De-Identification and Aggregation Policy

Department	Reference Number	Organizational Scope	ICES Site	IPC Scope
PLO	015-00-00	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)
September 2022	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)	Senior Director, Research, Data and Financial Services
	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:

1.1.1 ICES' position with respect to de-identification and aggregation of **Identifiable Information**.

1.1.2 ICES' policy on re-identification.

1.1.3 The accountable roles and responsibilities of **ICES Agents** for de-identification and aggregation of Identifiable Information.

2.0 SCOPE

2.1 This policy applies to ICES Agents involved in:

2.1.1 The ae-identification and aggregation process of Identifiable Information;

2.1.2 The use of **De-Identified Information**;

2.1.3 The **Re-Identification Risk Assessment ("RIRA")** process; and

2.1.4 ICES activities requiring re-identification of De-Identifiable Information.

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.**

2.3 References to De-Identified Information in this policy are only with regards to when the De-Identified Information is ICES Data, namely:

2.3.1 **Aggregate Data (Summary Output)**; and

2.3.2 **Publishable Data.**

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

3.0 ROLES AND RESPONSIBILITIES

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

3.1.1 Accountable for ensuring that ICES defines and implements appropriate procedures to enable ICES to meet the requirements of this policy.

3.2 Senior Director, Research, Data and Finance / Senior Director, Strategic Partnerships and Digital Services

3.2.1 Ensures ICES has procedures with respect to the processes and criteria for De-Identified Information.

4.0 DETAILS

4.1 <u>De-Identified Information definition</u>

4.1.1 De-identification is the process of transforming **Direct Personal Identifiers ("DPIs")** and **Quasi-Identifiers** related to an individual and, as a result of de-identification, either:

(a) The information no longer identifies the individual; or

(b) It is not reasonably foreseeable in the circumstances that the information could be utilized, either alone or with other information, to identify the individual.

4.1.2 At ICES, De-Identified Information is ICES Data or Corporate Information relating to an individual in which both DPIs and Quasi-Identifiers have been transformed and/or removed, and, when necessary, appropriate administrative, technical, and physical safeguards are in place so that it is not reasonably foreseeable in the circumstances that the information could be used, either alone or with other information, to identify the individual. The level and type of de-identification required is contextual and determined on a case-by-case basis.

4.2 <u>Aggregate Data (Summary Output) definition</u>

4.2.1 Aggregation is the process of summarizing data to a group level such that, subject to the presence of **Small Cells** (cell sizes of fewer than six), the risk of re-identification is very low.

4.2.2 At ICES, Aggregate Data (Summary Output) is ICES Data that has been compiled from record-level data to a level of aggregation that ensures that the identity of individuals cannot be determined by reasonably foreseeable methods. Aggregate Data (Summary Output) containing small cells may be Identifiable Information or De-Identified Information and must be determined on a case-by-case basis. It may also contain additional **ICES Confidential Information** and, as such, access is limited to members of the **Project Team**.

4.3 <u>Considerations about De-Identified Information and Aggregate Data (Summary Output) definitions</u>

4.3.1 ICES' definitions of De-Identified Information and Aggregate Data (Summary Output) must adhere to the following requirements:

(a) They must be consistent with the definitions of:

(i) "identifying information" set out in subsection 4(2) of the *Personal Health Information Protection Act ("**PHIPA**");*

(ii) "de-identify" set out in section 2 of *PHIPA*;

(iii) "personal information" set out in the *Freedom of Information and Protection of Privacy Act ("**FIPPA**")*; and

(b) They must include consideration of context-specific risks, such as cell sizes, which may, particularly in combination with other available information, increase the risk of re-identification.

4.3.2 ICES must continue to explore new tools available or in development that may assist in ensuring this policy and related procedures are based on an assessment of the actual risk of re-identification of an individual.

4.4 Data Minimization

4.4.1 ICES adheres to **Data Minimization** principles when collecting, using, and disclosing ICES Data.

4.4.2 ICES must not use or disclose Identifiable Information if other information, namely De-Identified Information, will serve the purpose instead.

4.5 Creation and disclosure of De-Identified Information

4.5.1 De-Identified Information is created and shared with a Project Team in accordance with the *RAE-DSH – Creating and Sharing Aggregate Data (Summary Output) Procedure*.

4.5.2 De-Identified Information is subject to a Re-Identification Risk Assessment, in accordance with the *Re-Identification Risk Assessment Procedure*, prior to disclosure to **Data Recipients** (such as **Knowledge Users**) or disseminating publicly.

(a) The RIRA process is to ensure that the De-Identified Information intended for disclosure does not identify an individual and it is not reasonably foreseeable in the circumstances that the information could be used, either alone or with other information, to identify an individual.

4.5.3 Any use and disclosure of De-Identified Information must have regard to the restrictions related to Small Cells contained in applicable legal agreement(s) and written research plans pursuant to which ICES initially collected the Identifiable Information.

4.5.4 Below in an overview of access and disclosure of De-Identified Information, which is further detailed in this policy and associated procedures.

	Aggregate Data (Summary Output)	**Publishable Data**
Access	• Can be shared with ICES Agents and Collaborating Researchers on the Project Team	• Can be shared publicly

Disclosure	• Cannot be included in manuscript submissions • Cannot be published in Reports	• Can be included in manuscript submissions • Can be published in Reports
Cell Size	• May contain cell sizes fewer than six	• May not contain cell sizes fewer than six
Risk Clearance	• Not subject to a RIRA but the responsible ICES Agent must ensure there is no reasonable risk of re-identification in the circumstances	• Must be subject to a RIRA

4.6 Aggregate Data (Summary Output)

4.6.1 Aggregate Data (Summary Output) may be shared with members of a Project Team even if they are not ICES Agents, subject to the following requirements:

(a) They are identified as **Collaborating Researchers** on the **Privacy Impact Assessment ("PIA")** for the **ICES Project**; and

(b) They each sign a "Collaborating Researchers Non-Disclosure Agreement" prior to receiving access to the Aggregate Data (Summary Output).

4.6.2 The above conditions are safeguards implemented by ICES to ensure:

(a) The Aggregate Data (Summary Output) remains De-Identified Information since Small Cells may be present; and

(b) Additional ICES Confidential Information that may be contained with the Aggregate Data (Summary Output) is protected.

4.6.3 In accordance with Data Minimization principles, Aggregate Data (Summary Output) should be shared only with members of the Project Team and not distributed amongst ICES Agents who are not on the Project Team.

4.7 Publishable Data

4.7.1 Publishable Data may be disclosed publicly, such as inclusion in manuscript submissions or published in **Reports**, without additional conditions because it has been subject to:

(a) A RIRA, in accordance with the *Re-Identification Risk Assessment Procedure*, to confirm the risk of re-identification is very low; and

(b) A review to confirm it does not contain ICES Confidential Information.

4.8 Risk of re-identification

4.8.1 The risk 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 the De-Identified Information could be utilized, either alone or with other information, to identify an individual.

4.8.2 ICES takes a risk-based approach to assessing the risk of re-identification, including assessing against a criteria, as set out in the *Re-Identification Risk Assessment Procedure*.

4.8.3 There is a risk of re-identification if a RIRA concludes there is a risk where it could be reasonably foreseeable in the circumstances that the De-Identified Information could be utilized, either alone or with other information, to identify an individual.

4.9 Re-Identification

4.9.1 Non-permitted re-identification

(a) Except as permitted in section 4.9.2 below, ICES Agents are prohibited from using De-Identified Information (including information in Small Cells) to identify an individual. This includes:

(i) Attempting to decrypt information that is encrypted for the purpose of re-identification;

(ii) Attempting to identify an individual based on unencrypted information; and

(iii) Relying on prior knowledge in combination with De-Identified Information in order to re-identify an individual.

(b) Prohibitions on re-identification are set out in:

(i) ICES' policies, standards, and procedures;

(ii) The **ICES Agent and Confidentiality Agreement ("ICES Agent CA")**;

(iii) **Third Party Service Provider Agreements**; and

(iv) Privacy and security training and awareness materials.

(c) The above prohibition is also subject to audits in accordance with the *Privacy and Security Audit Policy.*

4.9.2 Permitted re-identification

(a) In some circumstances, **Data Covenantors** are permitted to re-identify individuals using De-Identified Information. Circumstances may include:

(i) Re-Identification of **Coded Data** in order to address data quality issues;

(ii) Converting information back into the identifiable form for returning data to the Data Provider; and

(iii) Permitting ICES and researchers to contact patients for approved purposes.

(b) Re-Identification of this nature is subject to the following requirements:

(i) The re-identification must be permitted by the law (e.g. under s.11.2 of *PHIPA*) , as approved by the Director, PLO;

(ii) The Data Covenantor must be acting in the course of their duties for ICES when engaging in re-identification; and

(iii) The re-identification must be reviewed, approved, and conducted in accordance with applicable policies, standards, and procedures, including but not limited to:

(A) *Cohort Disclosure Procedure; and*

(B) *Secure Collection, Disclosure, and Transfer of PHI/PI Procedure.*

5.0 RELATED DOCUMENTATION

5.1 Policies

5.1.1 *Privacy and Security Audit Policy*

5.2 Standards

5.2.1 *Information Classification Standard*

5.3 Procedures

5.3.1 *Cohort Disclosure Procedure*

5.3.2 *RAE-DSH – Creating and Sharing Aggregate Data (Summary Output)*

5.3.3 *Re-Identification Risk Assessment Procedure*

5.3.4 *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 Incident and 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:** Policy, Procedures, and Practices with Respect to De-Identification and Aggregation ○ **Coroners Addendum:** Policy, Procedures, and Practices with Respect to De-Identification and Aggregation ○ **CYFSA Addendum:** Policy, Procedures, and Practices with Respect to De-Identification and Aggregation ■ Added content regarding ICES' role as a Prescribed Entity under CYFSA ■ Added additional details regarding Cell Sizes and Re-Identification ■ Revised to reflect updated template and standardized language in Sections 6.0 to 9.0
2025-07-31	■ Revised to update ICES Information classification; Re-ordered content and additional revisions for clarity.