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	2025-10-31	Triennial	October 2028	2025-07-30
Authority (Title)	Chief Privacy and Legal Officer			
Policy Owner (Title)	Director, Privacy and Legal Office			
Required Reviewers (Titles)				

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** must be collected in accordance with ICES' obligations set out in the *Privacy Policy*, including but not limited to ensuring collection is in accordance with applicable legislation, regulation, and other obligations (e.g. legal agreements), and compliance requirements set out by the Information and Privacy Commissioner of Ontario ("**IPC**")

1.1.2 Set out ICES' position with respect to the collection of **Non-Identifiable Data**.

1.1.3 Clarify that data collected by ICES becomes ICES Data at the point of collection.

1.1.4 Establish the accountable and responsible roles that enable the collection of data.

1.1.5 Identify circumstances that may require additional processes and/or review prior to the collection of data.

2.0 SCOPE

2.1 This policy governs the collection of data for subsequent use, disclosure, and other **Processing** as ICES Data.

2.2 References to **Identifiable Information** in this policy are only with regards to when the Identifiable Information is ICES Data, namely:

2.2.1 **Personal Health Information ("PHI")**;

2.2.2 **Personal Information ("PI")**; and

2.2.3 **Other Identifiable Data**.

Further information regarding types of ICES Data is set out in the *Information Classification Standard*.

2.3 ICES may at times act as an external service provider to a client. Any data received by ICES when acting as an external service provider is not ICES Data and this policy does not apply.

3.0 ROLES AND RESPONSIBILITIES

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

3.1.1 Delegated authority to manage and govern ICES Data;

3.1.2 Ensures ICES meets the requirements of this policy.

3.2 Director, Privacy and Legal Office ("**PLO**") / Director, Research and Analysis ("**R&A**")

3.2.1 Develops procedures in compliance with and to support implementation of this policy at ICES.

3.3 Director, Data Quality and Information Management ("**DQIM**")

3.3.1 Develops procedures in compliance with and to support implementation of this policy at ICES.

3.3.2 Ensures ICES Data that was initially collected from a Data Provider is securely returned or securely destroyed following applicable retention periods.

3.4 **Executive Team**

3.4.1 Determines when ICES will initiate a new collection of Identifiable Information.

4.0 DETAILS

4.1 *Privacy Policy*

4.1.1 The *Privacy Policy* addresses the following matters related to the collection of ICES Data:

(a) ICES' legal authorities governing collection of Identifiable Information, including but not limited to PHI/PI;

(b) ICES' collection of Identifiable Information for **Statistical Analysis (Analytics)** and **Research**; and

(c) ICES' protection principles when collecting Identifiable Information.

4.1.2 In addition to this policy, any collection of ICES Data must meet the requirements and obligations set out in the *Privacy Policy*.

4.2 Collection of Identifiable Information for use as General Use Data or Controlled Use Data

4.2.1 The Executive Team determines when ICES will initiate a new collection of Identifiable Information for use as **General Use Data ("GUD")** or **Controlled Use Data ("CUD")**.

4.2.2 Executive Team decisions are informed by the guidance and recommendations from the Data Integration & Strategic Committee ("**DISC**"), which is the cross-departmental committee responsible for overseeing the acquisition and integration of **ICES Data Holdings**, including **ICES Derived Data Holdings**.

4.2.3 Proceeding with the decision to collect the Identifiable Information is contingent on completion of a **Privacy Impact Assessment ("PIA")** to confirm ICES' legal authority for the collection.

4.2.4 A **Statement of Purpose ("SOP")** must be created for new collections of Identifiable Information that will be used as GUD or CUD, as set out in the *Statements of Purpose for ICES Data Holdings Containing PHI/PI Policy.*

4.3 Collection of Identifiable Information for use as Project-Specific Data

4.3.1 ICES permits collection of Identifiable Information for use as **Project-Specific Data ("PSD")**. The applicable processes for determining whether to initiate a new collection may depend on the nature of the **ICES Project** or **Third Party Research Project ("TPR Project")**, as further detailed in applicable procedures such as:

(a) *Primary Data Collection Procedure*

(b) *Project Intake Adjudication and Initiation Procedure*

4.3.2 Proceeding with the decision to collect the Identifiable Information is contingent on completion of a PIA to confirm ICES' legal authority for the collection.

4.4 Privacy Impact Assessments

4.4.1 Prior to permitting collection of Identifiable Information, a PIA must be completed in accordance with the *Privacy Impact Assessment Policy*.

4.4.2 The PIA process is used to document:

(a) If a request to collect Identifiable Information is approved; and

(b) Any conditions or restrictions that must be satisfied prior to the collection of Identifiable Information.

4.4.3 As a **Prescribed Entity**, ICES does not collect PHI/PI if there is knowledge of non-compliance or serious privacy risk.

4.4.4 PIAs are conducted by Privacy **Subject Matter Experts ("SMEs")** and the CPLO has ultimate accountability for completion of PIAs.

4.5 Data Sharing Agreements / legal agreements

4.5.1 Prior to collection of Identifiable Information, ICES must execute a **Data Sharing Agreement ("DSA")**, or equivalent applicable legal agreement, which will govern the collection of the data from the **Data Provider**.

4.5.2 DSAs and other agreements are executed in accordance with the following policies, standards, and/or procedures:

(i) *Contract Policy*;

(ii) *Data Sharing Review and Execution Procedure*;

(iii) *Data Sharing Agreement Standard* for:

(A) PHI collected under the *Personal Health Information Protection Act ("**PHIPA**");* and

(B) PI collected under the *Child, Youth and Family Services Act ("**CYFSA**")*

(iv) *Section 52.1(1) Agreement Policy* for PI collected under the *Coroners Act*.

4.5.3 In some circumstances**,** Other Identifiable Data may be collected as **Publicly Sourced Data ("PUB")** in accordance with section 4.9 below. In such instances, the requirement set out in this section 4.5 does not apply.

4.5.4 Legal agreements are completed through Legal Services and the CPLO has ultimate accountability for execution of applicable agreements, as required.

4.6 Indigenous Data

4.6.1 Collection of **Indigenous Data** may be subject to additional review and approval requirements.

4.6.2 **ICES Agents** seeking to collect Indigenous Data must:

(a) Review the information available on the **ICES Intranet**: Indigenous Data at ICES Working with Indigenous Data and Partners

(b) Consult with the Indigenous Partnerships, Data and Analytics ("**IPDA**") department regarding any additional requirements that may be specific to the specific Indigenous Data being requested to collect.

4.7 PHI collected through Primary Data Collection

4.7.1 ICES may collect PHI through **Primary Data Collection ("PDC")** where **Abstractors** collect PHI from the medical records management system of a **Health Information Custodian ("HIC")**.

4.7.2 PHI collected through PDC activities must be collected for the primary purpose of an approved ICES Project.

4.7.3 ICES Projects that include PDC activities are conducted in accordance with the *Primary Data Collection Standard* and applicable procedures.

4.8 Non-Identifiable Data

4.8.1 Collection of Non-Identifiable Data is permitted provided that the collection and use of the data meets the following criteria:

(a) It is free of any encumbrances and does not infringe **Intellectual Property** rights.

(b) It is in accordance with applicable legislation and/or regulations, if the data is subject to legislation and/or regulations;

(c) It does not violate the rights of contracting parties;

(d) It is not contrary to ICES' mission, vision, and strategy;

(e) It does not violate the spirit of **Indigenous Data Sovereignty** and OCAP®;

(f) It is in accordance with ICES' policies, standards, and procedures; and

(g) It does not create the risk of negatively impacting ICES' reputation and/or public goodwill.

4.8.2 Non-Identifiable Data may be subject to completion of a **Data Sharing Request ("DSR")** form or license agreement between ICES and the Data Provider, setting out ICES' lawful authority to collect the requested data and authorize how ICES may subsequently use it.

4.8.3 In some circumstances, Non-Identifiable Data may be collected as PUB in accordance with section 4.9 below.

4.9 Data collected as Publicly Sourced Data

4.9.1 ICES may collect Other Identifiable Data and Non-Identifiable Data as PUB from a publicly accessible source.

(a) PHI/PI must not be collected as PUB.

4.9.2 Collections of PUB do not require an agreement between ICES and the source of the PUB to authorize ICES' collection and/or use.

4.9.3 Any collection of PUB requires determination of applicable governance, permissions, obligations, and/or process requirements for the data.

4.10 Secure transfer of ICES Data

4.10.1 Data must be securely transferred to ICES in accordance with *Information Handling Standard* and the *Secure Collection, Disclosure, and Transfer of PHI/PI Procedure.*

4.10.2 The Director, DQIM, or their delegate, must verify the applicable legal agreement is in place between ICES and the Data Provider prior to the transfer of data to ICES.

4.11 Secure retention of ICES Data

4.11.1 ICES Data is securely retained in accordance with the *Information Handling Standard* and the *ICES Data Retention Schedule Standard.*

4.12 Secure return or destruction of ICES Data

4.12.1 The Director, DQIM, must ensure that ICES Data is either securely returned or destroyed following the applicable retention period(s) set out in the *ICES Data Retention Schedule Standard*.

4.12.2 ICES Data must be securely returned in accordance with the *Information Handling Standard* and the *Secure Collection, Disclosure, and Transfer of PHI/PI Procedure.*

4.12.3 ICES Data must be securely destroyed in accordance with the *Information Handling Standard*, *Secure Disposal Standard,* and the *Destruction of ICES Data Procedure*.

4.13 Monitoring and detection of unauthorized collection of Identifiable Information

4.13.1 To avoid risk of ICES collecting Identifiable Information without authorization, in addition to the operational activities conducted by DQIM prior to transfer, ICES implements other monitoring and detection practices, including investigations by Privacy SMEs with respect to inappropriate collections, which may be identified through activities such as:

(a) Investigations of suspected **Privacy Breaches**;

(b) Ongoing reviews of PIAs; or

(c) Consultations with Privacy Services.

5.0 RELATED DOCUMENTATION

5.1 Policies

5.1.1 *Contract Policy*

5.1.2 *Privacy Impact Assessment Policy*

5.1.3 *Privacy Policy*

5.1.4 *Section 52.1(1) Agreement Policy*

5.1.5 *Statements of Purpose for ICES Data Holdings Containing PHI/PI Policy.*

5.2 Standards

5.2.1 *Data Sharing Agreement Standard*

5.2.2 *ICES Data Retention Schedule Standard*

5.2.3 *Information Classification Standard*

5.2.4 *Information Handling Standard*

5.2.5 *Primary Data Collection Standard*

5.2.6 *Secure Disposal Standard*

5.3 Procedures

5.3.1 *Data Sharing Review and Execution Procedure*

5.3.2 *Destruction of ICES Data Procedure*

5.3.3 *Primary Data Collection Procedure*

5.3.4 *Project Intake Adjudication and Initiation Procedure*

5.3.5 *Secure Collection, Disclosure, and Transfer of PHI/PI 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 breach 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 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: ▪ 01-04: Policy, Procedures, and Practices for the Collection of Personal Health Information ○ Coroners Addendum: ▪ 05-04: Policy, Procedures and Practices for the Collection of Personal information ○ CYFSA Addendum: ▪ 06-04: Policy, Procedures and Practices for the Collection of Personal information

	■ Added content regarding ICES' role as a Prescribed Entity under *CYFSA* (not yet in effect) ■ Added further details clarifying the roles and responsibilities of the ICES Agents involved in reviewing and determining whether to approve the collection of PHI/PI. ■ Updated to reflect: ○ Revised document template and standardized language in Sections 6.0 to 9.0 ○ Revised glossary terms and titles of ICES policies, standards, and procedures
2025-10-31	■ Removed content that was duplicative with information found in the *Privacy Policy* and the *Privacy Impact Assessment Policy*; revised to reflect updated ICES Information classification