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	2025-10-31	Triennial	October 2028	2025-07-31
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 a **Privacy Impact Assessment ("PIA")** must be conducted by ICES.

1.2 A PIA is a risk management tool used by ICES to:

1.2.1 Verify any collection, use, or disclosure of **Identifiable Information** by **ICES Agents** is in accordance with:

(a) Applicable laws, including but not limited to:

(i) *Personal Health Information Protection Act* ("**PHIPA**")

(ii) Coroners Act

(iii) Child, Youth and Family Services Act ("**CYFSA**")

(b) Applicable compliance requirements set out in the **IPC Manual**, **Coroners Addendum**, and **CYFSA Addendum**.

1.2.2 Identify the impacts of all collections, uses, and disclosures of Identifiable Information on individuals' privacy;

1.2.3 Confirm the purpose for the collection, use, or disclosure of Identifiable Information aligns with ICES' **Corporate Objects**;

1.2.4 Assess if **Data Minimization** principles are being applied.

2.0 SCOPE

2.1 This policy applies to all ICES Agents who:

2.1.1 Conduct PIAs;

2.1.2 Carrying out activities that require a PIA to be conducted

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 ICES Agents comply with this policy and its procedure.

3.1.2 Ensures that any ICES' policies, standards, and procedures regarding PIAs should be developed with consideration of the following IPC publications:

(a) *Privacy Impact Assessment Guidelines for the Ontario Personal Health Information Protection Act*

(b) *Planning for Success: Privacy Impact Assessment Guide*

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

3.2.1 Delegated day-to-day responsibility from the CPLO for the oversight of the Privacy program

3.3 Manager, Privacy Services / Managing Privacy Counsel

3.3.1 Ensures all PIAs are conducted in accordance with ICES' lawful authority to collect, use, disclose, and otherwise process Identifiable Information.

3.3.2 May delegate the responsibility to appropriate Privacy **Subject Matter Experts ("SMEs")** but retains overall accountability.

3.4 Privacy SMEs

3.4.1 Delegated day-to-day responsibility from the CPLO to conduct PIAs

3.4.2 Privacy SMEs include ICES Agents in the PLO department, Research & Analysis ("**R&A**") department, and at **ICES Sites**.

4.0 DETAILS

4.1 Circumstances requiring a PIA

4.1.1 A PIA must be conducted in the following circumstances:

(a) A new collection of Identifiable Information;

(b) The proposed creation of a new **ICES Data Holding** containing Identifiable Information

(i) A new ICES Data Holding may be created through a new collection of Identifiable Information and/or through creation of an **ICES Derived Data Holding** using Identifiable Information already collected by ICES.

(c) New use of Identifiable Information for an **ICES Project**;

(d) New uses of Identifiable Information as part of another activity or tool, including amendments to an ICES Data Holding's **Statement of Purpose ("SOP")** to reflect new uses.

(e) Introducing or changing a business process, information system, Technology Resource, or program that impacts existing and future collections, uses, disclosures, and/or other **Processing** of Identifiable Information;

(f) Disclosing Identifiable Information for the purpose of a **Third Party Research Project ("TPR Project")** or for other non-research purposes; or

(g) Establishing or changing a **Third Party Service Provider ("TPSP")** relationship that involves processing Identifiable Information.

4.1.2 Existing ICES Data Holdings containing Identifiable Information

(a) ICES must have a PIA completed for all ICES Data Holdings (including ICES Derived Data Holdings) containing Identifiable Information.

(b) ICES Data Holdings containing Identifiable Information must be reviewed on a triennial basis to confirm a PIA exists for each one.

(c) If there is no PIA completed for an existing ICES Data Holding then the Director, PLO must develop a timetable to ensure a PIA is completed for these data holdings.

4.1.3 De-Identified Information and Non-Identifiable Data

(a) A PIA is not necessarily required prior to ICES collecting, using, or disclosing De-Identified Information and/or Non-Identifiable Data, however the Manager, Privacy Services / Managing Privacy Counsel may determine that a PIA should be completed in such circumstances.

4.1.4 Agreements regarding Identifiable Information

(a) A **Data Sharing Agreement ("DSA")**, or any other legal agreement regarding the collection, disclosure, or transfer of Identifiable Information, cannot be executed by ICES until a PIA is completed.

4.1.5 Risks

(a) No planned activities requiring a PIA may be implemented until all risks identified when conducting a PIA are either resolved or documented and managed through the ERM program in accordance with the *Risk Management Policy*.

4.2 Timing of conducting and reviewing a PIA

4.2.1 ICES Agents must request a PIA be conducted prior to implementing and carrying out the planned activity. This includes requesting a PIA:

(a) At the conceptual design stage when planning the activity;

(i) If the plans have changed during the detailed design and implementation stages then the PIA must be amended to reviewed and revised, as needed.

(b) Prior to any new collection of Identifiable Information;

(c) Prior to any new use of an existing ICES Data Holding containing Identifiable Information, including creation of an ICES Derived Data Holding or use in an ICES Project. These activities also include new **Record Linkages** and/or **Data Linking**.

(d) Prior to disclosure of Identifiable Information for the purpose of a TPR Project or for non-research purposes;

(e) Prior to any new use of Identifiable Information by a TPSP.

4.2.2 The CPLO may direct that a PIA be conducted in circumstances where a PIA is required but does not exist.

4.3 Circumstances not requiring a PIA

4.3.1 A PIA is not required if the planned activities identified in a request do not fall within the circumstances identified in section 4.1 above.

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

(a) There is no change being proposed to the existing handling practices used for the Identifiable Information; or

(b) The existing handling practices used for the Identifiable Information has already been subject to a PIA.

4.4 Determinations not to complete a required PIA

4.4.1 A determination may be made to not complete a PIA even if the planned activities fall within the circumstances identified in section 4.1 above.

4.4.2 A determination to not complete a PIA can only be made by:

(a) Manager, Privacy Services / Managing Privacy Counsel;

(b) Director, PLO; or

(c) CPLO

4.4.3 Determinations not to complete a PIA should only be made in limited circumstances and only when there is minimal risk involved with the contemplated activities.

(a) The risk must be assessed in accordance with the *Risk Management Policy.*

(b) If a PIA is not completed, the matter must be documented and managed through ICES' Enterprise Risk Management ("ERM") program in accordance with the *Risk Management Policy*.

4.4.4 Determinations must be confirmed in writing (typically email) by the decision maker, including the rationale for the determination. The document must be saved with other documentation related to the PIA.

4.4.5 Determinations not to complete a PIA must also be logged in accordance with section 4.9 below.

4.5 Required content of a PIA

4.5.1 The CPLO approves the electronic form(s) used for conducting PIAs. At minimum, a PIA must include the information set out in Appendix A.

4.6 Conducting a PIA

4.6.1 The process for conducting a PIA is set out in the *Privacy Impact Assessment Review and Analysis Procedure*.

4.6.2 Secondary review of draft PIAs

(a) The Director, PLO or Manager, Privacy Services / Managing Privacy Counsel must conduct secondary review of a draft PIA prior to finalization of the Privacy SME's assessment when it is one of the following activities:

(i) Proposed new collections of Identifiable Information for an ICES Data Holding; and

(ii) Any PIA that has been identified as having a higher level of complexity.

(b) The PIA is reviewed for accuracy and completeness.

(c) Even if a change is made to the PIA as a result of the secondary review, the Privacy SME remains responsible for the review and assessment within the PIA.

4.7 Assessment considerations

4.7.1 General assessment considerations

(a) When conducting a PIA, the Privacy SME considers the following:

(i) The purpose of the planned activity;

(ii) Whether the Identifiable Information involved in the planned activity is necessary to achieve the purpose. Assessments must ensure:

(A) Other information, namely De-Identified Information, will not serve the purpose; and

(B) No more Identifiable Information is being requested, including being collected and retained, than is reasonably necessary to meet the purpose.

(iii) Whether ICES has authority to collect, use, disclose, and/or otherwise process the Identifiable Information in relation to the planned activity based on any conditions and restrictions that apply to it as set out in:

(A) Applicable legislation;

(B) Legal agreements between ICES and the **Data Provider**;

(C) **Research Ethic Board ("REB")** approvals; and/or

(D) Any other applicable standards, guidelines, or materials, such as those issued by the Information and Privacy Commissioner of Ontario ("**IPC**").

(iv) Whether collection, use, disclosure, and/or other processing of Identifiable Information requires processing that is not in accordance with ICES' existing policies, standards, and procedures.

(v) Whether there are other privacy implications associated with the planned activity.

4.7.2 Statistical Analysis (Analytics) or Research purposes

(a) A PIA must capture whether the proposed collection, use, or disclosure of Identifiable Information is for **Research** purposes or **Statistical Analysis (Analytics)**.

(b) A Privacy SME conducting the PIA must have regard to:

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

(ii) Whether the legislative authority relied on by ICES to collect the Identifiable Information contemplates Statistical Analysis (Analytics).

(c) If the relied upon legislative authority does not contemplate Statistical Analysis (Analytics) then ICES must solely rely on its Research authority as set out in ICES' **Corporate Objects** in order to collect and use the Identifiable Information.

4.7.3 Research purposes

(a) Where the collection, use, or disclosure of Identifiable Information is for Research purposes, the Privacy SME conducting the PIA must also complete the following reviews:

(i) Review the written research plan to ensure it complies with the requirement of any applicable statute and its regulation(s);

(ii) Ensure the written research plan is approved by a REB**;**

(iii) Ensure a copy of the REB approval of the written research plan is included with the PIA documentation; and

(iv) Ensure that the Identifiable Information being requested is consistent with the Identifiable Information described in the written research plan that was approved by the REB.

(v) Ensure that the ICES Agent(s) requesting collection, use, or disclosure of PHI/PI for Research purposes have attested they will comply with the additional obligations set out in the *Use of ICES Data Policy*;

(vi) If the Research relies on **Personal Information ("PI")** collected by ICES under the *Coroners Act*, and the lawful authority being relied upon for the Research is section 4 of Ontario Regulation 523/18 to the *Coroners Act*, ensure:

(A) The Chief Coroner consents to the use of PI for the Research;

(B) The purpose of the Research is related to the health or safety of the public or any segment of the public; and

(C) The requirements set out in section 3 of Ontario Regulation 523/18 are met.

(vii) If the Research is an ICES Project that relies on PI collected by ICES under the *CYFSA*, ensure there is written confirmation from each member of the approving REB that their personal interest in the use of the PI or the performance of the research does not conflict or appear to conflict with the member's ability to objectively review the research plan as set out in section 4 of Ontario Regulation 191/18 to the *CYFSA*.

4.7.4 Collaborating Researchers

(a) In accordance with the *Disclosure of ICES Data Policy*, ensure that individuals identified on the PIA as Collaborating Researchers have executed a "Collaborating Researcher Non-Disclosure Agreement" for ICES.

4.8 Amendments

4.8.1 When amendments are requested to an existing PIA, the existing PIA (or PIAs) must be reviewed by the Privacy SME in order to:

(a) Assess the proposed change in the amendment request with an understanding of the activities already permitted in the existing PIA; and

(b) Ensure the activities permitted in the existing PIA continues to be consistent with ICES' policies, standards, and procedures.

4.9 Logging PIAs

4.9.1 PIAs must be logged and tracked. One or more logs may be used, and, at minimum, the log(s) must include the required content set out in Appendix B.

4.9.2 The Director, PLO is responsible for ensuring the completed log(s) comply with this policy.

4.9.3 The log(s) are updated and maintained in accordance with the *Privacy Impact Assessment Review and Analysis Procedure*.

4.10 Ongoing reviews of PIAs

4.10.1 Completed PIAs must be reviewed on an ongoing basis to ensure:

(a) The PIA continues to accurately reflect the activities contemplated in the PIA; and

(b) The PIA continues to be consistent with ICES' policies, standards, and procedures.

4.10.2 The Director, PLO is responsible for ensuring that PIAs are reviewed on an ongoing basis.

4.10.3 PIAs for ICES Project must be reviewed by the **Project Team** throughout the course of the ICES Project.

4.10.4 For all other types of PIAs, the PIA must be reviewed annually by the initial **Requestor**, or a suitable delegate familiar with the activities contemplated in the PIA.

4.10.5 Project Teams / Requestors and Privacy SMEs must review an existing PIA for the above considerations whenever an amendment to the PIA is requested. This amendment process may be considered the required review for the purpose of this section of the policy.

5.0 RELATED DOCUMENTATION

5.1 Policies

5.1.1 Disclosure of ICES Data Policy

5.1.2 *Risk Management Policy*

5.1.3 *Use of ICES Data Policy*

5.2 Standards

5.3 Procedures

5.3.1 *Privacy Impact Assessment Review and Analysis 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

Privacy Impact Assessment Policy

Change Date (YYYY-MM-DD)	Change Notes
2025-07-31	■ Reviewed for compliance with ICES' obligations as a Prescribed Entity: ○ IPC Manual: ▪ 01-25: Policy, Procedures, and Practices for Privacy Impact Assessments ▪ 01-26: Log of Privacy Impact Assessments ○ Coroners Addendum: ▪ 05-26: Policy, Procedures and Practices for Privacy Impact Assessments ▪ 05-27: Log of Privacy Impact Assessments ○ CYFSA Addendum: ▪ 06-26: Policy, Procedures and Practices for Privacy Impact Assessments ▪ 06-27: Log of Privacy Impact Assessments ■ Added content regarding ICES' role as a Prescribed Entity under *CYFSA* (not yet in effect) ■ Updated to reflect: ○ Revised document template and standardized language in Sections 6.0 to 9.0 ○ Revised glossary terms and titles of ICES policies, standards, and procedures
2025-10-31	Revised to reflect updated ICES Information classification terms General revisions to re-distribute content between this policy and the *Privacy Impact Assessment Review and Analysis Procedure*

Appendix A

Privacy Impact Assessments – Required Content	
At minimum, PIAs must describe the following information:	
	1. The ICES Data Holding (including ICES Derived Data Holding), business process. information system, Technology Resource, relevant program, ICES Project, or TPR Project
	2. The nature and type of Identifiable Information involved
	3. The source(s) of the Identifiable Information
	4. The purpose for which the Identifiable Information is proposed to be collected, used, disclosed, or otherwise processed
	5. The reason(s) that the Identifiable Information is required for the purpose
	6. The flow of the Identifiable Information
	7. The lawful authority for each collection, use, disclosure, and/or other processing of the Identifiable Information
	8. The limitations (if any) imposed on collection, use, disclosure, and/or other processing
	9. The anticipated Record Linkages and/or Data Linking of the Identifiable Information with other information, including documenting the lawful authority for linking the Identifiable Information
	10. Whether nor not the Identifiable Information will be de-identified and/or aggregated
	11. If the De-Identified Information will be re-identified, the specific purposes for which and the circumstances in which this re-identification will occur
	12. Any conditions or restrictions (if any) imposed on re-identification
	13. The applicable retention period of the Identifiable Information
	14. The secure manner in which the Identifiable Information will be retained, transferred, and disposed of
	15. The administrative, technical, and physical safeguards implemented or proposed to be implemented to protect Identifiable Information, including functionality for: • Logging access, use, modification, and disclosure of Identifiable Information; and • Auditing to detect unauthorized use or disclosure
	16. The Privacy SME's finding(s) arising from their assessment
	17. The risks to the privacy of individuals whose Identifiable Information is or will be part of the contemplated activities in the PIA, and an assessment of the risks
	18. Recommendations arising from the PIA to address and eliminate or reduce the privacy risks identified
PIAs for ICES Data Holdings (including ICES Derived Data Holdings) must also include the data holding's Statement of Purpose ("SOP"), including:	

	19. The purpose of the ICES Data Holding
	20. A description of the Identifiable Information contained in the ICES Data Holding
	21. The source(s) of the Identifiable Information
	22. An explanation for the need for the Identifiable Information in relation to the identified purpose of the ICES Data Holding
	23. An explanation why De-Identified Information would not service the identified purpose of the ICES Data Holding

Appendix B

Privacy Impact Assessments – Log Requirements	
At minimum, the log (or combined logs if more than one) of PIAs must include the following information:	
	For every PIA request
	1. The ICES Data Holding (including ICES Derived Data Holding), business process. information system, Technology Resource, relevant program, ICES Project, or TPR Project
	2. Which of ICES' Prescribed Entity designation(s) engaged (*PHIPA*, *Coroners Act*, and/or *CYFSA*)
	3. The Privacy SME assigned to conduct the PIA
	4. The date the PIA was requested
	When determined a PIA will not be completed
	5. The reason(s) for determining a PIA will not be completed
	6. The ICES Agent who made the determination
	7. The date the determination was made
	When a PIA is started but does not proceed (ie. withdrawn, not required)
	8. The date the PIA was confirmed by the Privacy SME as not proceeding
	9. The reason(s) the PIA is not proceeding
	When a PIA is completed
	10. The date the PIA was completed
	11. For ICES Projects, if the project's purpose is Statistical Analysis (Analytics) or Research
	12. The finding(s) arising from the PIA
	13. Risk(s), if any, associated with the finding(s)
	14. Recommendation(s), if any, associated with the finding(s) and/or risk(s)
	Addressing each recommendation arising from a completed PIA
	15. The ICES Agent(s) responsible for addressing the recommendation
	16. The estimated date that the recommendation is expected to be addressed
	17. The planned manner in which the recommendation is expected to be addressed
	18. The actual date that the recommendation is addressed
	19. The actual manner in which the recommendation is addressed