

Disclosure of ICES Data Policy



Department	Reference Number	Organizational Scope	ICES Site	IPC Scope
PLO	017-00-00	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)
2022-06-01	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)	Director, Data & Analytic Services			
	Director, Strategic Partnerships			

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 This policy sets out the requirements when **ICES Agents** disclose **ICES Data**, which includes both **Identifiable Information** and **De-Identified Information**.
- 1.2 Generally, ICES discloses Identifiable Information for:
 - 1.2.1 **Third Party Research Projects** (“**TPR Projects**”), which includes disclosure of:
 - (a) **Risk Reduced Coded Data** (“**RRCD**”); and
 - (b) **Cohort Disclosure Lists**.
 - 1.2.2 Use by other **Prescribed Entities** and **Prescribed Persons** in accordance with their prescribed purposes under the *Personal Health Information and Protection Act* (“**PHIPA**”).
- 1.3 Generally, ICES discloses De-Identified Information for:
 - 1.3.1 **ICES Projects** where **Aggregate Data (Summary Output)** is disclosed to **Collaborating Researchers** who are members of the **Project Team**;
 - 1.3.2 ICES Projects where **Publishable Data** is disclosed to **Knowledge Users**, such as policymakers; and
 - 1.3.3 Dissemination of results of ICES Projects as Publishable Data.
- 1.4 When disclosing ICES Data, ICES ensures:
 - 1.4.1 The disclosure is consistent with ICES’ **Corporate Objects**;
 - 1.4.2 The disclosure complies with applicable laws, and their regulations, including but not limited to:

Disclosure of ICES Data Policy



- (a) *PHIPA*;
- (b) *Coroners Act*; and
- (c) *Child, Youth and Family Services Act ("CYFSA")*

1.4.3 The disclosure is in accordance with any legal agreements governing the ICES Data; and

1.4.4 The disclosure adheres to **Data Minimization** principles.

2.0 SCOPE

2.1 This policy applies to all ICES Agents when:

- 2.1.1 Disclosing ICES Data to a specific **Data Recipient**; and
- 2.1.2 Disseminating results of an ICES Project.

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 **Non-Identifiable Data**;
- 2.3.2 Aggregate Data (Summary Output); and
- 2.3.3 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 this policy to ensure all disclosures of ICES Data comply with applicable laws and any other legal requirements.

3.2 Director, Data & Analytic Services ("DAS") / Director, Strategic Partnerships / Director, Data Quality and Information Management ("DQIM")

- 3.2.1 Ensure all standards and procedures relating to the disclosure of ICES Data comply with this policy.

4.0 DETAILS

4.1 Lawful authority for disclosure of Identifiable Information

- 4.1.1 ICES as a Corporation

Disclosure of ICES Data Policy



- (a) Any disclosure of Identifiable Information must be in accordance with ICES' authority as a not-for-profit corporation and, specifically, as permitted by ICES' Corporate Objects.

4.1.2 PHIPA

- (a) As a Prescribed Entity under *PHIPA*, ICES may disclose PHI in the following circumstances:
 - (i) Disclosure for TPR Projects (research purposes) in accordance with s.44 of *PHIPA* as if ICES were **Health Information Custodian ("HIC")**, which is permitted by s.18(4) of Ontario Regulation 329/04 to *PHIPA*.
 - (ii) Disclosure to other Prescribed Entities and to Prescribed Persons, for their prescribed purposes (non-research purposes) as set out in *PHIPA*, in accordance with s.18(4) of Ontario Regulation 329/04 to *PHIPA*.
 - (iii) Disclosure as required by law.
- (b) ICES may disclose De-Identified Information created from ICES' use of this PHI.

4.1.3 Coroners Act

- (a) As a Prescribed Entity under the *Coroners Act*, ICES may disclose PI in the following circumstances:
 - (i) Disclosure for TPR Projects (research purposes) in accordance with s.5 of Ontario Regulation 523/18 to the *Coroners Act*.
 - (ii) Disclosure to the Chief Coroner for non-research purposes in accordance with s.6 of Ontario Regulation 523/18 for the *Coroners Act*.
 - (iii) Disclosure as required by law.
- (b) Except as identified above, ICES is prohibited by law from disclosing this PI for any other non-research purposes. ICES may disclose De-Identified Information created from ICES' use of this PI.

4.1.4 CYFSA

- (a) As a Prescribed Entity under the *CYFSA*, ICES collects PI under the *CYFSA* for use by ICES and only discloses this PI as required by law.
- (b) ICES is prohibited by law from disclosing PI for non-research purposes except if the disclosure is required by law or the disclosure is to another Prescribed Entity under the *CYFSA*.
- (c) Regardless of ICES' permitted legal authority to disclose this PI, ICES does not permit disclosure of PI for research or non-research purposes. ICES may disclose De-Identified Information created from ICES' use of this PI.

4.1.5 Other applicable laws and legal agreements

Disclosure of ICES Data Policy



- (a) ICES may disclose Other Identifiable Data for research or non-research purposes provided such disclosure is permitted by:
 - (i) Any applicable laws governing the Other Identifiable Data; and
 - (ii) Any applicable legal agreements between ICES and the Data Provider that governs ICES' permitted collection, use, and disclosure of the Other Identifiable Data.

4.2 Data Minimization

- 4.2.1 ICES adheres to Data Minimization principles when disclosing Identifiable Information, including:
 - (a) Not disclosing Identifiable Information if other information, such as De-Identified Information, will serve the purpose; and
 - (b) Not disclosing more Identifiable Information than is reasonably necessary to meet the purpose.

4.3 Oversight of disclosure of Identifiable Information

- 4.3.1 Disclosures of Identifiable Information for TPR Projects are managed through the DAS department, and ICES Agents in this department are responsible for:
 - (a) Oversight of TPR Projects to ensure all applicable requirements set out in s.4.4 below are addressed prior to disclosure;
 - (b) Retaining relevant documentation about the TPR Project, including but not limited to:
 - (i) Review and approval requests;
 - (ii) Research ethics materials; and
 - (iii) Copies of the completed **Privacy Impact Assessment ("PIA")** and executed agreement between ICES and the **Third Party Researcher**.
- 4.3.2 Disclosures of Identifiable Information for non-research purposes, such as disclosure to another Prescribed Entity or Prescribed Person, are managed through the Strategic Partnerships department, and the ICES Agents in this department are responsible for:
 - (a) Oversight of the planned disclosure to ensure all applicable requirements set out in s.4.4.1 below are addressed prior to disclosure;
 - (b) Retaining relevant documentation about the disclosure, including but not limited to:
 - (i) Review and approval requests;
 - (ii) Copies of the completed PIA and executed agreement between ICES and the Data Recipient.
- 4.3.3 In addition to the above, ICES Agents in Privacy Services, Legal Services, and DQIM retain documentation related to their applicable processes for these disclosure activities. For instance, retention of PIAs, legal agreements, and **Certificates of Destruction**, respectively.

4.4 Requirements for disclosure of Identifiable Information

- 4.4.1 Disclosure of Identifiable Information is subject to following requirements being met prior to disclosure:

Disclosure of ICES Data Policy



- (a) For TPR Projects only:
 - (i) **Research Ethics Board (“REB”)** approval of a written research plan.
 - (ii) For PI initially collected by ICES under the *Coroners Act*, consent from the Chief Coroner.
- (b) For all disclosures of Identifiable Information:
 - (i) Completion of a PIA.
 - (ii) Execution of a legal agreement between ICES and the Data Recipient.
 - (iii) Management of any identified risks.

4.4.2 When disclosing Identifiable Information, it must also be securely transferred, retained, and returned or destroyed, as applicable.

4.5 Research ethics approval

- 4.5.1 The TPR Project must have a written research plan that was approved by an REB and complies with requirements of applicable law governing the Identifiable Information.
- 4.5.2 The approving REB must meet any membership requirements or other criteria set out for it in applicable law governing the Identifiable Information intended for disclosure, including but not limited to *PHIPA* and the *Coroners Act*.
- 4.5.3 REB approval is reviewed and confirmed by ICES as part of the PIA process and further requirements related to REB approval are set out in the *Privacy Impact Assessment Policy*.

4.6 Chief Coroner’s consent for disclosure of PI for research purposes

- 4.6.1 ICES requires the consent of the Chief Coroner prior to any disclosure of PI for a TPR Project when the PI was initially collected by ICES under the *Coroners Act*.
- 4.6.2 The Chief Coroner must consent to the disclosure for the specific TPR Project, and the research purpose must be related to the health or safety of the public or any segment of the public.
- 4.6.3 The consent from the Chief Coroner is reviewed and confirmed by ICES as part of the PIA process.

4.7 Privacy Impact Assessments

- 4.7.1 All disclosures of Identifiable Information must be assessed in a PIA in accordance with the *Privacy Impact Assessment Policy*.
- 4.7.2 The PIA determines if:
 - (a) ICES has lawful authority to disclose the information by law and legal agreements;
 - (b) Any and all conditions or restrictions set out in applicable laws and their regulations have been satisfied; and
 - (c) The disclosure is in accordance with ICES’ policies, standards, and procedures.

4.8 Legal agreements

- 4.8.1 A legal agreement must be executed between ICES and the Data Recipient prior to disclosure of Identifiable Information, in accordance with the *Contract Policy*.

Disclosure of ICES Data Policy



4.9 Risk management

- 4.9.1 Any unaddressed conditions, restrictions, or unresolved risks identified in a PIA and/or a legal agreement between ICES and the Data Recipient must be addressed through ICES' Enterprise Risk Management ("ERM") program and in accordance with the *Risk Management Policy*.
- 4.9.2 Decisions to move forward with a particular disclosure of Identifiable Information must be made taking into consideration the *Risk Management Policy*.

4.10 Secure transfer of Identifiable Information

- 4.10.1 When ICES discloses Identifiable Information containing **Direct Personal Identifiers ("DPPIs")**, the information must be securely transferred by ICES to the Data Recipient in accordance with the *Information Handling Standard* and the *Secure Collection, Disclosure, and Transfer of PHI/PI Procedure*.
- 4.10.2 When ICES discloses Identifiable Information in the form of RRCD, the Third Party Researcher may only access the RRCD on a secure **ICES Data Environment**. Only De-Identified Information may be released from the ICES Data Environment to the Third Party Researcher.

4.11 Secure return or destruction of Identifiable Information

- 4.11.1 The Director, DQIM, or their delegate, must ensure that Identifiable Information is either securely returned or destroyed in accordance with the terms of the legal agreement executed by ICES and the Data Recipient, including but not limited to the method of secure return or destruction, and the retention period.
- 4.11.2 If the Identifiable Information is not securely returned or a Certificate of Destruction is not received within the time frame identified in the applicable legal agreement, such findings must be reported to Legal Services for advising on next appropriate steps. The CPLO and/or Chief Executive Officer ("CEO") may be consulted as needed to address the issue.
- 4.11.3 In instances where ICES disclosed Identifiable Information as required by law, different legal requirements may apply and Legal Services must advise on the matter.

4.12 Disclosure of De-Identified Information

- 4.12.1 De-Identified Information is created through ICES' use of ICES Data. As such, all requirements set out in ICES' policies, standards, and procedures for use of ICES Data must be met first, including but not limited to the *Use of ICES Data Policy*.
- 4.12.2 Permitted disclosure of Aggregate Data (Summary Output)
 - (a) ICES may disclose Aggregate Data (Summary Output) to Collaborating Researchers if the following requirements are met:
 - (i) They sign a "Collaborating Researcher Non-Disclosure Agreement" for ICES;
 - (ii) They are identified as a Collaborating Researcher on the PIA for the ICES Project; and
 - (iii) The Aggregate Data (Summary Output) that will be disclosed is created in accordance with the *De-Identification and Aggregation Policy*.
 - (b) The "Collaborating Researcher Non-Disclosure Agreement" must be signed prior to the

Disclosure of ICES Data Policy



Collaborating Researcher being listed on the project's PIA.

- (i) The Privacy SME reviewing the PIA is responsible for confirming the agreement is on record at ICES (logged and filed with the Privacy and Legal Office), and the PIA cannot proceed to review and approval without all listed Collaborating Researchers have a signed agreement in place.
- (c) The “Collaborating Researcher Non-Disclosure Agreement” must require the Collaborating Researcher to agree that they will not use the Aggregate Data (Summary Output) to identify an individual, including not attempt to decrypt information that is encrypted or identify an individual based on unencrypted information and/or the Collaborating Researcher’s prior knowledge.

4.12.3 Permitted disclosure of Publishable Data

- (a) ICES may disclose Publishable Data to Data Recipients or the public, such as:
 - (i) Disclosure to Knowledge Users, such as policymakers;
 - (ii) Dissemination of results of ICES Projects.
- (b) All disclosures of Publishable Data must be reviewed in accordance with the *De-Identification and Aggregation Policy*, including completion of a **Re-Identification Risk Assessment (“RIRA”)** prior to the disclosure, to ensure the De-Identified Information does not identify an individual and it is not reasonably foreseeable in the circumstances that the information could be utilized, either alone or with other information, to identify an individual.

5.0 RELATED DOCUMENTATION

5.1 Policies

- 5.1.1 *Contract Policy*
- 5.1.2 *De-Identification and Aggregation Policy*
- 5.1.3 *Risk Management Policy*
- 5.1.4 *Use of ICES Data Policy*

5.2 Standards

- 5.2.1 *Information Classification Standard*
- 5.2.2 *Information Handling Standard*

5.3 Procedures

- 5.3.1 *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**.

Disclosure of ICES Data Policy



- 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 **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.*

Disclosure of ICES Data Policy



9.0 CHANGE TABLE

Change Date (YYYY-MM-DD)	Change Notes
2025-07-30	<ul style="list-style-type: none">■ Reviewed for compliance with ICES' obligations as a Prescribed Entity:<ul style="list-style-type: none">○ IPC Manual:<ul style="list-style-type: none">■ Policy, Procedures, and Practices for Disclosure of Personal Health Information for Research Purposes and the Execution of Research Agreements■ Log of Research Agreements○ Coroners Addendum:<ul style="list-style-type: none">■ Policy, Procedures and Practices for Disclosure of Personal information for Research Purposes and the Execution of Research Agreements■ Log of Research Agreements■ Reviewed and revised as part of ongoing review of ICES' Policy Suite activities■ Revised to reflect updated template and standardized language in Sections 6.0 to 9.0
2025-10-31	<ul style="list-style-type: none">■ Renamed from <i>Disclosure of ICES Data for Research Purposes and Execution of Research Agreements Policy</i>■ Revised to add information from the <i>Disclosure of ICES Data for Purposes other than Research Policy</i> so the <i>Disclosure of ICES Data Policy</i> can now govern all disclosures by ICES■ Relocated research agreement-related matters to the <i>Contract Policy</i>■ Revised to reflect updated ICES Information classification