Disclosure of ICES Data for Purposes Other than Research Policy

Department	Document Number	Organizational Scope	ICES Site	IPC Scope
PLO	PO.016	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)**
June 2022	September 2022	Triennially	September 2025	N/A

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

Required Reviewers (Titles)		
Director, DQIM	Director, SP	

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

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 **Procedures** and **Practice**s 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 ICES' *Risk Management Policy* and ICES' *Risk Management Standard*.

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 Ontario's *Personal Health Information Protection Act* **("PHIPA")**, the *Coroners Act*, and their regulations as applicable;

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 Requirements prior to disclosing PHI/PI

4.2.1 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 researching, 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 pursuant to ICES' *Risk Management Standard* and associated **Procedures**.

4.2.2 **Data Sharing Agreements**

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

4.2.3 **Exceptions and Risks identified**

a. Any conditions, restrictions, or **Risks** identified in a **PIA** and/or **DSA** must be addressed pursuant to ICES' *Ongoing Review of Privacy and Security Policies, Procedures, Practices and Exceptions Policy*, ICES' *Risk Management Policy,* ICES' *Risk Management Standard,* and ERM **Procedures** as applicable.

4.2.4 **Secure transfer**

a. All disclosures of **PHI/PI** must be conducted in accordance with ICES' *Secure Transfer of PHI/PI Procedures*, which includes a requirement that a **DSA** be executed prior to any disclosure of **PHI/PI**.

4.3 **Secure return or destruction**

4.3.1 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**.

4.3.2 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.

4.4 **Documentation related to approved disclosures of PHI/PI**

4.4.1 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 logged in ICES' **Project PIA Log** or ICES' **PIA Log**.

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

4.5.1 To **Knowledge Users**, such as policy-makers; and

4.5.2 For incorporation of results of an **ICES Project** into publications and reports.

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

4.6.1 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 ICES' *Use of ICES Data Policy*.

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

4.6.3 Prior to disclosures of **De-Identified Data**, the Responsible ICES Scientist must conduct a **Re-Identification Risk Assessment ("RIRA")**, in accordance with ICES' *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 *Ongoing Review of Privacy and Security Policies, Procedures, Practices, and Exceptions Policy*

5.2 *Change Management Policy*

5.3 *Discipline and Corrective Action in Relation to ICES Data Policy*

5.4 *Termination or Cessation of Employment or Contractual Relationship in Relation to ICES Data Policy*

5.5 *Re-Identification Risk Assessment Procedure*

5.6 *Use of ICES Data Policy*

5.7 *Secure Transfer of PHI/PI Procedure*

5.8 *Risk Management Policy*

5.9 *Execution of Data Sharing Agreement Standard*

5.10 *Risk Management Standard*

5.11 *Privacy Impact Assessment 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*.