Segregation of Personal Information Policy

Department	Reference Number	Organizational Scope	ICES Site	IPC Scope
PLO	027-00-00	ICES Network	ICES Network	Coroners Act / CYFSA
Original Date (YYYY-MM-DD)	**Current Version** (YYYY-MM-DD)	**Review Frequency**	**Next Review** (Month YYYY)	**Supersedes** (if applicable)
2019 October	2025-10-31	Triennial	October 2028	2025-07-31

Authority (Title)	Chief Privacy and Legal Officer
Policy Owner (Title)	Director, Privacy and Legal Office
Required Reviewers (Titles)	Director, Data Quality and Information Management

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 This policy sets out ICES' methods of segregating **Personal Information ("PI")** collected by ICES as a **Prescribed Entity** under the following legislation:

1.1.1 *Coroners Act* and its regulations; and

1.1.2 *Child, Youth and Family Services Act ("**CYFSA**")* and its regulations.

1.2 ICES must securely segregate the above PI from other **ICES Data**, including **Personal Health Information ("PHI")** and **Other Identifiable Data**.

1.2.1 For clarity, PI collected under the *Coroners Act* and PI collected under the *CYFSA* must be segregated from each other.

1.3 Segregation of PI is achieved at ICES through various methods, including segregation through technical means and through compliance oversight. ICES' methods of segregation may vary depending on specific stage of the PI's data lifecycle.

1.4 Even when not possible to technically segregate PI, such as once it is linked to other ICES Data for a specific **ICES Project**, ICES must continue to meet all statutory and compliance obligations specific to the PI.

2.0 SCOPE

2.1 This policy applies to PI collected by ICES as a Prescribed Entity under the following legislation:

2.1.1 *Coroners Act* and its regulations; and

2.1.2 *CYFSA* and its regulations.

3.0 ROLES AND RESPONSIBILITIES

3.1 **Data Covenantors**

3.1.1 Receives, stores, encodes, and performs **Record Linkages** and quality assessment on PI.

3.2 **ICES Analytic Staff**

3.2.1 Performs **Data Linking** to create **Project Datasets**

4.0 DETAILS

4.1 Personal Information as Fully Identifiable Data

4.1.1 PI that ICES collects must be securely stored separate from other ICES Data. Role-based access controls must be in place to ensure the PI, which is **Fully Identifiable Data** at the time of collection, is accessed solely by Data Covenantors.

4.1.2 Data Covenantors are granted access to segregated folders containing the PI solely for the following purposes:

(a) Receiving and storing the PI;

(b) **Encoding** the data to assign an **ICES Key Number ("IKN")** and ensure any **Direct Personal Identifiers ("DPIs")** are removed;

(c) Performing Record Linkages; and

(d) Assessing the quality of the Record Linkages

4.2 ICES Data Holdings containing Personal Information

4.2.1 As part of coding processes, assigning an IKN at ICES relies on a limited amount of PHI being linked to the PI. Besides the assignment of an IKN, no other ICES Data may be linked to the PI until the PI is approved for use in an ICES Project or for disclosure for a **Third Party Research Project ("TPR Project")**.

4.2.2 As an **ICES Data Holding**, all of ICES' existing controls apply to PI to ensure the data remains secure in a separate library using logical separation and role-based access control mechanisms to govern access in accordance with the *Access to ICES Data Standard*.

4.2.3 PI is prohibited from being used to create an **ICES Derived Data Holding** to ensure that the PI remains segregated from other ICES Data.

4.3 Use of Personal Information in ICES Projects and disclosure for Third Party Research Projects

4.3.1 PI may be linked to other ICES Data for use in an ICES Project or for disclosure for a TPR Project.

(a) In accordance with the *Privacy Policy,* PI collected by ICES as a Prescribed Entity under the *CYFSA* is not permitted to be disclosed for the purpose of TPR Projects.

4.3.2 Project-specific Data Linking and use or disclosure of PI is subject to ICES' existing approval processes for all ICES Projects and TPR Projects, including but not limited to completion of a **Privacy Impact Assessment ("PIA")** in accordance with the *Privacy Impact Assessment Policy*.

4.3.3 Only authorized ICES Analytic Staff assigned to a project may access the ICES Data Holding containing the PI in order to create the Project Dataset linking PI to other ICES Data.

(a) Consistent with **Data Minimization** principles, the Project Dataset identifies the limited cohort, timeframe, and variables required to achieve the purpose of the project. The Project Dataset is created and approved in accordance with the *Dataset Creation Plan Procedure.*

4.4 Use of Personal Information in ICES Projects and disclosure for Third Party Research Projects

4.4.1 PI linked to PHI results in data that constitutes **Mixed Records** under s.4(3) of the *Personal Health Information Protection Act ("**PHIPA**")*. Nonetheless, ICES must continue to adhere to all statutory and compliance requirements relevant to the applicable PI even once it is considered PHI as Mixed Records. For clarity, this means:

(a) For PI initially collected by ICES as a Prescribed Entity under the *Coroners Act*, ICES must continue to meet the requirements set out in the *Coroners Act*, its regulations, and the **Coroners Addendum**.

(b) For PI initially collected by ICES as a Prescribed Entity under the *CYFSA*, ICES must continue to meet the requirements set out in the CYFSA, its regulations, and the **CYFSA Addendum**.

4.5 Legislation, legal requirements, and related IPC considerations

4.5.1 ICES' segregation methods must be consistent with the following:

(a) *Coroners Act*;

(b) *CYFSA*;

(c) *PHIPA*;

(d) Other legal requirements that may be applicable; and

(e) Orders, guidelines, fact sheets, and best practices issued by the Information and Privacy Commissioner.

5.0 RELATED DOCUMENTATION

5.1 Policies

5.1.1 *Privacy Impact Assessment Policy*

5.1.2 *Privacy Policy*

5.2 Standards

5.2.1 *Access to ICES Data Standard*

5.3 Procedures

5.3.1 *Dataset Creation Plan 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 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.**

Segregation of Personal Information Policy

9.0 CHANGE TABLE

Change Date (YYYY-MM-DD)	**Change Notes**
2025-07-31	■ Reviewed for compliance with ICES' obligations as a Prescribed Entity: ○ Coroners Addendum: ▪ 05-05: Policy, Procedures and Practices for the Segregation of Personal Information ■ Updated to reflect revised standardized language in Sections 6.0 to 9.0
2025-10-31	■ Added content regarding ICES' role as a Prescribed Entity under CYFSA (not yet in effect) ■ Added further details regarding the methods ICES uses to segregate PI from other ICES Data through the data lifecycle