Privacy Impact Assessment Policy

Department	Document Number	Organizational Scope	ICES Site	IPC Scope
PLO	PO.011	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)**
June 2014	September 2022	Triennially	September 2025	800PR-PR-002

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** identifies the circumstances in which **Privacy Impact Assessments** ("**PIA**") must be conducted by ICES.

2.0 SCOPE

2.1 This **Policy** applies to every **ICES Agent**.

3.0 ROLES AND RESPONSIBILITIES

3.1 ICES **Chief Privacy and Legal Officer** ("**CPLO**").

3.1.1 Accountable for the design of **PIAs** and ensuring that **ICES Agents** comply with this **Policy** and its **Procedures**.

3.2 ICES Director, **Privacy and Legal Office** ("**PLO**")

3.2.1 Delegated by the ICES **CPLO** to have day-to-day responsibility for the oversight of the privacy program;

3.2.2 Responsible for overseeing the **Procedures** in support of conducting **PIAs** and the logging of **PIAs**, ensuring that conditions, restrictions, recommendations, and **Risks** identified in **PIAs** are documented and logged appropriately in in accordance with ICES' *Maintaining a Consolidated Log of Recommendations Policy* and in appropriate **Department Risk Registers** ("**DRR**") or **Enterprise Risk Register** ("**ERR**") as set out in ICES' *Risk Management Policy.*

3.3 ICES Manager, Privacy

3.3.1 Responsible for ensuring that all **PIAs** are conducted in accordance with ICES' lawful authority to collect, use, and disclose **Personal Health Information** ("**PHI**") and **Personal Information** ("**PI**").

3.4 ICES Privacy **Subject Matter Experts** ("**SME**")

3.4.1 ICES **CPLO** has delegated day-to-day responsibility for the conduct and execution of **PIAs** to the ICES Privacy **SMEs** in the ICES **PLO** or ICES Research & Analysis department, as applicable, and this is communicated on ICES' **PLO** page of the **ICES Intranet**.

4.0 DETAILS

4.1 General Principles

4.1.1 A **PIA** is a risk management tool that enables ICES to adhere to applicable laws and other legal requirements and to identify the impacts of all collections, uses, and disclosures of **PHI/PI** on individuals' privacy.

4.1.2 A **PIA** must be completed for all new or amended collections, uses, or disclosures of **PHI/PI** by **ICES Agents** on behalf of ICES.

4.1.3 A **PIA** must be completed for any new or amended business processes, information systems, **Technology Resources**, or programs involving **PHI/PI.**

4.1.4 ICES conducts **PIAs** to verify that:

a. Any collection, use, or disclosure of **PHI/PI** by **ICES Agents** is in accordance with the *Personal Health Information Protection Act* ("**PHIPA**"), the *Coroners Act*, their applicable regulations, as well as other applicable laws;

b. The purpose for the collection, use, or disclosure of **PHI/PI** aligns with ICES' **Corporate Objects**;

c. Other information, including **De-identified Data**, will not serve the identified purpose; and

d. No more **PHI/PI** will be collected, used, or disclosed than is reasonably necessary for the identified purpose.

4.1.5 If ICES must collect, use, or disclose **De-Identified Data** and/or **Non-PHI/PI**, the ICES Manager, Privacy will determine whether a **PIA** or another vehicle must be utilized and any associated documentation thereof.

4.1.6 The circumstances in which **PIAs** are required to be conducted include:

a. A proposed new collection of **PHI/PI**;

b. The creation of any new **ICES Data Holding**;

c. Any new use of **PHI/PI,** whether for an **ICES Project** or as part of another activity or tool;

d. Introducing or substantially changing a business process, information system, **Technology Resource,** or program that involves **PHI/PI**;

e. Disclosing **PHI/PI** to another organization or a **Third Party Researcher**; or

f. Establishing or changing a **Third Party Service Provider** ("**TPSP**") relationship that involves **PHI/PI**.

4.1.7 No change that requires a **PIA** may be implemented until all **Risks** identified have been eliminated, accepted, or have a satisfactory mitigation plan in place by the applicable **Risk Owner**, as set out in ICES' *Risk Management Policy*.

4.1.8 A **Data Sharing Agreement** ("**DSA**") cannot be executed until a **PIA** has been completed by an ICES Privacy **SME**.

4.2 **PIA** requests

4.2.1 **ICES Agents** are responsible for requesting that **PIA** be conducted:

a. At the conceptual design stage of planned activity (with respect to proposed new **ICES Data Holdings** involving **PHI/PI** and new or changes to existing business processes, information systems, **Technology Resources,** or programs involving **PHI/PI**) and that they be reviewed and revised, if necessary, during the detailed design and implementation stages;

b. Before any new collection of **PHI/PI**;

c. Before any new use of **PHI/PI** from existing **ICES Data Holdings**;

d. Before any disclosure of **PHI/PI** to another person/organization or to a **Third Party Researcher**; or

e. Before any new use of **PHI/PI** by a **TPSP**.

4.2.2 **ICES Agents** must contact ICES' **PLO** to request a **PIA** before proceeding with any changes to ICES' **PHI/PI**.

4.2.3 ICES **CPLO** may also direct that a **PIA** be conducted if a **PIA** does not exist, but is required.

4.3 Content of **PIA**

4.3.1 ICES permits two **PIA** templates: one for reviewing lawful authorities in support of **ICES Projects** ("**Project PIA**") and another template for all other **PIAs** conducted.

4.3.2 At a minimum, both **PIAs** must describe, the:

a. **ICES Data Holding**, business process information system, **Technology Resource**, or program at issue;

b. Nature and type of **PHI/PI** collected, used, or disclosed, or that is proposed to be collected, used, or disclosed and its sources;

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

d. Purpose and rationale (reason) for the collection, use, or disclosure of **PHI/PI**;

e. Flow of **PHI/PI**;

f. Legal authority for each collection, use, and disclosure of **PHI/PI**;

g. Limitations (if any) imposed on collection, use, and disclosure;

h. **Record Linkages** (if any), including whether or not **PHI/PI** will be linked to other information;

i. Applicable retention periods for the **PHI/PI**;

j. Secure manner in which the **PHI/PI** will be retained, transferred, and disposed of;

k. Administrative, technical, and physical safeguards implemented or proposed to protect **PHI/PI**, including functionality for logging access, use, modification, and disclosure of **PHI/PI** and functionality for auditing to detect unauthorized use or disclosure;

l. **Risks** and mitigation strategies; and

m. Recommendations arising from **PIAs** and associated responsibilities of **ICES Agents**, including compliance oversight and timelines.

4.4 Review and analysis of **PIAs**

4.4.1 A **PIA** must capture whether the collection, use, or disclosure of **PHI/PI** is for **Research** purposes or whether the use of **PHI/PI** is for **Statistical Analysis** (also called **Analytics**).

4.4.2 In determining whether to consider whether the collection, use, or disclosure of **PHI/PI** is for **Research** purposes or for **Statistical Analysis**, the ICES Privacy **SME** may have regard to:

a. Whether the purpose is legitimately **Research** or **Statistical Analysis**; and

b. Whether the legislative vehicle relied on for disclosing **PHI/PI** to ICES does not contemplate **Statistical Analysis** and ICES must rely solely on its **Research** authority as set out in its **Corporate Objects** for the collection and use.

4.4.3 **Procedures** for conducting **Project PIAs** are set out in ICES' *Privacy Impact Assessment Review and Analysis for ICES Projects Procedure*.

4.4.4 **Procedures** for conducting all other **PIAs** are set out in ICES' *Privacy Impact Assessment Review and Analysis Procedure*.

4.4.5 When an ICES Privacy **SME** finds no lawful authority for the collection, use, or disclosure of **PHI/PI** for **Research** or for **Statistical Analysis**, the finding of this review must be communicated to the requester as soon as practicable and any **Risks** escalated as necessary pursuant *ICES' Risk Management Policy*.

4.5 Review and analysis of **PIAs**: **Research** purposes

4.5.1 Prior to any finalization of a review or analysis for the collection, use, or disclosure of **PHI/PI** for **Research** purposes, the ICES Privacy **SME** must:

a. Review the written research plan to ensure it complies with the requirements of any statute and its regulations;

b. Ensure that the written research plan was approved by a **Research Ethics Board** ("**REB**");

c. Ensure that a copy of the **REB** approval of the written research plan is included in the **PIA** documentation;

d. Ensure that the **PHI/PI** being requested is consistent with the **PHI/PI** identified in the written research plan approved by the **REB**;

e. Ensure that other information, namely **De-Identified Data,** will not serve the **Research** purpose and no more **PHI/PI** is being requested than is reasonably necessary to meet the **Research** purpose; and

f. Ensure that the **ICES Agent(s)** requesting collection, use, or disclosure of **PHI/PI** for **Research** purposes has acknowledged and signed off that they will comply with s44(6)(a) to (f) of **PHIPA** (for **PHI**) or s5 of O. Reg. 523/18 to the *Coroners Act* (for **PI**).

4.6 Addressing conditions, restrictions, and recommendations

4.6.1 If any conditions or restrictions are identified in the **PIA**, such information must be captured in ICES' **Consolidated Log of Recommendations** as set out in *ICES' Maintaining a Consolidated Log of Recommendations Policy*.

4.6.2 If any further documentation must be completed, provided, or executed with respect to the collection, use, or disclosure of **PHI/PI** identified in a **PIA**, such documentation must be included in ICES' **Consolidated Log of Recommendations**.

4.6.3 If any further documentation must be completed, provided, or executed with respect to an existing business process, information system, **Technology Resource,** or program involving **PHI/PI**, such documentation must be included in ICES' **Consolidated Log of Recommendations**.

4.6.4 The ICES Director, **PLO** is responsible for:

a. Addressing the recommendations arising from **PIAs** or for assigning other **ICES Agent(s)** to address the recommendations;

b. For overseeing the Privacy **SME**'s establishment of timelines to address recommendations; and

c. For ensuring the implementation of the recommendations in accordance with ICES' **PIA Procedures** and ICES' *Maintaining a Consolidated Log of Recommendations Policy.*

4.7 Secure retention, return, and disposal of **PHI/PI** and **PIAs**

4.7.1 Any **PHI/PI** collected and used by ICES must be retained only for the period set out in the applicable **PIA**, **DSA,** and written research plan approved by the **REB,** in compliance with the *ICES Data Retention Schedule Standard.*

4.7.2 Any **PHI/PI** that must be securely returned to the **Data Provider** must be in accordance with the time frame and in the manner identified in the applicable **PIA**, **DSA,** and written research plan approved by the **REB**.

4.7.3 Any **PHI/PI** that must be disposed of in a secure manner must be completed in the time frame and manner set out in the applicable **PIA**, **DSA,** and written research plan approved by the **REB**, in compliance with ICES' *Destruction of ICES Data Procedure.*

4.8 Log of **PIAs**

4.8.1 All required metrics in relation to **PIAs** must be logged, including when:

a. **PIAs** are completed;

b. **PIAs** are initiated but have not been completed; and

c. There is a determination that a **PIA** is not required.

4.8.2 PIAs must be logged in the log applicable to the planned activities:

a. **ICES Project PIA Log** for **ICES Projects**;

b. **TPR Project PIA Log** for **Third Party Research Projects**; or

c. **ICES PIA Log** for all other activities;

4.8.3 The log must include whether the purpose of the planned activities is for **Research** or **Statistical Analysis**.

4.8.4 If any **PIAs** are initiated but not completed, that information must be captured in the applicable log**.**

4.8.5 If the ICES Manager, Privacy or ICES Privacy **SME** decides that a **PIA** is not required that information must be captured in the applicable log, as applicable.

4.8.6 The ICES Manager, Privacy is responsible for ensuring that all reviews and analyses with respect to **PIAs** are communicated to the initial requester in a timely manner from the date of the initial request to the ICES Privacy **SME** as set out in ICES' **PIA Procedures**.

4.9 Ongoing compliance, monitoring, and auditing

4.9.1 Once a **PIA** has been completed, it should be reviewed on an ongoing basis in order to ensure that it continues to be accurate and continues to be consistent with ICES' information practices as set out in ICES' *Privacy and Security Audit Policy*.

4.9.2 The ICES Director, **PLO** is responsible for ensuring that **PIAs** are reviewed in accordance with ICES' *Privacy and Security Audit Policy*.

4.9.3 The following criteria must be assessed by the ICES Director, **PLO** as part of the compliance monitoring activity in the frequency set out in ICES' *Privacy and Security Audit Policy* and **Annual Audit Schedule**:

a. Whether **PIAs** have been conducted for all new collections, uses, or disclosures of **PHI/PI**;

b. Whether **PIAs** have been conducted for all new business process, information system, **Technology Resource,** or program involving **PHI/PI**;

c. Whether **PIAs** have been conducted with respect to all **TPSPs** accessing **PHI/PI**;

d. Whether **PIAs** are out of date and need to be amended; and

e. Whether the details set out in **PIAs** match with the details set out in **DSAs**.

5.0 RELATED DOCUMENTATION

5.1 Policies

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

5.1.2 *Change Management Policy*

5.1.3 *Privacy and Security Audit Policy*

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

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

5.1.6 *Privacy Incident Breach Management Policy*

5.1.7 Maintaining a Consolidated Log of Recommendations Policy

5.1.8 Risk Management Policy

5.2 Standards

5.2.1 ICES Data Retention Schedule Standard

5.2.2 *Cybersecurity Incident Management Standard*

5.3 Procedures

5.3.1 Destruction of ICES Data Procedure

5.3.2 Privacy Impact Assessment Review and Analysis Procedure

5.3.3 Privacy Impact Assessment Review and Analysis for ICES Projects Procedure

5.4 Guidelines

5.5 Tools

5.5.1 ICES Project PIA Form

5.5.2 ICES General PIA Form

5.5.3 **ICES Project PIA Log**

5.5.4 **ICES PIA Log**

5.5.5 **TPR Project PIA Log**

6.0 TRAINING AND COMMUNICATION

6.1 **Policies, Standards,** 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** and **Standards** 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, Standards,** 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, Standards,** or **Procedures**, in accordance with ICES' *Privacy Incident Breach Management Policy* and ICES' *Cybersecurity Incident Management Standard*, as applicable, and 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, Standards,** and **Procedures** may be subject to a range of **Disciplinary Actions** in accordance with 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*.

7.4 Compliance is subject to audit in accordance with 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*.