Segregation of Personal Information Policy

Department	Document Number	Organizational Scope	ICES Site	IPC Scope
DQIM	027-00-00	ICES Network Policy	ICES Network	Coroner's Act
Original Date (month yyyy)	**Last Review Date** (month yyyy)	**Frequency of review** (month yyyy)	**Next Review Due Date** (month yyyy)	**Supersedes (if applicable)**
October 2019	2025-07-31	Triennially	July 2028	PO.027

Authority (Title)	Policy Owner (Title)
Chief Privacy & Legal Officer	Director, Data Quality and Information Management

Required Reviewers (Titles)		
Director, PLO		

Please refer to the **glossary** for terms and 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 set out requirements for the segregation of **Personal Information ("PI")** collected from the Chief Coroner under the *Coroners Act* and its regulation.

2.0 SCOPE

2.1 This **Policy** applies to **PI** collected by ICES with respect to its status as a **Prescribed Entity** under the *Coroners Act* and its regulation.

3.0 ROLES AND RESPONSIBILITIES

4.0 DETAILS

4.1 **PI** collected under the *Coroners Act* and its regulation must be securely segregated from other **PI** and **Personal Health Information ("PHI")** held by ICES. This requirement is applicable to **PI**, including **Fully Identifiable Data, Coded Data**, and **Risk Reduced Coded Data ("RRCD")**.

4.2 **PI** collected by ICES under the *Coroners Act* and its regulation are segregated from other **PI** and **PHI** in ICES' custody and control through access control groups. The secure manner of segregation must be consistent with the *Coroners Act,* Ontario's *Personal Health Information Protection Act* **("PHIPA")**, and other legal requirements, as well as orders, guidelines, fact sheets, and best practices issued by the **Information and Privacy Commissioner of Ontario ("IPC")**.

4.3 Access to **Fully Identifiable Data** is restricted to ICES **Data Covenantors** who meet all requirements in accordance with the applicable **Data Sharing Agreements ("DSA")**.

4.4 **Data Covenantors** are granted access to segregated folders containing **Fully Identifiable Data** solely for the following purposes:

4.4.1 Receiving and storing data.

4.4.2 Performing **Record Linkages**.

4.4.3 Creating **Coded Data**.

4.4.4 Assessing the quality of **Record Linkages**.

5.0 RELATED DOCUMENTATION

5.1 *Privacy and Security Incident Breach Management Policy*

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

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

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

5.5 *Change Management Policy*

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**.

9.0 CHANGE TABLE

Change Date (YYYY-MM-DD)	**Change Notes**