Disclosure of ICES Data for Purposes Other than Research Policy

Department	Reference Number	Organizational Scope	ICES Site	IPC Scope
PLO	016-00-00	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	2025-07-30	Triennual	July 2028	N/A
Authority (Title)	Chief Privacy and Legal Officer			
Policy Owner (Title)	Director, PLO			
Required Reviewers (Titles)	Director, DQIM			
	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 The purpose of this Policy is to:

1.1.1 Define the rules for the disclosure of **ICES Data** by **ICES Agents** to authorized entities to ensure consistency with the mandate of ICES, in accordance with applicable laws and other legal requirements with respect to:

(a) Limiting disclosure of **Personal Health Information ("PHI")** and **Personal Information ("PI")** if other information will serve the purpose; and

(b) Not to disclose more PHI/PI than is reasonably necessary to meet the purpose for the disclosure.

2.0 SCOPE

2.1 This Policy applies to all ICES Agents who disclose ICES Data.

3.0 ROLES AND RESPONSIBILITIES

3.1 ICES Chief Privacy and Legal Officer ("CPLO") is accountable for this overarching Policy to ensure that all disclosures of ICES Data are in compliance with applicable laws and any other legal requirements.

3.2 ICES Director, Strategic Partnerships, and ICES Director, Data Quality and Information Management ("DQIM") are responsible for ensuring that all standards and procedures relating to the disclosure of ICES Data are in compliance with this Policy.

4.0 DETAILS

4.1 Authority for disclosure of PHI/PI

4.1.1 All disclosures of PHI/PI must be assessed in a **Privacy Impact Assessment ("PIA")** for the purposes of identifying whether the disclosure of such PHI/PI is lawful; however, the ultimate decision for moving forward with a particular disclosure of PHI/PI must be made taking into consideration the *Risk Management Policy.*

(a) ICES as a Corporation

(i) Any disclosures of PHI/PI by ICES Agents must be in accordance with ICES' authority as a not-for-profit corporation and specifically, as permitted by ICES' **Corporate Objects**.

(b) Authority as Permitted or Required by Law

(i) ICES will only disclose **PHI/PI** where permitted or required by law including, as applicable:

(A) *Personal Health Information Protection Act* ("*PHIPA*") and its regulations;

(B) The *Coroners Act* and its regulation;

(ii) ICES may disclose PHI to other **Prescribed Entities ("PEs")** in accordance with s.18(4) of O. Reg. 329/04 to *PHIPA* and to **Prescribed Persons ("PPs")** in accordance with s.18(4) of O. Reg. 329/04 to *PHIPA* for their prescribed purposes; and

(iii) Any disclosures must be assessed and approved in accordance with any other applicable ICES Policies, Procedures, and agreements.

(c) Authority Under Contracts

(i) Any disclosure of PHI/PI by ICES Agents must be consistent with the **Data Sharing Agreement ("DSA"),** or other applicable agreement, that governs the collection and use of such PHI/PI by ICES.

4.2 Prohibited disclosures of PI initially collected from the Chief Coroner

4.2.1 For PI initially collected by ICES as a Prescribed Entity under the Coroners Act, disclosure of PI is limited to disclosures required by law and disclosures to the Chief Coroner for purposes other than research.

4.2.2 All other disclosures of this PI for non-research purposes are prohibited.

4.3 Requirements prior to disclosing PHI/PI

4.3.1 Privacy Impact Assessments

(a) Prior to any disclosure of PHI/PI, ICES must be satisfied that a PIA pursuant to ICES' *Privacy Impact Assessment Policy* has been conducted by an ICES Privacy **Subject Matter Expert ("SME")** which sets out the requirements that must be satisfied and the criteria that must be considered for determining whether to approve or deny the request for the disclosure of PHI/PI for purposes other than **Research**, including but not limited to ensuring that:

(i) The disclosure is permitted or required under applicable laws, regulations, and other legal requirements, and that any and all conditions or restrictions set out in the applicable laws and their regulations have been satisfied;

(ii) The PHI/PI does not contain any additional identifying information not necessary or relevant to the purpose of the disclosure;

(iii) The PHI/PI does not contain any additional identifying information not necessary or relevant to the purpose of the disclosure; and

(iv) No more PHI/PI is disclosed than is reasonably necessary to meet the identified purpose.

(b) An analysis must be set out in the applicable PIA and communicated in written format to the requester; and

(c) If any risks are identified in the applicable PIA, such risks must be escalated in accordance with the *Risk Management Policy*.

4.3.2 Data Sharing Agreements

(a) Any disclosures of PHI/PI must also have a corresponding DSA executed in accordance with *Data Sharing Agreement Standard* prior to any disclosure of PHI/PI for purposes other than **Research**.

4.3.3 Exceptions and risks identified

(a) Any conditions, restrictions, or risks identified in a PIA and/or DSA must be addressed in accordance with the *Risk Management Policy.*

(b) Any exceptions to ICES' policies, standards, and procedures must be approved in accordance with the *Change Management and Exceptions Policy*.

4.3.4 Secure transfer

(a) All disclosures of PHI/PI must be conducted in accordance with the *Secure Collection, Disclosure, and Transfer of PHI/PI Procedure*, which includes a requirement that a DSA be executed prior to any disclosure of PHI/PI.

4.4 Secure return or destruction

4.4.1 ICES DQIM personnel are responsible for ensuring that records of PHI/PI disclosed to a person or organization for purposes other than research are either securely returned or securely disposed of, as the case may be, following the retention period outlined in the DSA or the date of termination of the DSA.

4.4.2 If records of PHI/PI are not securely returned or a certificate of destruction is not received within a reasonable period of time following the retention period identified in the DSA or the date of termination of the DSA, such finding must be reported to the ICES CPLO, who will engage the ICES Chief Executive Officer ("CEO") to discuss next steps.

4.5 Documentation related to approved disclosures of PHI/PI

4.5.1 All documentation related to the receipt, review, approval or denial of requests for the disclosure of PHI/PI for purposes other than research must be in accordance with the *Privacy Impact Assessment Policy*.

4.6 Disclosing De-Identified Data

4.6.1 ICES may disclose **De-Identified Data** in the following circumstances:

(a) To **Knowledge Users**, such as policy-makers; and

(b) For incorporation of results of an **ICES Project** into **Reports**.

4.6.2 Requirements prior to disclosing De-Identified Data for purposes other than Research

(a) Prior to the disclosure of De-Identified Data, ICES Agents must satisfy themselves that the use of PHI/PI to create the De-Identified Data is permitted under *Use of ICES Data Policy*.

(b) If the use of PHI/PI to create the De-Identified Data is permitted under the *Use of ICES Data Policy*, then such disclosures are permitted pursuant to this Policy.

(c) Prior to disclosures of De-Identified Data, the **Responsible ICES Scientist** must conduct a **Re-Identification Risk Assessment ("RIRA**"), in accordance with the *Re-Identification Risk Assessment Procedure* and be satisfied the De-Identified Data 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 *Change Management and Exceptions Policy*

5.1.2 *Privacy Impact Assessment Policy*

5.1.3 *Risk Management Policy*

5.1.4 *Use of ICES Data Policy*

5.2 Standards

5.2.1 Data Sharing Agreement 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**.

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 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 for Disclosure of Personal Health Information for Purposes Other Than Research ○ **Coroners Addendum:** Policy, Procedures and Practices for Disclosure of Personal information for Purposes Other Than Research ■ 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