purpose of analysis or compiling statistical information with respect to the management of, evaluation or monitoring of, the allocation of resources to or planning for all or part of the health system. These disclosures are permitted without consent provided that ICES has in place **Practices** and **Procedures** approved and reviewed by the **Information and Privacy Commissioner of Ontario ("IPC")** every three years from the date of their initial approval. The review and approval of ICES' **Practices** and **Procedures** is supported through the application of the *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities* ("**IPC Manual**").

1.3 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 **Personal Information ("PI")** from the Chief Coroner of Ontario for the purpose of research, data analysis or the compilation of statistical information related to the health or safety of the public, or any segment of the public. ICES must have in place **Policies** and **Procedures** approved by the **IPC** every three years, and this review is supported through the application of the *Coroners Act Addendum to the Manual for the Review and Approval of Persons and Prescribed Entities* **("IPC Addendum")**

1.4 As set out in the **IPC Manual** and **IPC Addendum**, to protect the privacy of individuals whose **PHI/PI** is received by ICES and to maintain the confidentiality of that information, ICES must have *a Privacy and Security Governance and Accountability Policy* for ensuring compliance with **PHIPA,**

the *Coroners Act*, and their regulations, and for demonstrating compliance with the privacy and security **Policies**, **Procedures,** and **Practices** implemented and operationalized.

1.5 This **Policy** sets out ICES' *Privacy and Security Governance and Accountability Policy* in relation to **PHIPA,** the *Coroners Act*, and their regulations, but also with respect to any other instance in which ICES leverages legal authority under any other statute and/or regulation of Ontario or Canada or its status as a legal not-for-profit corporation duly incorporated in the province of Ontario.

2.0 SCOPE

2.1 This policy applies to ICES and **ICES Agents**.

3.0 ROLES AND RESPONSIBILITIES

4.0 DETAILS

4.1 Governance

4.1.1 **Chief Executive Officer ("CEO")** Accountability

a. ICES' **CEO** is ultimately accountable for ensuring that ICES **and ICES Agents** comply with **PHIPA**, the *Coroners Act*, their regulations, and with all Privacy and security **Policies**, **Procedures**, and **Practices** implemented; and

b. ICES' **CEO** is ultimately accountable for ensuring the security of any **PHI/PI** collected, used, disclosed, transferred, retained and destroyed by ICES and for ensuring that ICES has the resources and technology to implement and execute the security program successfully.

4.1.2 **Chief Privacy and Legal Officer ("CPLO")** Delegated Accountability

a. Authority is delegated by ICES' **CEO** to ICES' **CPLO** for executive oversight of the Privacy and security (hereinafter referred to as the "Cybersecurity" program). The ICES **CPLO** reports directly to the **CEO**;

b. ICES' **CPLO** is accountable for the successful execution and implementation of ICES' Privacy and Cybersecurity program in compliance with all regulatory and external requirements; and

c. The ICES **CPLO** meets monthly with the ICES **CEO** and provides a written report in respect of the ICES **CPLO's** accountabilities for each of the ICES' **Privacy and Legal Office ("PLO")** and ICES' Cybersecurity department.

4.1.3 ICES Board of Directors

a. ICES' **CPLO** must provide quarterly written reports to ICES' **Finance, Audit & Risk Committee** ("**FAR**") Committee of ICES' Board of Directors, with regards to the two departments which form part of the ICES **CPLO's** accountabilities:

   i. ICES' **PLO** functions in each of: Privacy, Legal, Risk, Audit, Compliance; and

   ii. Cybersecurity.

b. ICES' **CPLO** attends each meeting of the ICES **FAR** and is available to answer questions posed by ICES **FAR** committee members. Should the ICES **CPLO** not be available to attend an ICES **FAR** meeting, the ICES Director, **PLO** and/or ICES Director, Cybersecurity will attend as delegates; and

c. The Chair of the ICES **FAR** committee must present the minutes corresponding to the ICES **PLO**/Cybersecurity written report to ICES' Board of Directors for formal adoption and approval at each quarterly ICES Board of Directors meeting.

4.1.4 ICES' **CPLO** must set out the following in the ICES **PLO**/Cybersecurity written reports to the **FAR**:

a. ICES **PLO**

   i. Address the initiatives undertaken by the Privacy program, including Privacy training and the development and implementation of Privacy policies, procedures and practices;

   ii. Include a discussion of the **Privacy Audits** and **Privacy Impact Assessments** ("**PIAs**") conducted, including the results of and any recommendations arising from these investigations and the status of implementation of the recommendations;

   iii. Include information about **Privacy Incidents**, **Breaches** and **Complaints** that were investigated, including the results of and any recommendations arising from these investigations and the status of implementation of the recommendations;

   iv. Include information about legal matters;

   v. Include information about compliance issues, including but not limited to: contractual compliance, regulatory compliance, and the Privacy and Security Audit Program; and

   vi. Include information about enterprise-level **Risks** with a corresponding dashboard that also sets out metrics on department **Risks** across the **ICES Network**.

b. Cybersecurity

   i. Address the initiatives undertaken by the Cybersecurity department including security training and the development and implementation of security **Policies**, **Procedures**, and **Practices**;

   ii. Include a discussion of the security audits conducted, including the results and recommendations arising from the security audits and the status of implementation of the recommendations; and

iii. Include information about **Security Breaches** investigated, including the results of and any recommendations arising from these investigations and the status of the implementation of the recommendations.

4.2 Roles

4.2.1 Privacy, Risk, and Compliance

a. ICES Director, **PLO**

i. The ICES **CPLO** has delegated day-to-day responsibility to the ICES Director, **PLO** for the oversight of the Privacy, Risk, and Compliance programs for ICES;

ii. The ICES **CPLO** maintains a current job profile that includes all responsibilities and obligations for the ICES Director, **PLO**;

iii. The ICES **CPLO** meets and reviews the duties and responsibilities of the ICES Director, **PLO** at least monthly and ensures that any corresponding documentation is kept up-to-date;

iv. The ICES Director, **PLO** provides monthly reports to the ICES **CPLO** on all privacy, risk, and compliance activities;

v. The ICES Director, **PLO** has responsibility for the oversight of all ICES Privacy Analysts and ICES Risk and Compliance Analysts at each of the **ICES Sites**. Such individuals are not **ICES Employees**, but rather, **Site Employees** of the **Host Institution** with whom ICES has a contractual relationship in respect of an **ICES Site**; and

vi. The ICES **Director**, reviews the duties and responsibilities of these analysts at least monthly, provides opportunities for regular meetings, and ensures that any corresponding documentation is kept-up-to-date.

b. ICES Manager, Privacy

i. The ICES Director, **PLO** has provided the ICES Manager, Privacy with authority to manage all aspects of the Privacy program for ICES;

ii. The ICES Director, **PLO** maintains a current job profile that includes all responsibilities for the ICES Manager, Privacy;

iii. The ICES Director, **PLO** meets and reviews the duties and responsibilities of the ICES Manager, Privacy at least monthly and ensures that any corresponding documentation is kept up-to-date;

iv. The ICES Manager, Privacy provides monthly reports to the ICES Director, **PLO** on all relevant aspects of ICES' Privacy program; and

v. The ICES Manager, Privacy has responsibility to ensure that the ICES Research Program and Project **PIA** Coordinators who review **PIAs for ICES Projects** utilizing **General Use Data ("GUD")** or **Controlled Use Data ("CUD")** do so in compliance with **PHIPA,** the *Coroners Act*, and their regulations. ICES Research Program and

Project **PIA** Coordinators have a dotted line reporting relationship into the ICES Manager, Privacy for any work related to these **PIAs**.

4.2.2 Cybersecurity

a. ICES Director, Cybersecurity

i. The ICES **CPLO** has delegated day-to-day responsibility to the ICES Director, Cybersecurity for the oversight of the security program for ICES, including but not limited to: strategy development, external stakeholder engagement, and leading large-scale Cybersecurity initiatives and projects;

ii. The ICES **CPLO** maintains a current job profile that includes all responsibilities and obligations for the ICES Director, Cybersecurity;

iii. The ICES **CPLO** meets and reviews the duties and responsibilities of the ICES Director, Cybersecurity and at least monthly and ensures that any corresponding documentation is kept up-to-date; and

iv. The ICES Director, Cybersecurity provides monthly reports to the ICES **CPLO** on all cybersecurity activities.

b. ICES Manager, Cybersecurity

i. The ICES Director, Cybersecurity has provided the ICES Manager, Cybersecurity with authority for executing the Cybersecurity department's strategy for ICES, including but not limited to internal stakeholder engagement (departments, teams), leading new processes, **Policies**, tools, forms, logs, identifying and establishing new processes, coordinating tactical and operational changes and remediation activities with ICES' Information Technology operations and oversight and coordination of complex **Threat Risk Assessments**;

ii. The ICES Director, Cybersecurity maintains a current job profile that includes all responsibilities for the ICES Manager, Cybersecurity;

iii. The ICES Director, Cybersecurity meets and reviews the duties and responsibilities of the ICES Manager, Cybersecurity at least monthly and ensures that any corresponding documentation is kept up-to-date; and

iv. The ICES Manager, Cybersecurity provides monthly reports to the ICES Director, Cybersecurity on all relevant aspects of ICES' Cybersecurity security program.

4.3 Privacy and Security Committees

4.3.1 All committees with Privacy and Cybersecurity involvement are set out in ICES' *Governance and Operations Charter*.

4.4 Governance and Organizational Chart

4.4.1 An organizational chart setting out Privacy and Cybersecurity roles is set out and posted on **ICES' Intranet**.

4.5 Privacy and Security Framework communication to **ICES Network**

4.5.1 This **Policy** is posted on **ICES' Intranet** and available to all **ICES Agents**.

4.5.2 The ICES **CPLO** maintains a site on **ICES' Intranet** to update all **ICES Agents** on ICES **PLO-**related and Cybersecurity-related matters, and a more detailed organizational chart is included therein.

4.5.3 Any updates to the ICES' *Privacy and Security Governance and Accountability Policy* is communicated at committee meetings, newsletters and via email as needed.

5.0 RELATED DOCUMENTATION

5.1 *Privacy and Security Governance and Accountability Policy*

5.2 *Governance and Operations Charter*

5.3 *Incident Breach Management Policy*

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

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

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

5.7 *Change Management 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 PLO/Cybersecurity Intranet site.

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**.

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*