Segregation of Personal Information Policy

Department	Document Number	Organizational Scope	ICES Site	IPC Scope
DQIM	PO.027	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	September 2022	Triennially	September 2025	N/A

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.

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** 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** 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** 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** or **Procedures**, in accordance with ICES' *Privacy and Security Incident Breach Management Policy* and associated **Procedures**, as set out in the framework posted on the ICES **PLO**/Cybersecurity site on the **ICES Intranet.**

7.3 All other violations under ICES privacy and security **Policies** and **Procedures** may be subject to a range of **Disciplinary Actions** including warning, temporary or permanent loss of **Access Privileges**, legal sanctions and/or termination of employment for cause, or contract with ICES pursuant to *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* and associated **Procedures**.

7.4 Compliance is subject to annual audit by an ICES Privacy **SME** or ICES Risk & Compliance Analyst pursuant to the **Annual Audit Schedule** established under 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*.