



# Third Party Service Provider Policy

Department	Document Number	Organizational Scope	ICES Site	IPC Scope
PLO	PO.004	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)
September 2022	N/A	Triennially	September 2025	N/A
Authority (Title)		Policy Owner (Title)		
Chief Privacy and Legal Officer		Director, PLO		
Required Reviewers (Titles)				
N/A				

Please refer to the [glossary](#) for terms and definitions.

## 1.0 PURPOSE

1.1 This **Policy** summarizes the obligations of ICES and the authority, obligations, and duties for **Third Party Service Providers (“TPSPs”)** who access and use **Personal Health Information (“PHI”)** or **Personal Information (“PI”)** during their engagement with ICES. This **Policy** also summarizes ICES’ position with respect to acting as a **TPSP** for external parties (e.g. **Third Party Researchers**, Ontario Health in respect of a prescribed registry, COO in respect of FNIGC Data).

## 2.0 SCOPE

2.1 This **Policy** applies to all legal entities, including sole proprietors, individuals, partnerships, or corporations who sign a contract with ICES to provide services as set out in ICES’ *Contract Policy*. This **Policy** also applies to ICES with respect to obligations it may accept arising out of a relationship of servitude to a designated third party.

## 3.0 ROLES AND RESPONSIBILITIES

### 4.0 DETAILS

#### 4.1 Obligations on ICES

4.1.1 All **TPSPs** that are permitted to access and use **PHI/PI** while providing services to ICES shall be considered **ICES Agents**, with the possible exception of **Electronic Service Providers (“ESPs”)**.

4.1.2 A template agreement must be developed in a form approved by the ICES **Chief Privacy and Legal Officer (“CPLO”)** containing the required language as mandated by the **Information and Privacy Commissioner of Ontario (“IPC”)** (the “**TPSP Template**”).

4.1.3 All **TPSPs** must execute a written contract with ICES that includes the required language set out in the **TPSP Template** prior to such **TPSP** accessing and using the **PHI/PI**.

4.1.4 ICES **CPLO** is responsible for ensuring that all **TPSPs** enter into such a contract.



# Third Party Service Provider Policy

- 4.1.5 **TPSPs** are prohibited from being given access to **PHI/PI** until they have executed the **ICES Agent and Confidentiality Agreement (“ICES Agent CA”)** and have been provided privacy and security training pursuant to ICES’ *Privacy and Security Training and Awareness Policy*.
- 4.1.6 **ICES** shall not provide **PHI/PI** to a **TPSP** if other information, namely **De-identified Data**, will serve the purpose and will not provide more **PHI/PI** than is reasonably necessary to meet the purpose set out in the contract.
- 4.1.7 The **ICES Information Custodian** is responsible for determining the necessary amount of **PHI/PI** to be provided by ICES to meet a specific purpose, including whether other available information, namely **De-identified Data**, will serve the purpose set out in the contract.
- 4.1.8 The **ICES Information Custodian** is responsible for ensuring that ICES does not provide more **PHI/PI** than is reasonably necessary to meet the purpose.
- 4.1.9 The **ICES Information Custodian** is responsible for ensuring that **PHI/PI** provided to a **TPSP** are either securely returned to ICES or are securely disposed of following the termination of the contract as further set out in ICES’ *Secure Transfer of PHI/PI Procedure*.
- 4.1.10 ICES must ensure that retention for all contracts executed with **TPSP** accessing **PHI/PI** meets the criteria set out by the **IPC** including:
  - a. A log must be maintained of all contracts executed with **TPSPs**; and
  - b. All executed contracts must be retained in ICES’ designated **Contract Management Software (“CMS”)**.
- 4.1.11 The ICES **CPLO** has overall accountability for ascertaining that all contracts are logged with delegation of responsibility assigned to ICES’ Legal Services personnel, ICES Research & Analysis personnel, the ICES Science Office, and/or ICES’ Procurement department as set out in ICES’ *Contract Review Procedure*.
- 4.2 Entitlements for **TPSPs**
  - 4.2.1 **TPSPs** are granted access to ICES infrastructure, resources, and **ICES Data** in accordance with ICES’ **Policies, Procedures**, and any applicable contracts.
- 4.3 Authority, Obligations, and Duties for **TPSPs**
  - 4.3.1 **Authority** - In acting on behalf of ICES, **TPSPs** only have the authority expressly granted to them by ICES during the term of their agency relationship as set out in the **ICES Agent CA** and any other contractual documentation between ICES and the **TPSP** that identifies the services to be provided to ICES.
  - 4.3.2 **Obligations** - **TPSPs** must always act in accordance and comply with:



# Third Party Service Provider Policy

- a. ICES' **Policies** and **Procedures**;
- b. The obligations set out in the contract(s) executed between the **TPSP** and ICES;
- c. The duration of their term as an **ICES Agent**, as explicitly set out in the **ICES Agent CA**; and
- d. The limited purpose for which they have been designated an **ICES Agent** and **TPSP** by ICES.

#### 4.3.3 **Duties - TPSPs** accessing **PHI/PI** must also comply with the *ICES Agent Policy* such that they:

- a. Only engage in activities expressly permitted by ICES **Policies**, **Procedures**, and any applicable contracts; and
- b. Not sign documents, or click-to-accept terms and conditions, on behalf of ICES.

#### 4.4 **ICES Abstractors**

4.4.1 In addition to any other requirements in this **Policy**, **ICES Abstractors** shall comply with ICES' **Policies** and **Procedures** applicable to their role, and any other requirements communicated to them by their designated **ICES Project Manager**.

#### 4.5 **Electronic Service Providers**

4.5.1 Contracts with **ESPs** shall explicitly state whether such **TPSP** is also an **ICES Agent** in providing services pursuant to the contract.

4.5.2 If an **ESP** is not an **ICES Agent**, ICES must include a term in the contract that explicitly prohibits the **ESP** from using **PHI/PI**, except as necessary while providing services pursuant to the contract.

4.5.3 If an **ESP** is not an **ICES Agent**, ICES must include a term in the contract that explicitly prohibits the **ESP** from disclosing **PHI/PI** to which it has access while providing services, except as required by law.

#### 4.6 **ICES Scientists**

4.6.1 If an **ICES Scientist** as an **ICES Agent** also acts in a **TPSP** capacity, they must ensure that they are managing their cross-appointments in such a way that they avoid any perceived or actual conflicts of interest, in accordance with the ICES' *Conflict of Interest Policy*.

#### 4.7 **Expectations**

4.7.1 **ICES Agents** must know and follow all ICES **Policies** and **Procedures**, , in particular those applicable to their role at ICES and ICES' *Code of Conduct Policy*.

#### 4.8 **ICES acting as a Third Party Service Provider**

4.8.1 From time to time, ICES may act as a **TPSP** for an external third party. In such circumstances, ICES must enter into a contract with the third party, setting out each party's respective roles, obligations, and authorities, in a manner that is consistent with legal and regulatory requirements. Decision making about such activities should be conducted in advance and may require a **Privacy Impact Assessment ("PIA")** to be conducted, and **Policies** and **Procedures** to be enabled in advance of the commencement of such a relationship of servitude by ICES.



# Third Party Service Provider Policy

## 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 *Privacy and Security Audit Policy*
- 5.4 *Discipline and Corrective Action in Relation to ICES Data Policy*
- 5.5 *Termination or Cessation of Employment or Contractual Relationship in Relation to ICES Data Policy*
- 5.6 *Privacy and Security Incident Breach Management Policy*
- 5.7 *Code of Conduct Policy*
- 5.8 *Conflict of Interest Policy*
- 5.9 *ICES Agent Policy*
- 5.10 *Contract Review Procedure*
- 5.11 *Secure Transfer of PHI/PI Procedure*
- 5.12 *Privacy and Security Training and Awareness Policy*
- 5.13 *Contract 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 ICES **PLO/Cybersecurity** site on the **ICES Intranet**.
- 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**.



## Third Party Service Provider Policy

- 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*.