

Record Linkage and Data Linking Standard



Department	Reference Number	Organizational Scope	ICES Site	IPC Scope
DQIM	014-02-00	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)
2025-10-31	2026-09-10	Annual	September 2027	2025-10-31
Authority (Title)		Senior Director, Research, Data and Financial Services		
Policy Owner (Title)		Director, Data Quality and Information Management		
Required Reviewers (Titles)		Director, Privacy and Legal Office		

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 standard outlines:

- 1.1.1 ICES' permitted uses of **Identifiable Information** to conduct **Record Linkages** and **Data Linking**;
- 1.1.2 Obligations and requirements when conducting Record Linkages and Data Linking; and
- 1.1.3 Logging requirements for requested, approved, and completed Record Linkages and Data Linking.

1.2 ICES conducts Record Linkages and Data Linking for the purposes of:

- 1.2.1 Administration of its scientific programs and services, including **Statistical Analysis (Analytics)** and **Research**; and
- 1.2.2 Disclosure of **ICES Data**, in accordance with the *Disclosure of ICES Data Policy*.

2.0 SCOPE

2.1 This standard applies to any Record Linkages and Data Linking conducted by **ICES Agents**.

2.2 References to Identifiable Information in this standard 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**.

Record Linkage and Data Linking Standard



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

3.0 ROLES AND RESPONSIBILITIES

3.1 ICES Agents

- 3.1.1 If authorized in accordance with the *Access to ICES Data Standard*, conducts Record Linkages and/or Data Linking.

4.0 DETAILS

4.1 Lawful authority to link Identifiable Information

- 4.1.1 When ICES conducts Record Linkages and Data Linking with Identifiable Information, it is a use of that Identifiable Information by ICES. As such, Record Linkages and Data Linking must be in accordance with ICES' lawful authorities for using Identifiable Information as set out in the *Use of ICES Data Policy*.

4.2 Segregation of Personal Information

- 4.2.1 Any Record Linkages and Data Linking of PI that was initially collected by ICES as a **Prescribed Entity** under the *Coroners Act* and under the *Child, Youth and Family Services Act ("CYFSA")* must comply with the segregation requirements set out in the *Segregation of Personal Information Policy*.

4.3 Record Linkage

- 4.3.1 Record Linkage is conducted on Identifiable Information after it is collected by ICES and all requirements regarding collection of Identifiable Information, as set out in the *Collection of ICES Data Policy*, must be met prior to conducting Record Linkages.
- 4.3.2 Record Linkages requires ICES to use the Identifiable Information, in its **Fully Identifiable Data** form, to create **Coded Data** by:
 - (a) Transforming and/or removing all **Direct Personal Identifiers ("DPIs")**;
 - (b) Transforming and/or removing some **Quasi-Identifiers**; and
 - (c) Assigning an **ICES Key Number ("IKN")**.
- 4.3.3 Record Linkages must be conducted in accordance with the *Creating Coded Data at ICES Procedure* and completed only by authorized ICES Agents as set out in the *Access to ICES Data Standard*.
- 4.3.4 Record Linkage is sometimes referred to as data matching or entity resolution.

4.4 Data Linking

- 4.4.1 ICES conducts the following kinds of Data Linking to create:
 - (a) **Project Datasets**; and
 - (b) **ICES Derived Data Holdings**
- 4.4.2 Data Linking uses Identifiable Information in the **ICES Data Repository**, which includes:
 - (a) **General Use Data ("GUD")**;

Record Linkage and Data Linking Standard



- (b) **Controlled Use Data (“CUD”)**; and
- (c) **Project-Specific Data (“PSD”)**.

4.5 Mixed Records obligations

- 4.5.1 ICES links PI or Other Identifiable Data to PHI, this results in data that constitutes **Mixed Records** under s.4(3) of the *Personal Health Information Protection Act (“PHIPA”)*.
- 4.5.2 ICES’ use, disclosure, and other **Processing** of Mixed Records must comply with *PHIPA*, its regulation, and applicable compliance requirements that ICES has a Prescribed Entity under *PHIPA*.
- 4.5.3 Additionally, ICES must continue to adhere to all legal obligations and compliance requirements relevant to the applicable PI or Other Identifiable Data even once it is linked as Mixed Records. This includes, but is not limited to:
 - (a) Complying with the *Coroners Act*, its regulations, and the **Coroners Addendum** for PI that ICES collected as a Prescribed Entity under the *Coroners Act*;
 - (b) Complying with the *CYFSA*, its regulations, and the **CYFSA Addendum** for PI that ICES collected as a Prescribed Entity under the *CYFSA*; and
 - (c) Complying with any obligations associated with Other Identifiable Information based applicable laws, legal agreements, or other requirements.

4.6 Project Datasets: project-specific Data Linking

- 4.6.1 ICES conducts project-specific Data Linking of Coded Data in order to create Project Datasets for **ICES Projects** and **Third Party Research Projects (“TPR Projects”)**.
- 4.6.2 Project-specific Data Linking to create a Project Dataset is subject to:
 - (a) Completion of a **Privacy Impact Assessment (“PIA”)**, in accordance with the *Privacy Impact Assessment Policy*; and
 - (b) Approval of the **Dataset Creation Plan (“DCP”)**, in accordance with the *Dataset Creation Plan Procedure*.
- 4.6.3 Additional requirements may apply based on the specific nature of the project that will use the Project Dataset. See:
 - (a) The *Use of ICES Data Policy* regarding ICES Project requirements; and
 - (b) The *Disclosure of ICES Data Policy* regarding TPR Project requirements.
- 4.6.4 Project-specific Data Linking must be conducted in accordance with the *RAE-DSH – Creating Datasets for Other Level Users Procedure* by authorized ICES Agents as set out in the *Access to ICES Data Standard*.
- 4.6.5 Project Datasets created through project-specific Data Linking must be de-identified as soon as practicable after the purpose of the linkage is fulfilled. To the extent possible, ICES Agents should use the **Aggregate Data (Summary Output)** once it is created from the Project Dataset, instead of the Project Dataset itself, to carry out the project. De-identification of the Project Dataset is conducted in accordance with the *De-Identification and Aggregation Policy*.

Record Linkage and Data Linking Standard



4.7 Creation of ICES Derived Data Holdings

- 4.7.1 ICES conducts Data Linking to create ICES Derived Data Holdings by linking Coded Data from existing ICES Data Holdings.
- 4.7.2 Prior to creation of an ICES Derived Data Holding, the following conditions must be met:
 - (a) The Director, Research and Analysis (“**R&A**”) must determine there is a need for the data holding and it could be used in a broad range of ICES Projects;
 - (b) A request for the proposed ICES Derived Data Holding must be submitted to the Data Integration & Strategy Committee (“**DISC**”) for approval, with the decision clearly documented in DISC’s meeting minutes; and
 - (c) A PIA must be conducted.
- 4.7.3 In accordance with the *Segregation of Personal Information Policy*, PI is prohibited from being used to create an ICES Derived Data Holding to ensure that the PI remains segregated from other ICES Data.
- 4.7.4 An ICES Derived Data Holding is subject to:
 - (a) The obligations and restrictions, if any, of the GUD and CUD that is used to create the ICES Derived Data Holding; and
 - (b) Any requirements set out for ICES Data Holdings in ICES’ policies, standards, and procedures.
- 4.7.5 Only authorized ICES Agents, as set out in the *Access to ICES Data Standard*, are permitted to create ICES Derived Data Holdings.

4.8 Logging requirements

- 4.8.1 ICES maintains information regarding all requests and approvals for Record Linkages and Data Linking of Identifiable Information and, if needed, can promptly generate a log from its information. The information below is in the approved PIAs for the requests and maintained by Privacy Services:
 - (a) The name of the **Requestor** of the PIA as the ICES Agent requesting the Record Linkage or Data Linking;
 - (b) The date of approval of the PIA; and
 - (c) The names of GUD, CUD, and/or PSD approved to be linked.
- 4.8.2 ICES Agents in the DQIM department also maintain a log of Record Linkages of Fully Identifiable Data.

4.9 Secure retention of ICES Data

- 4.9.1 ICES Data is securely retained in accordance with the *Information Handling Standard* and the *ICES Data Retention Schedule Standard*.

4.10 Secure destruction of ICES Data

- 4.10.1 ICES Data must be securely destroyed in accordance with the *Information Handling Standard*, *Secure Disposal Standard*, and the *Destruction of ICES Data Procedure*.

Record Linkage and Data Linking Standard



5.0 RELATED DOCUMENTATION

5.1 Policies

- 5.1.1 *Collection of ICES Data Policy*
- 5.1.2 *De-Identification and Aggregation Policy*
- 5.1.3 *Disclosure of ICES Data Policy*
- 5.1.4 *Privacy Impact Assessment Policy*
- 5.1.5 *Segregation of Personal Information Policy*
- 5.1.6 *Use of ICES Data Policy*

5.2 Standards

- 5.2.1 *Access to ICES Data Standard*
- 5.2.2 *ICES Data Retention Schedule Standard*
- 5.2.3 *Information Classification Standard*
- 5.2.4 *Information Handling Standard*
- 5.2.5 *Secure Disposal Standard*

5.3 Procedures

- 5.3.1 *Creating Coded Data at ICES Procedure*
- 5.3.2 *Dataset Creation Plan Procedure*
- 5.3.3 *Destruction of ICES Data Procedure*
- 5.3.4 *RAE-DSH – Creating Datasets for Other Level Users 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

Record Linkage and Data Linking Standard



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 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
2026-09-10	■ Added details about the approval requirements for ICES Derived Data Holdings

Please refer to the [Change Log](#) for historical changes to this standard.