Statements of Purpose for Data Holdings Containing PHI/PI Policy

Department	Document Number	Organizational Scope	ICES Site	IPC Scope
PLO	PO.013	ICES Network Policy	ICES Network	All Acts
Original Date (Month yyyy)	**Last Review Date** (Month yyyy)	**Frequency of review**	**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)		
N/A		

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

1.0 PURPOSE

1.1 The purpose of this **Policy** is to set out that **Statements of Purpose** ("**SOP**") for **ICES Data Holdings** containing **Personal Health Information** ("**PHI**") and **Personal Information** ("**PI**") must be:

1.1.1 developed and implemented each time ICES collects **PHI/PI** as authorized in a **Privacy Impact Assessment** ("**PIA**");

1.1.2 reviewed and maintained regularly to ensure accuracy;

1.1.3 amended in accordance with any **Data Sharing Agreement** ("**DSA**")**;** and

1.1.4 approved by the ICES Manager, Privacy.

2.0 SCOPE

2.1 This policy applies to all **ICES Agents** involved in the development, implementation, review, and maintenance of **SOPs.**

3.0 ROLES AND RESPONSIBILITIES

4.0 DETAILS

4.1 Colllection

4.1.1 All **SOPs** must include:

a. The purpose of the **ICES Data Holding**,

b. The **PHI/PI** contained in the **ICES Data Holding**;

c. The source(s) of the **PHI/PI**; and

d. The need for the **PHI/PI** in relation to the identified purpose.

4.1.2 ICES Privacy **Subject Matter Experts** ("**SMEs**") are expected to complete the **SOPs** following the conclusion of a **PIA** for each **ICES Data Holding** containing **PHI/PI**.

4.1.3 ICES Privacy **SMEs** are expected to consult with the ICES Director, Strategic Partnerships or their delegate to confirm the **SOP** before finalizing the **PIA**.

4.1.4 From time to time, other ICES departments may need to be consulted in the development of a **SOP**. All ICES Privacy **SMEs** are expected to engage those individuals who can contribute to an accurate **SOP**.

4.1.5 All ICES Privacy **SMEs** have delegated authority to approve the **SOP** in the **PIA,** as directed by the ICES Manager, Privacy.

4.1.6 The ICES Manager, Privacy has been delegated day-to-day authority to manage the privacy program with respect to **SOPs** and can, at their discretion, review any **SOP** completed by the ICES Privacy **SME**.

4.1.7 All **SOPs** must be included in **DSAs** which are executed between ICES and the **Data Provider** disclosing the **PHI/PI** to ICES.

4.1.8 Following the execution of a **DSA**, all SOPs must be posted on the ICES **Data Holdings Obligations** ("**DHO**") page by the ICES Risk and Compliance Analyst such that access is enabled to all **ICES Agents**.

4.2 Review and Maintenance

4.2.1 The ICES Director, **Privacy and Legal Office** ("**PLO**") must review **SOPs** on an ongoing basis to ensure:

a. Their continued accuracy; and

b. That the **PHI/PI** collected for the purposes of the **ICES Data Holding** is still necessary for the identified purpose.

4.2.2 The ICES Director, **PLO** must set out a schedule at the beginning of each fiscal year which outlines the plan for reviewing **SOPs**.

4.2.3 Such plan for reviewing **SOPs** must be approved by the ICES **Chief Privacy and Legal Officer** ("**CPLO**") and included in any operational work for the ICES **PLO**.

4.2.4 Any changes to the **SOPs** must be discussed at the ICES Science Office, Privacy, Research & Development ("**SOPRAD**") meeting, which includes individuals from the Science Office, Compliance, Privacy, Strategic Partnerships, and Research and Analysis at ICES.

4.2.5 Any changes to the **SOPs** must be ultimately approved at the ICES **Change Advisory Board** ("**CAB**").

4.3 Amendment

4.3.1 An **SOP** must be amended prior to undertaking activity that is inconsistent with the **SOP** as approved.

4.3.2 Any amendments to **SOPs** must be mutually agreed to by ICES and the applicable **Data Provider** and reflected in an amendment to the **DSA** and, if applicable, **REB** approval.

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*

6.0 TRAINING AND COMMUNICATION

6.1 Policies 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*.

Statements of Purpose for Data Holdings Containing PHI/PI Policy