De-Identification and Aggregation Policy

Department	Document Number	Organizational Scope	ICES Site	IPC Scope
PLO	PO.015	ICES Network Policy	ICES Network	All Acts
Original Date (month yyyy)	**Last Review Date** (month yyyy)	**Frequency of review** (month yyyy)	**Next Review Due Date** (month yyyy)	**Supersedes (if applicable)**
September 2022	N/A	Triennially	September 2025	N/A

Authority (Title)	Policy Owner (Title)
Chief Privacy and Legal Officer	Director, PLO

Required Reviewers (Titles)		
Sr. Director, Research, Data & Financial Services	Director, DQIM	Director, R&A

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

1.0 PURPOSE

1.1 The purpose of this **Policy** is to:

1.1.1 Set out ICES' position with respect to **De-Identificatio**n and **Aggregation** of **Personal Health Information ("PHI")** and **Personal Information ("PI")**.

1.1.2 Set out ICES' **Policy** on **Re-Identification**.

1.1.3 Establish the accountable roles and responsibilities for **De-Identification** and **Aggregation** of **PHI/PI**.

2.0 SCOPE

2.1 This **Policy** applies to:

2.1.1 All **ICES Agents** involved in the **De-Identification** and **Aggregation** process of **PHI/PI** for **ICES Purposes**.

2.1.2 All **ICES Agents** involved in the use of **De-Identified Data –** including **Aggregate Data (Summary Output)** and **Publishable Data** - for **ICES Purposes**.

2.1.3 All **ICES Agents** involved in **Re-Identification Risk Assessment** ("**RIRA**").

3.0 ROLES AND RESPONSIBILITIES

3.1 ICES **Chief Privacy and Legal Officer ("CPLO")** is accountable for ensuring that ICES defines and implements appropriate **Procedures** to enable ICES to meet the requirements of this **Policy**.

3.2 ICES Senior Director, for the platform of Research and Data, and the ICES Senior Director, Strategic Partnerships and Digital Services are responsible for ensuring that ICES has **Procedures** and criteria with respect to the processes and criteria for **De-Identified Data**.

3.3 ICES **Principal Investigator**, or if the **Principal Investigator** is not a **Full Status ICES Scientist** the **Responsible ICES Scientist**, is responsible for conducting and documenting **RIRAs**.

3.4 **ICES Staff Scientists** are responsible for conducting and documenting **RIRAs** for **ICES Projects** completed for ICES **Knowledge Users**.

4.0 DETAILS

4.1 General Principles

4.1.1 The meaning ascribed to **De-Identification** must be consistent with the definition set out in the *Personal Health Information Protection Act, 2004* **("PHIPA")** such that in relation to the **PHI** of an individual, **De-Identification** means to remove any information that identifies the individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify the individual.

4.1.2 ICES will not use or disclose **PHI/PI** if other information, namely **De-Identified Data**, will serve the identified purposes instead. **PHI/PI** must be used or disclosed only where **De-Identified Data** will not serve the identified purposes.

4.1.3 **Aggregate Data (Summary Output)** is a type **De-Identified Data** at ICES that is subject to the following conditions when sharing with members of a **Project Team** who are not **ICES Agents**, because such **Aggregate Data (Summary Data)** may contain **ICES Confidential Information** and/or **Third Party Confidential Information**:

a. Such individuals who are not **ICES Agents** are identified as **ICES Collaborating Researchers** on the **Privacy Impact Assessment** ("**PIA**") for the **ICES Project**; and

b. Such individuals sign an **ICES Collaborating Researchers** Non-Disclosure Agreement prior to receiving access to the **Aggregate Data (Summary Data)**.

4.1.4 **Publishable Data** is a type of **De-Identified Data** that may be shared publicly without additional conditions because it is created once **ICES Confidential Information** and/or **Third Party Confidential Information** is removed from **Aggregate Data (Summary Output)**.

4.1.5 Limitations for using and disclosing **De-Identified Data** are set out below:

Type of De-Identified Data	Access	Disclosure	Cell Size	Risk Clearance
Publishable Data	Can be shared publicly	-Can be included in manuscript submissions for potential **ICES Publications** -Can be published in **Reports**	May not contain cell sizes fewer than six	Must be subject to a **RIRA**
Aggregate Data (Summary Output)	Can be shared with **Project Team** subject to the restrictions set out in this **Policy** for **ICES Collaborating Researchers**	-Cannot be included in manuscript submissions for potential **ICES Publications** -Cannot be published in **Reports**	May contain cell sizes fewer than six	Not subject to a **RIRA** but responsible **ICES Agents** must ensure there is no reasonable risk of re-identification in the circumstances

4.1.6 The process and criteria for creating and sharing of **De-Identified Data** is set out in accompanying **Procedures** subject to this **Policy**.

4.1.7 **Publishable Data** must be reviewed and assessed by the responsible **ICES Agents** identified in this **Policy** prior to disclosure by ICES, including its inclusion in manuscripts submissions or published in **Reports**, such that the **Publishable Data** does not:

a. Contain information that identifies an individual or could foreseeably be used, either alone or with other information, to re-identify an individual;

b. Contain cell-sizes fewer than six; and

c. Contain **ICES Confidential Information** and **Third Party Confidential Information**.

4.1.8 The **RIRA** process and criteria for reviewing and sharing **Publishable Data**, including in manuscripts or **Reports**, is set out in accompanying **Procedures** to this **Policy**.

4.1.9 ICES must continue to explore new tools developed to assist in ensuring that the **Policy** and **Procedures** with respect to **De-Identification** and **Aggregation** are based on an assessment of the actual risk of **Re-identification**.

4.1.10 **ICES Agents**, other than **Data Covenantors** in the course of their duties for ICES, are explicitly prohibited from attempting to decrypt information that is encrypted, attempting to identify an individual based on unencrypted information and attempting to identify an individual based on prior knowledge.

4.1.11 Prohibitions on **Re-identification**, except as permitted under s.11.2 of **PHIPA**, are set out in a variety of ICES' **Policies**, **Procedures**, the **ICES Agent and Confidentiality Agreement ("ICES Agent CA")** template, the **Third Party Service Provider Agreement** template, and privacy and security training and awareness material, and are subject to audits pursuant to ICES' Privacy and Security Audit program.

4.2 Cell Sizes

4.2.1 Any **Procedures** at ICES that are subject to this **Policy** must have regard to, and must be consistent with the meaning of "identifying information" in s.4(2) of **PHIPA** with respect to cell-sizes fewer than six.

4.2.2 Any use and disclosure of **De-Identified Data** must have regard to the restrictions related to cell sizes of fewer than six contained in **Data Sharing Agreements ("DSA")**, **Research Agreements,** and written research plans to which ICES is subject.

4.2.3 All **ICES Agents** are prohibited from using **De-Identified Data**, including information in cell-sizes of fewer than six to **Re-identify** an individual, except as permitted under s.11.2 of **PHIPA**.

4.3 Re-Identification

4.3.1 At ICES, the concept of **Re-identification** must take into consideration contextual factors (thoughtful consideration based on a combination of pre-existing and general knowledge) where it could be reasonably foreseeable in the circumstances that such **De-Identified Data** could be utilized, either alone or with other information, to identify an individual.

4.3.2 If an assessment of **Re-identification** concludes that there is a risk where it could be reasonably foreseeable in the circumstances that such **De-Identified Data** could be utilized, either alone or with other information to identify the individual, such risk is considered a **Re-identification Risk**.

4.3.3 The criteria for assessing the **Re-Identification Risk** must include:

a. Who is the intended audience for the **Publishable Data**? What background information is it reasonable to expect that the intended audience is known or assumed to have?

b. Whether other directly identifying information or indirectly identifying information is available to the audience and could be used, together with the **Publishable Data,** to **Re-Identify** an individual;

c. Whether there is a reasonable chance a person or group with prior knowledge will be able to inadvertently **Re-identify** an individual and whether there is an inherent risk of re-identification in the **Publishable Data**; and

d. Such criteria are hereinafter known as "**Re-identification Risk Assessment Criteria**".

4.4 Documentation of a **RIRA**

4.4.1 Each time a **RIRA** is completed, a corresponding sub-folder must be created in the **Project T: Drive Folder** where **Risk Cleared Deliverables** must be saved.

4.4.2 A sub-folder of **Risk Cleared Deliverables** must be established for each **ICES Project**.

4.4.3 For **Non-Appointed ICES Agents** (**NAIAs**), **Aggregate Data (Summary Data)** must be risk-cleared prior to being shared with the **NAIA** outside of the **Analytic Environment**. For **ICES Project** output that does not result in deliverables shared outside of the **Project Team**, a copy of the **Risk Cleared Deliverables** also needs to be saved in a sub-folder to the **Project T: Drive Folder**.

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 *Privacy and Security Audit Policy*

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

5.6 *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 PLO/Cybersecurity Intranet site.

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*.