Privacy Impact Assessment Policy

Department	Reference Number	Organizational Scope	ICES Site	IPC Scope
PLO	011-00-00	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)
June 2014	2025-07-31	Triennial	Juy 2026	PO.011
Authority (Title)	Chief Privacy and Legal Officer			
Policy Owner (Title)	Director, Privacy and Legal Office			
Required Reviewers (Titles)				

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 Policy identifies the circumstances in which Privacy Impact Assessments ("PIA") must be conducted by ICES.

2.0 SCOPE

2.1 This Policy applies to every ICES Agent.

3.0 ROLES AND RESPONSIBILITIES

3.1 Chief Privacy and Legal Officer ("CPLO")

3.1.1 Accountable for the design of PIAs, and related processes, and ensuring that ICES Agents comply with this Policy and its Procedures.

3.1.2 Ensure that any PIA Policies, Procedures, and Practices have regard to guidelines created by the IPC relating to PIAs, including the *Privacy Impact Assessment Guidelines for the Ontario Personal Health Information Protection Act* and *Planning for Success: Privacy Impact Assessment Guide*.

3.2 Director, Privacy and Legal Office ("PLO")

3.2.1 Delegated by the CPLO to have day-to-day responsibility for the oversight of the privacy program;

3.2.2 Responsible for overseeing the Procedures in support of conducting PIAs, the logging of PIAs, ensuring that conditions, restrictions, findings, , recommendations, and Risks identified in PIAs are documented and logged appropriately in accordance with the Consolidated Log Policy and in the appropriate Department Risk Registers ("DRR") or Enterprise Risk Register ("ERR") as set out in the Risk Management Policy.

3.3 Manager, Privacy

3.3.1 Responsible for ensuring that all PIAs are conducted in accordance with ICES' lawful authority to collect, use, and disclose Personal Health Information ("PHI") and/or Personal Information ("PI"), and may delegate this responsibility to appropriate team members but retains overall accountability.

3.4 Privacy Subject Matter Experts ("SME")

3.4.1 The CPLO has delegated day-to-day responsibility for the conduct and execution of PIAs to the Privacy SMEs in the PLO or Research & Analysis department, as applicable, and this is communicated on PLO page of the ICES Intranet.

4.0 DETAILS

4.1 General Principles

4.1.1 A PIA is a risk management tool and ICES conducts PIAs to:

(a) Verify any collection, use, or disclosure of PHI/PI by ICES Agents is in accordance with any applicable laws, and related requirements set by the IPC in the PHIPA Manual, *Coroners Act* Addendum, and the CYFSA Addendum;

(b) Identify the impacts of all collections, uses, and disclosures of PHI/PI on individuals' privacy;

(c) Confirm the purpose for the collection, use, or disclosure of PHI/PI aligns with ICES' Corporate Objects;

(d) Assess if other information, including De-Identified Data, will serve the identified purpose; and

(e) Assess if no more PHI/PI will be collected, used, or disclosed than is reasonably necessary for the identified purpose.

4.1.2 A PIA must be completed in the following circumstances:

(a) A proposed new collection of PHI/PI;

(b) An existing or proposed ICES Data Holding containing PHI/PI;

(c) Any new use of PHI/PI, whether for an ICES Project or as part of another activity or tool;

(d) Introducing or changing a business process, information system, Technology Resource, or program that impacts existing and future collections, uses, retention, disclosures, and/or destructions of PHI/PI;

(e) Disclosing PHI/PI to another organization or a Third Party Researcher; or

(f) Establishing or changing a Third Party Service Provider ("TPSP") relationship that involves PHI/PI.

4.1.3 ICES must have a PIA for all existing ICES Data Holdings containing PHI/PI at ICES. If there is no PIA for an existing ICES Data Holding containing PHI/PI, the CPLO, or their delegate, is responsible for developing a timetable to ensure a PIA is completed.

4.1.4 ICES Data Holdings containing PHI/PI will be reviewed by the CPLO, or their delegate, on a triennial basis to confirm a PIA exists for each data holding.

4.1.5 If ICES must collect, use, or disclose De-Identified Data and/or Non-PHI/PI, the Manager, Privacy will determine whether a PIA or another vehicle must be utilized and any associated documentation thereof.

4.1.6 No change that requires a PIA may be implemented until all Risks identified have been eliminated, accepted, or have a satisfactory mitigation plan in place by the applicable Risk Owner, as set out in the Risk Management Policy.

4.1.7 A Data Sharing Agreement ("DSA") cannot be executed until a PIA has been completed by an Privacy SME.

4.2 PIA requests

4.2.1 ICES Agents are responsible for requesting a PIA be conducted in the following circumstances:

(a) At the conceptual design stage of planned activity (with respect to proposed new ICES Data Holdings involving PHI/PI and the introduction of new or changes to existing business processes, information systems, Technology Resources, or programs involving PHI/PI) and that they be reviewed and revised, if necessary, during the detailed design and implementation stages;

(b) Before any new collection of PHI/PI;

(c) Before any new use of PHI/PI from existing ICES Data Holdings;

(d) Before any disclosure of PHI/PI to another person/organization or to a Third Party Researcher; or

(e) Before any new use of PHI/PI by a TPSP.

4.2.2 ICES Agents must contact Privacy Services to request a PIA before proceeding with any changes to PHI/PI.

4.2.3 The CPLO may direct that a PIA be conducted if a PIA does not exist, but is required.

4.3 Determinations that a PIA is not required

4.3.1 The Privacy SME who receives the request to conduct a PIA must assess the request and determine if a PIA required.

4.3.2 A PIA is not required if the planned activities outlined in the request do not fall within the circumstances identified in section 4.1.2 above.

(a) With respect to activities concerning business processes, information systems,Technology Resources, or programs, a PIA may not be required where:

(i) no change to existing PHI/PI handling practices is being proposed; or

(ii) the existing PHI/PI handling practices have been subjected to a PIA previously.

4.3.3 When the Privacy SME determines that a PIA is not required, they must communicate this determination to the requestor in writing and include reasons for the determination, including the criteria that were used.

4.3.4 The Privacy SME must document in the applicable log:

(a) the determination that a PIA was not required;

(b) the reasons for the determination; and

(c) the date on which the determination was made.

4.4 Content of PIA

4.4.1 ICES permits two PIA templates: one for reviewing lawful authorities in support of ICES Projects ("Project PIA") and another template for all other PIAs conducted.

4.4.2 At a minimum, both PIAs must describe:

(a) the ICES Data Holding, business process information system, Technology Resource, or program at issue;

(b) the source(s) of the PHI/PI;

(c) the purpose and rationale (reason) for the collection, use, or disclosure or proposed collection, use, or disclosure of PHI/PI, including why de-identified or aggregate information will not serve the identified purpose;

(d) the flow of PHI/PI;

(e) the legal authority for each collection, use, and disclosure of PHI/PI;

(f) the limitations (if any) imposed on collection, use, and disclosure;

(g) the Record Linkages (if any), including whether or not PHI/PI will be linked to other information;

(h) whether or not the PHI/PI will be de-identified and/or aggregated and the specific purposes for which, and the circumstances in which, the de-identified and/or aggregate information will be re-identified, if any, and the conditions or restrictions imposed;the applicable retention periods for the PHI/PI;

(i) the secure manner in which the PHI/PI will be retained, transferred, and disposed of;

(j) the administrative, technical, and physical safeguards implemented or proposed to be implemented to protect PHI/PI, including functionality for logging access, use, modification, and disclosure of PHI/PI and functionality for auditing to detect unauthorized use or disclosure;

(k) the risks to the privacy of individuals whose PHI/PI is or will be part of the data holding, information system, technology, or program, and an assessment of the risks and mitigation strategies; and

(l) the recommendations arising from PIAs to address and eliminate or reduce the privacy risks identified, and associated responsibilities of ICES Agents, including compliance oversight and timelines.

4.5 Review and analysis of PIAs

4.5.1 A PIA must capture whether the collection, use, or disclosure of PHI/PI is for Research purposes or whether the use of PHI/PI is for Statistical Analysis (also called Analytics). In determining whether to consider whether the collection, use, or disclosure of PHI/PI is for Research purposes or for Statistical Analysis, the Privacy SME may have regard to:

(a) Whether the purpose is legitimately Research or Statistical Analysis; and

(b) Whether the legislative vehicle relied on for disclosing PHI/PI to ICES does not contemplate Statistical Analysis and ICES must rely solely on its Research authority as set out in its Corporate Objects for the collection and use.

4.5.2 Procedures for conducting Project PIAs are set out in the Privacy Impact Assessment Review and Analysis for ICES Projects Procedure.

4.5.3 Procedures for conducting all other PIAs are set out in the Privacy Impact Assessment Review and Analysis Procedure.

4.5.4 Where a Privacy SME finds no lawful authority for the collection, use, or disclosure of PHI/PI for Research or for Statistical Analysis, the finding of this review must be communicated to the requester as soon as practicable and any Risks escalated as necessary pursuant the Risk Management Policy.

4.5.5 Any PIA conducted on a proposed new collection of PHI/PI and any PIA whose assessment is considered to be of a high level of complexity by the Privacy SME must be reviewed by the Director, PLO prior to finalization of the assessment.

4.6 Review and analysis of PIAs: Research purposes

4.6.1 Prior to any finalization of a review or analysis for the collection, use, or disclosure of PHI/PI for Research purposes, the ICES Privacy SME must:

(a) Review the written research plan to ensure it complies with the requirements of any statute and its regulations;

(b) Ensure that the written research plan was approved by a Research Ethics Board "REB");

(c) Ensure that a copy of the REB approval of the written research plan is included in the PIA documentation;

(d) Ensure that the PHI/PI being requested is consistent with the PHI/PI identified in the written research plan approved by the REB;

(e) Ensure that other information, namely De-Identified Data, will not serve the Research purpose and no more PHI/PI is being requested than is reasonably necessary to meet the Research purpose; and

(f) Ensure that the ICES Agent(s) requesting collection, use, or disclosure of PHI/PI for Research purposes has acknowledged and signed off that they will comply with:

(i) s. 44(6)(a) to (f) of PHIPA, for PHI collected by ICES as a Prescribed Entity under PHIPA;
(ii) s. 5 of Ontario Reg. 523/18 to the *Coroners Act* for PI collected by ICES as a Prescribed Entity under the *Coroners Act*; or
(iii) Ontario Reg. 191/18 of CYFSA, for PI collected by ICES as a Prescribed Entity under the CYFSA.

4.7 Addressing conditions, restrictions, , and recommendations

4.7.1 When there are recommendations that are unaddressed at the time the PIA is concluded, the outstanding recommendations are handled in accordance with:

(a) The Privacy Impact Assessment Review and Analysis for ICES Projects Procedure for PIAs for ICES Projects; and

(b) The Privacy Impact Assessment Review and Analysis Procedure for all other types of PIAs.

4.7.2 If any conditions, restrictions, findings, , or recommendations are identified in the PIA, such information must be captured in the Consolidated Log as set out in the Consolidated Log Policy.

4.7.3 If any further documentation must be completed, provided, or executed with respect to the collection, use, or disclosure of PHI/PI identified in a PIA, such documentation must be included in the Consolidated Log .

4.7.4 If any further documentation must be completed, provided, or executed with respect to an existing business process, information system, Technology Resource, or program involving PHI/PI, such documentation must be included in the Consolidated Log .

4.8 Secure retention, return, and disposal of PHI/PI and PIAs

4.8.1 Any PHI/PI collected and used by ICES must be retained only for the period set out in the applicable PIA, DSA, and written research plan approved by the REB, in compliance with the ICES Data Retention Schedule Standard.

4.8.2 Any PHI/PI that must be securely returned to the Data Provider must be in accordance with the time frame and in the manner identified in the applicable PIA, DSA, and written research plan approved by the REB.

4.8.3 Any PHI/PI that must be disposed of in a secure manner must be completed in the time frame and manner set out in the applicable PIA, DSA, and written research plan approved by the REB, in compliance with the Destruction of ICES Data Procedure.

4.9 Log of PIAs

4.9.1 All required metrics in relation to PIAs must be logged, including when:

(a) PIAs are completed;

(b) PIAs are initiated but have not been completed; and

(c) There is a determination that a PIA is not required.

4.9.2 PIAs must be logged in the log applicable to the planned activities:

(a) ICES Project PIA Log for ICES Projects;

(b) TPR Project PIA Log for Third Party Research Projects; or

(c) ICES PIA Log for all other activities;

4.9.3 The Director, PLO, Privacy is responsible for maintaining the PIA logs listed in s. 4.9.2 above.

4.9.4 The log must include whether the purpose of the planned activities is for Research or Statistical Analysis.

4.9.5 If any PIAs are initiated but not completed, that information must be captured in the applicable log.

4.9.6 If the Manager, Privacy or Privacy SME decides that a PIA is not required, that information must be captured in the applicable log, as applicable.

4.9.7 The Manager, Privacy is responsible for ensuring that all reviews and analyses with respect to PIAs are communicated to the initial requester in a timely manner from the date of the initial request to the Privacy SME as set out in ICES' PIA Procedures.

4.10 Ongoing compliance, monitoring, and auditing

4.10.1 Once a PIA has been completed, it should be reviewed on an ongoing basis in order to ensure that it continues to be accurate and continues to be consistent with ICES' information practices as set out in the Privacy and Security Audit Policy.

4.10.2 The Director, PLO is responsible for ensuring that PIAs are reviewed in accordance with the Privacy and Security Audit Policy.

4.10.3 The following criteria must be assessed by the Director, PLO as part of the compliance monitoring activity in the frequency set out in the Privacy and Security Audit Policy and Annual Audit Schedule:

(a) Whether PIAs have been conducted for all new collections, uses, or disclosures of PHI/PI;

(b) Whether PIAs have been conducted for all new business process, information system, Technology Resource, or program involving PHI/PI;

(c) Whether PIAs have been conducted with respect to all TPSPs accessing PHI/PI;

(d) Whether PIAs are out of date and need to be amended/updated; and

(e) Whether the details set out in PIAs match with the details set out in DSAs.

4.10.4 In addition to the above activities in section 4.10 as part of Compliance Audit activities, reviews of existing PIAs will also occur in the following manner:

(a) PIAs for ICES Projects must be reviewed on an ongoing basis throughout the course of the ICES Project by the Project Team to ensure that the PIA continues to be accurate.

(b) For all other PIAs that are not ICES Projects, if a PIA was not amended within the past year, the PIA will be reviewed by the department team that requested the PIA to confirm the PIA reflects current practices/processes for the applicable ICES Data Holding containing PHI/PI.

5.0 RELATED DOCUMENTATION

5.1 Policies

5.2 Standards

5.3 Procedures

5.4 Tools

5.4.1 ICES Project PIA Form

5.4.2 ICES General PIA Form

5.4.3 ICES Project PIA Log

5.4.4 ICES PIA Log

5.4.5 TPR Project PIA Log

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**