Collection of ICES Data Policy

Department	Reference Number	Organizational Scope	ICES Site	IPC Scope
PLO	010-00-00	ICES Network	ICES Network	All Acts
Original Date (YYYY-MM-DD)	**Current Version** (YYYY-MM-DD)	**Review Frequency**	**Next Review** (Month YYYY)	**Supersedes** (if applicable)
June 2014	2025-07-30	Triennial	July 2028	PO.010

Authority (Title)	Chief Privacy and Legal Officer
Policy Owner (Title)	Director, Privacy and Legal Office
Required Reviewers (Titles)	N/A

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

Provisions highlighted in grey are not yet in effect and are subject to review and approval by the Information and Privacy Commissioner.

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.

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 Privacy and Legal Office ("PLO") delegate.

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

3.3 The Director, PLO, the Director, Research and Analysis ("R&A"), and the 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 as a Prescribed Entity

(a) ICES is designated a **Prescribed Entity** under section 18(1) of Ontario Regulation 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.

(b) ICES is designated a **Prescribed Entity** under section 2 of Ontario Regulation 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.

(c) ICES is designated as a **Prescribed Entity** under section 1 of O. Reg 191/18 of the *Child, Youth and Family Services Act* ("*CYFSA*") for the purposes of section 293 of the *CYFSA* and as such, ICES has legal authority to collect **PI** as defined under the *CYFSA* for the purpose of analysis or compiling statistical information with respect to the management of, evaluation or monitoring of services, the allocation of resources to or planning for those services, including their delivery. ICES is committed to complying with the provisions of *CYFSA* and its regulations applicable to **Prescribed Entities**.

(d) As a **Prescribed Entity**, ICES does not collect **PI** if there is knowledge of non-compliance or serious risk.

4.1.2 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*, *Coroners Act*, and *CYFSA* as applicable.

4.1.3 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.

4.1.4 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*, the *CYFSA*, and 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**.

4.1.5 ICES must 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 must 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).

4.1.6 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**.

4.1.7 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.

4.1.8 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**.

4.1.9 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 standards and procedures; and

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

4.2.2 ICES obtains completed **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 collects and uses **Publicly Sourced Data ("PUB")**, a type of **Non-PHI/PI**. Such collections do not require an agreement with the source of the **PUB** to authorize the collection and/or use. Any collection of **PUB** requires determination of any governance, permissions, obligations or process requirements.

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.

4.3.2 ICES will only collect **PHI/PI** if its **Corporate Objects** align with the intended purpose for the collection and use of **PHI/PI** as set out in *PHIPA* (for **PHI**), the *Coroners Act* (for **PI** collected from the Chief Coroner), and the *CYFSA* (for **PI** collected by ICES as a **PE** under that statute).

4.4 Types of PHI/PI Collected and its Sources

4.4.1 The types of **PHI/PI** ICES collects, and from whom, includes::

(a) **PHI** directly from **HICs**, other PEs, or **Prescribed Persons**;

(b) **PHI** from **HICs** through ICES' Primary Data Collection ("PDC") program;;

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

(d) **PI**, other than **PI** collected by ICES under the *Coroners Act* and *CYFSA*, collected by other organizations or entities in the public and private sectors and other privacy legislation applies to that **PI**;

(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;

(f) **PI** collected from service providers under the *CYFSA*; and

(g) Personal information about an individual health care practitioner who is engaged in a provider capacity, collected with consent of the individual provider or without consent if there is authority to collect lawfully as set out in a **PIA**.

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 the *Privacy Impact Assessment Policy*; and

(b) **ICES Projects** involving **PDC** activities, where **PHI** is collected from **HICs** by Abstractors, must be collected for the primary purpose of an approved **ICES Project**, and in accordance with the following policies, standards, and/or procedures:

(i) *Privacy Impact Assessment Policy;*

(ii) *Third Party Service Provider Policy*;

(iii) *ICES Agent Policy*,

(iv) *Primary Data Collection Standard*, and applicable procedures.

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 Determinations to collect **PHI/PI** as an **ICES Data Holding** are made by the Executive Team ("ET") with guidance and recommendations from the Data Integration & Strategic Committee ("DISC"), which is the cross-departmental committee responsible for overseeing the acquisition and integration of data holdings at ICES.

(a) Decisions to collect **PHI/PI** is subject to completion of a **PIA** and completion of any applicable agreement(s) that will govern the collection by ICES from the **Data Provider**.

4.7.2 Prior to collection of **PHI/PI** being permitted, a **PIA** must be completed in accordance with the *Privacy Impact Assessment Policy*, which addresses the documentation that must be completed, by whom, the criteria for approving or denying the collection, as well as the method and format for communicating the decision.

4.7.3 PIAs are conducted by assigned Privacy **Subject Matter Experts ("SMEs").** Depending on the PIA's level of complexity, the **SME's** assessment in the **PIA** may be reviewed for accuracy and completeness by a senior member of PLO, such as the Director, PLO or CPLO. It is the assigned **SME**, however, who is ultimately responsible for the review and assessment of the **PIA**, to determine whether ICES can collect the requested **PHI/PI**.

(a) Such review and determination by the Privacy **SME** is completed in accordance with the process set out in *Privacy Impact 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 the 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).

4.7.4 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 Legal Services in accordance with the following polices, standards, and/or procedures:

(i) Contract Policy;

(ii) Data Sharing Review and Execution Procedure;

(iii) Data Sharing Agreement Standard; and

(iv) If the collection is **PI** from the Chief Coroner, the *Section 52.1(1) Agreement Policy*.

(b) Such **DSA** must in a form approved by the CPLO; and

(c) Each **DSA** must only permit activities consistent with the **SOP** approved by the Privacy **SME** in the corresponding approved **PIA**.

4.7.5 Ultimate accountability **PIAs** and **DSAs** resides with the CPLO.

4.7.6 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**), the *Coroners Act* (for **PI** collected by ICES from the Chief Coroner), or the *CYFSA* (for **PI** collected by ICES as a **PE** under that statute), and their applicable regulations;

(i) Depending on the complexity of the legislative framework, the Privacy **SME's** assessment may be reviewed by a senior member of the PLO (i.e. Manager, Privacy; Director, PLO; or CPLO) prior to completion of the **PIA**.

(b) Ensure that any and all conditions or restrictions set out in law (including *PHIPA*, the *Coroners Act*, and/or the *CYFSA*, and their regulations, as applicable), contract, or **REB** are satisfied;

(c) For PI collected pursuant to the *Coroners Act*, ensure an agreement is in place between ICES and the Chief Coroner in accordance with:

(i) s.52.1(1) of the *Coroners Act;*

(ii) *Section 52.1(1) Agreement Policy*; and

(iii) *Section 52.1(1) Agreement Standard*.

(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, collected or retained than is reasonably necessary to lawfully meet an identified **ICES Purpose**; and

(f) Ensure that any identified risks and or outstanding recommendations set out in **PIAs** are duly documented and then handled in accordance with the *Risk Management Policy.*

4.7.7 All **PIAs** conducted by Privacy **SMEs** are communicated to the **Requester** in accordance with the *Privacy Impact Assessment Policy* and its applicable procedures.

4.7.8 All **DSAs** enabled by Legal Services will be communicated to the **Requester** in the process set out in the *Contract Policy* and its applicable procedures.

4.7.9 Collections of **Indigenous Data** may be subject to additional review and approval requirements. **ICES Agents** seeking to collect **Indigenous Data** must review the "Indigenous Data at ICES" section on the **ICES Intranet** for information and consult with the Indigenous Partnerships, Data and Analytics ("IPDA") department regarding any additional requirements that may be specific to the particular **Indigenous Data** being requested for collection.

4.8 Secure Retention

4.8.1 All records of **PHI/PI** collected by ICES must be retained in a secure manner in accordance with the *Information Handling Standard* and the *ICES Data Retention Schedule Standard*.

4.9 Secure Transfer

4.9.1 All records of **PHI/PI** collected (undergoing collection) by ICES from a **Data Provider** must be transferred to ICES in a secure manner in accordance with the *Information Handling Standard* and the *Secure Collection, Disclosure, and Transfer of PHI/PI Procedure*.

4.9.2 Prior to the secure transfer of the **PHI/PI**, the 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.

4.9.3 In accordance with the *Secure Collection, Disclosure, and Transfer of PHI/PI Procedure*, prior to receiving the **PHI/PI**, DQIM personnel must verify there is a **DSA** in place between ICES and the **Data Provider** that authorizes ICES to collect the **PHI/PI**.

4.10 Secure Return or Disposal

4.10.1 All records of **PHI/PI** collected by ICES must be securely returned or destroyed in accordance with:

(a) *Secure Collection, Disclosure, and Transfer of PHI/PI Procedure*;

(b) *Destruction of ICES Data Procedure*; and

(c) *Secure Disposal Standard*.

4.10.2 The 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 the *Information Handling Standard* and the *Secure Collection, Disclosure, and Transfer of PHI/PI Procedure*.

4.10.4 If the records of **PHI/PI** are to be disposed of, the records must be disposed of in a secure manner and in accordance with the *Secure Disposal Standard* and *Destruction of ICES Data Procedure*.

4.11 Monitoring and detection of unauthorized collection of PHI/PI

4.11.1 To avoid risk of ICES collecting **PHI/PI** without authorization, in addition to the operational activities conducted by the DQIM team, ICES implements monitoring and detection practices, including Privacy **SMEs** conducting investigations with respect to inappropriate collections through suspected **Privacy Breaches**, in accordance with the *Privacy Breach Management Policy*, or through further investigation arising during a **PIA** review or consultation.

5.0 RELATED DOCUMENTATION

5.1 Policies

5.1.1 *Privacy Impact Assessment Policy*

5.1.2 *Third Party Service Provider Policy*

5.1.3 *ICES Agent Policy*

5.1.4 *Section 52.1(1) Agreement Policy*

5.1.5 *Risk Management Policy*

5.1.6 *Contract Policy*

5.1.7 *Privacy Breach Management Policy*

5.2 Standards

5.2.1 *Primary Data Collection Standard*

5.2.2 *Information Handling Standard*

5.2.3 *ICES Data Retention Schedule Standard*

5.2.4 *Secure Disposal Standard*

5.3 Procedures

5.3.1 *Secure Collection, Disclosure, and Transfer of PHI/PI Procedure*

5.3.2 *Destruction of ICES Data Procedure*

5.4 Tools

5.5 Guidelines

6.0 TRAINING AND COMMUNICATION

6.1 Policies, standards, and procedures are available on the **ICES Intranet**.

6.2 This policy and any related standards and/or 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's **Owner**.

6.3 Once new policies, standards, and procedures are published to the **ICES Intranet**, they are communicated to **ICES Agents** on the **ICES Intranet** and through ICES' weekly email with the organization's internal updates.

7.0 COMPLIANCE AND ENFORCEMENT

7.1 **ICES Agents** must comply with all applicable policies, standards, and procedures.

7.2 **ICES Agents** must notify a Privacy and/or Security **Subject Matter Expert ("SME")** at the first reasonable opportunity if they breache or believe there has been a breach of ICES' privacy and security policies, standards, or procedures in accordance with applicable policies and standards, including:

7.2.1 *Privacy Breach Management Policy*

7.2.2 *Security Incident Management Standard*

7.3 Enforcement of compliance with this policy is the responsibility of the the **ICES Agent** identified as the Authority of this policy.

7.4 All violations of policies**,** standards**,** and procedures may be subject to a range of **Disciplinary Actions** in accordance with applicable policies, including:

7.4.1 *Discipline and Corrective Action Policy*

7.4.2 *Termination of Employment Policy*

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

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

7.5 Compliance is subject to audit in accordance with applicable policies, including:

7.5.1 *Privacy and Security Audit Policy*

8.0 EXCEPTIONS

8.1 Any exceptions requested pursuant to this policy must be in accordance with applicable policies, including:

8.1.1 *Ongoing Review of ICES' Policy Suite Policy*

8.1.2 *Change Management and Exceptions Policy*

8.2 Exceptions cannot relieve ICES of its legal requirements, including but not limited to those established under:

8.2.1 *Personal Health Information Protection Act, 2004 ("PHIPA")* and its regulation;

8.2.2 *Coroners Act* and its applicable regulations;

8.2.3 *Child, Youth and Family Services Act, 2017 ("CYFSA")* and its applicable regulations; and

8.2.4 The **IPC Manual, Coroners Addendum,** and **CYFSA Addendum.**

9.0 CHANGE TABLE

Change Date (YYYY-MM-DD)	**Change Notes**
2025-07-30	■ Reviewed for compliance with ICES' obligations as a **Prescribed Entity**: ○ **IPC Manual:** Privacy Policy in Respect of its Status as a Prescribed Person or Prescribed Entity ○ **Coroners Addendum:** Privacy Policy in Respect of its Status as a Prescribed Entity ○ **CYFSA Addendum:** Privacy Policy in Respect of its Status as a Prescribed Entity ■ Added content regarding *CYFSA* ■ Revised to reflect updated template and standardized language in Sections 6.0 to 9.0 ■ Revised to reflect updated glossary terms and titles of ICES policies, standards, and procedures