Collection of ICES Data Policy

Department	Document Number	Organizational Scope	ICES Site	IPC Scope
PLO	**PO.010**	**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)**
June 2014	September 2022	Triennially	September 2025	800PR-PR-005

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:

1.1.1 Mandate that **ICES Data**, including **Personal Health Information ("PHI")**, **Personal Information ("PI")** and **Non-PHI/PI,** must be collected in accordance with applicable legislation, regulation, other legal obligations (e.g., contracts) and requirements set out by the **Information and Privacy Commissioner of Ontario** ("**IPC**").

1.1.2 Identify the purposes for which **PHI/PI** will be collected by ICES, the nature and type of **PHI/PI** that will be collected, from whom the **PHI/PI** will be collected, and the secure manner in which **PHI/PI** will be collected.

1.1.3 Set out ICES' position with respect to the collection of **Non-PHI/PI**.

1.1.4 Clarify that data, both **PHI/PI** and **Non-PHI/PI,** collected by ICES become **ICES Data** at the point of collection.

1.1.5 Establish the accountable and responsible roles to enable the collection of data.

2.0 SCOPE

2.1 This **Policy** governs the collection of **ICES Data** for **ICES Purposes**.

2.2 ICES may from time to time act as a service provider to a third party. In such cases, any data received by ICES acting as a service provider is received as an agent of the third party for whom ICES acts as service provider and, as such, does not constitute a collection of data by ICES. Any data received by ICES as a service provider must be in accordance with ICES' *Third Party Service Provider Policy* and any related procedures.

3.0 ROLES AND RESPONSIBILITIES

3.1 The management and governance of **ICES Data** is delegated to the **Chief Privacy and Legal Officer** ("**CPLO"**) or ICES **Privacy and Legal Office** (**"PLO**") delegate.

3.2 ICES **CPLO** is accountable for ensuring that ICES meets the requirements of this **Policy**.

3.3 ICES Director, **PLO,** ICES Director, **Research and Analysis ("R&A"),** and ICES Director, **Data Quality and Information Management ("DQIM")**, as applicable, are responsible for developing **Procedures** in compliance with this **Policy.**

4.0 DETAILS

4.1 General Principles: **PHI/PI**

4.1.1 ICES is designated a **Prescribed Entity** under section 18(1) of O. Reg. 329/04 for the purposes of section 45 of Ontario's *Personal Health Information Protection Act* **("PHIPA")**. As such, ICES has legal authority to collect **PHI** from a **Health Information Custodian ("HIC")** 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 a health system, including the delivery of services.

4.1.2 ICES is designated a **Prescribed Entity** under section 2 of O. Reg. 523/18 to the *Coroners Act*, for the purposes of section 52.1 of the *Coroners Act* and, as such, ICES has legal authority to collect **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.

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 ICES' **Corporate Objects**, but only if such **Corporate Objects** align with the intended purpose for the collection and use of **PHI/PI** as set out in **PHIPA** and *Coroners Act*, as applicable.

4.1.4 All collections of **PHI/PI** must be to lawfully further ICES' mission, vision, and strategy ("**ICES Purpose**") in accordance with ICES' **Corporate Objects** and not be used for any other purpose.

4.1.5 ICES relies on its ability to collect **PHI/PI** and is committed to protecting the **PHI/PI** it collects in accordance with applicable laws and other legal requirements, including the requirements under **PHIPA**, the *Coroners Act,* their applicable regulations, **Research Ethics Board ("REB")** approvals, ICES' Letters Patents, and applicable contractual arrangements. This includes ensuring that ICES has authority to collect **PHI/PI** and that the **Data Provider** has authority to disclose **PHI/PI**.

4.1.6 ICES shall collect **PHI/PI** only in the manner and to the extent permitted by applicable laws and other legal requirements. In accordance with **Data Minimization** principles, ICES shall collect no more **PHI/PI** than is reasonably necessary for the identified purpose(s), and only when other information, such as **De-Identified Data**, will not serve the identified purpose(s).

4.1.7 ICES respects and aims to incorporate the principle of **Indigenous Data Sovereignty** in its approach to data governance, including the collection of **Indigenous Data**. The First Nations principles of **OCAP** (Ownership, Control, Access, and Possession) also form part of ICES' approach to the collection of **PHI/PI**.

4.1.8 ICES enters into **Data Sharing Agreements** ("**DSA**") to document and authorize ICES' collection of **PHI/PI**, pursuant to the applicable **Privacy Impact Assessment ("PIA")** completed for the requested collection. Such **DSAs** set out ICES' lawful authority to collect the requested **PHI/PI**, and how the **PHI/PI** can be used after collection.

4.1.9 To rely on a statutory authority relating to **Research** for the collection of **PHI/PI**, ICES must be specifically named in the written research plan approved by the **REB**, and such written research plan must clearly articulate the data flow to ICES and ICES' role(s) in handling the **PHI/PI** for the **Research**.

4.1.10 In instances where ICES is not a designated entity in a legislation or regulation relied on by the **Data Provider** for disclosure of **PHI/PI** to ICES, ICES must ensure that it has lawful authority to collect the **PHI/PI** and the **Data Provider** has lawful authority to disclose the **PHI/PI**.

4.2 General Principles: **Non-PHI/PI**

4.2.1 ICES is permitted to collect **Non-PHI/PI** pursuant to this **Policy** only if such collection:

a. Is free of any encumbrances and does not infringe **Intellectual Property** ("**IP**") rights;

b. Is not contrary to applicable legislation and/or regulation;

c. Does not violate the rights of contracting parties;

d. Is not contrary to the mission and vision of ICES;

e. Does not violate the spirit of **Indigenous Data Sovereignty** and **OCAP**;

f. Is supported by applicable ICES **Procedures**; and

g. Does not negatively impact ICES' reputation and/or goodwill.

4.2.2 ICES obtains signed **Data Sharing Request** ("**DSR**") forms or **Licence Agreements** to document and authorize ICES' collections of **Licensed Data** (a type of **Non-PHI/PI**) and such **DSRs** or **Licence Agreements** set out ICES' lawful authority to collect the requested **Licensed Data**, and how it can be used after collection.

4.2.3 ICES can collect and use **Publicly Sourced Data** (a type of **Non-PHI/PI**) without requiring an agreement for authorization of the collection and use.

4.3 Governance of **PHI/PI**: Purposes of Collection

4.3.1 ICES collects **PHI/PI** for the purposes of the administration of its scientific programs and services, including:

a. Health system analysis and evaluation for **ICES Purposes** (sometimes referred to interchangeably as "**Statistical Analysis** or **Analytics**");

b. **Statistical Analysis** related to the health or safety of the public, or any segment of the public; and/or

c. Health-related **Research** conducted by ICES.

4.4 Types of **PHI/PI** Collected

4.4.1 ICES collects the following **PHI/PI**:

a. **PHI** directly from **HICs**, **Prescribed Entities** ("**PEs**"), or **Prescribed Persons** ("**PPs**");

b. **PHI** from **HICs** using **Third Party Service Providers** and **ICES Agents**, known as **Abstractors**, for ICES' **Primary Data Collection ("PDC")** program;

c. **PHI** collected by third parties for their research purposes;

d. **PI** as defined in relevant legislation collected by other organizations or entities in the public and private sectors;

e. **PI** collected from the Chief Coroner under the *Coroners Act* and as authorized through a **s.52.1(1) Agreement** between ICES and the Chief Coroner; and

f. Provider **PI,** information about an individual health care practitioner who is engaged in a provider capacity, collected with consent of the individual provider.

4.5 Categories of **ICES Data** Collected

4.5.1 **Procedures** must be established for all collections of **ICES Data** and will vary depending on the type, nature, and purposes of the collection in the circumstances.

a. **Project Specific Data ("PSD")**, **General Use Data ("GUD")**, and **Controlled Use Data ("CUD")** must be collected pursuant to ICES' *Privacy Impact Assessment Policy*; and

b. **ICES Projects** involving **PDC** activities where **PHI** is collected from **HICs** via **Abstractors** must be collected for the primary purpose of an approved **ICES Project**, and in accordance with ICES' *Privacy Impact Assessment Policy*, ICES' *Third Party Service Provider Policy*, *ICES Agent Policy*, *ICES' Primary Data Collection Standard* and ICES' *Primary Data Collection Procedure.*

4.6 Types of **Non-PHI/PI** Collection

4.6.1 **Procedures** must be established for all collections of **Non-PHI/PI** and will vary depending on the type, nature, and purposes of the collection in the circumstances.

4.7 Review and Approval Process for **PHI/PI**

4.7.1 Prior to collection of **PHI/PI** being permitted, a **PIA** must be completed in accordance with ICES' *Privacy Impacy Assessment Policy*. This **PIA** is reviewed by the appropriate ICES Privacy **Subject Matter Expert ("SME"),** depending on the complexity of the **PIA**, to determine whether to approve the collection of the requested **PHI/PI**.

a. Such review and determination by the ICES Privacy **SME** is completed in accordance with the process set out in ICES' *Privacy Impacy Assessment Policy* and its applicable **Procedures**, including the criteria that must be considered when making a determination to approve the collection of **PHI/PI** or not.

b. Such **PIA** must be in a form approved by ICES **CPLO**; and

c. Each **PIA** performed to assess the proposed collection of **PHI/PI** must include the generation of a **Statement of Purpose ("SOP")**, articulating the purpose(s) for which the **PHI/PI** will be collected, used, and disclosed (as applicable).

4.7.2 ICES requires that a description of **PHI/PI** collected by ICES for **ICES Purposes** is set out in a **DSA** duly executed by **ICES** and the **Data Provider**.

a. Such **DSA** is completed by ICES Legal Services in accordance with the ICES' *Data Sharing Review and Execution Procedure* and ICES' *Execution of Data Sharing Agreement Standard*.

b. Such **DSA** must in a form approved by ICES **CPLO**; and

c. Each **DSA** must incorporate the **SOP** in the form approved by the ICES Privacy **SME** in the corresponding approved **PIA**.

4.7.3 Ultimate accountability for **PIAs** and **DSAs** resides with ICES **CPLO**.

4.7.4 ICES Privacy **SMEs** responsible for determining whether to approve the collection of **PHI/PI** must:

a. Ensure that the collection is lawfully permitted by any of the mechanisms set out in this **Policy**, including but not limited to ensuring collection is permitted by **PHIPA** (for **PHI**) and the *Coroners Act* (for **PI**), and their applicable regulations;

b. Ensure that any and all conditions or restrictions set out in law, contract, or **REB** are satisfied;

c. For **PI**, ensure an agreement is in place between ICES and the Chief Coroner in accordance with s.52.1(1) of the *Coroners Act* and such agreement is in accordance with ICES' *Execution of a section 52.1(1) Agreement Policy*;

d. Ensure that ICES does not collect **PHI/PI** if other information, namely **De-Identified Data**, will lawfully serve an identified **ICES Purpose**;

e. Ensure that no more **PHI/PI** is being requested or collected and retained than is reasonably necessary to lawfully meet an identified **ICES Purpose**; and

f. Ensure that any risks or recommendations set out in **PIAs** are duly documented and adhere to the requirements set out in ICES' *Risk Management Policy*.

4.7.5 All **PIAs** conducted by ICES Privacy **SMEs** will be communicated to the requester in the process identified in ICES' *Privacy Impact Assessment Review and Analysis Procedure* and/or ICES' *Privacy Impact Assessment Review and Analysis for ICES Projects Procedure* as applicable.

4.7.6 All **DSAs** enabled by ICES Legal Services will be communicated to the requester in the process set out in ICES' *Data Sharing Review and Execution Procedure* and ICES' *Execution of Data Sharing Agreement Standard*.

4.7.7 Collections of **PHI/PI** may be subject to additional review and approval requirements depending on the type of collection.

4.8 Secure Retention

4.8.1 All records of **PHI/PI** collected by ICES shall be retained in a secure manner in compliance with the *ICES Data Retention Schedule Standard*.

4.9 Secure Transfer

4.9.1 All records of **PHI/PI** collected by ICES shall be transferred in a secure manner as set out in ICES' *Secure Transfer of PHI/PI Procedure.*

4.9.2 Prior to the secure transfer of the **PHI/PI**, the ICES Director, **Data Quality and Information Management ("DQIM"),** or delegate, is responsible for ensuring any conditions or restrictions that must be satisfied prior to the collection have in fact been satisfied.

4.10 Secure Return or Disposal

4.10.1 All records of **PHI/PI** collected by ICES shall be securely returned or destroyed in accordance with ICES' *Secure Transfer of PHI/PI Procedure,* and ICES' *Secure Disposal Standard,* respectively.

4.10.2 ICES Director, **DQIM** is responsible for ensuring that the records of **PHI/PI** that have been collected are either securely returned or securely disposed of, as the case may be, following the retention period or the date of termination set out in any documentation and/or agreements executed prior to the collection of the **PHI/PI**.

4.10.3 If the records of **PHI/PI** are to be returned to the person or organization from which they were collected, the records must be transferred in a secure manner and in compliance with ICES' *Secure Transfer of PHI/PI Procedure*.

4.10.4 If the records of **PHI/PI** are to be disposed of, such **PHI/PI** must be disposed of in a secure manner and in compliance with ICES' *Secure Disposal Standard.*

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

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

5.1.6 *Privacy Incident Breach Management Policy*

5.1.7 *Risk Management Policy*

5.1.8 *Execution of a section 52.1(1) Agreement Policy*

5.1.9 *Privacy and Security Governance and Accountability Policy*

5.1.10 *Third Party Service Provider Policy*

5.1.11 *ICES Agent Policy*

5.2 Standards

5.2.1 *Secure Disposal Standard*

5.2.2 *ICES Data Retention Schedule Standard*

5.2.3 *Execution of Data Sharing Agreement Standard*

5.2.4 *Risk Management Standard*

5.2.5 *Primary Data Collection Standard*

5.2.6 *Cybersecurity Incident Management Standard*

5.3 Procedures

5.3.1 *Secure Transfer of PHI/PI Procedure*

5.3.2 *Data Sharing Review and Execution Procedure*

5.3.3 *Privacy Impact Assessment Review and Analysis Procedure*

5.3.4 *Privacy Impact Assessment Review and Analysis for ICES Projects Procedure*

5.3.5 *Risk Management Procedure*

5.3.6 *Primary Data Collection Procedure*

5.4 Guidelines

5.5 Tools

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 **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*.