

Use of ICES Data Policy



Department	Reference Number	Organizational Scope	ICES Site	IPC Scope
PLO	014-00-00	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)
2022-09-30	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)	Senior Director, Research, Data and Financial Services			
	Director, Data Quality and Information Management			
	Director, Research and Analysis			
	Director, Data & Analytic Services			

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 sets out:

- 1.1.1 ICES' lawful authorities for use of **Identifiable Information** as **ICES Data**;
- 1.1.2 ICES Agent obligations when using ICES Data, including additional obligations when the use is for **Research**;
- 1.1.3 Categories of ICES Data available for use in the **ICES Data Repository**; and
- 1.1.4 Approval requirements and conditions for use of Identifiable Information, including additional requirements when the use is for Research.

1.2 ICES uses Identifiable Information only as permitted by ICES' **Corporate Objects** and as permitted by applicable law, including but not limited to:

- 1.2.1 *Personal Health Information Protection Act ("PHIPA")*;
- 1.2.2 *Coroners Act*; and
- 1.2.3 *Child, Youth and Family Services Act ("CYFSA")*.

1.3 Use of Identifiable Information includes but is not necessarily limited to:

- 1.3.1 Use in ICES Projects for **Statistical Analysis (Analytics)** or **Research**;
- 1.3.2 **ICES Agents** accessing the Identifiable Information; and
- 1.3.3 **Record Linkages** and **Data Linking**.

Use of ICES Data Policy

- 1.4 ICES Agents must only use ICES Data in accordance with ICES' policies, standards, and procedures.

2.0 SCOPE

- 2.1 This policy applies to all ICES Agents who use ICES Data or manage programs, departments, and **ICES Sites** where ICES Data is used.

- 2.2 References to Identifiable Information in this standard are only with regards to when the Identifiable Information is ICES Data, namely:

- 2.2.1 **Personal Health Information ("PHI");**

- 2.2.2 **Personal Information ("PI");** and

- 2.2.3 **Other Identifiable Data**

- 2.3 References to **De-Identified Information** in this standard are only with regards to when the De-Identified Information is ICES Data, namely:

- 2.3.1 **Non-Identifiable Data;**

- 2.3.2 **Aggregate Data (Summary Output);** and

- 2.3.3 **Publishable Data**

Further information regarding types of ICES Data is set out in the *Information Classification Standard*.

- 2.4 Additional requirements for use of ICES Data with regards to ICES Agent access are set out in the *Access to ICES Data Standard*.
- 2.5 Additional requirements for use of ICES Data with regards to Record Linkage and Data Linking are set out in the *Record Linkage and Data Linking Standard*.
- 2.6 Any viewing of Identifiable Information by an individual who is not an ICES Agent constitutes a disclosure of Identifiable Information by ICES, which is subject to the *Disclosure of ICES Data Policy*.
- 2.7 The specific procedures regarding the use of ICES Data depends on the type of ICES Data being used and the nature of the use.

3.0 ROLES AND RESPONSIBILITIES

- 3.1 Chief Privacy and Legal Officer ("**CPLO**")

- 3.1.1 Accountable for this policy to ensure all uses of ICES Data comply with applicable laws and any other legal requirements.

- 3.2 Senior Director, Research, Data and Financial Services

- 3.2.1 Ensures all uses of ICES Data comply with this policy.

- 3.3 Director, Data Quality and Information Management ("**DQIM**") / Director, Research and Analysis ("**R&A**") / Director, Data & Analytic Services ("**DAS**")

- 3.3.1 Ensure all standards and procedures relating to use of ICES Data comply with this policy.

Use of ICES Data Policy

4.0 DETAILS

4.1 Lawful authority to use of Identifiable Information

4.1.1 ICES as a Corporation

- (a) Any use of Identifiable Information must be in accordance with ICES' authority as a not-for-profit corporation and, specifically, as permitted by ICES' **Corporate Objects**.

4.1.2 PHIPA

- (a) As a **Prescribed Entity** under *PHIPA*, ICES may use PHI in the following circumstances:
 - (i) Statistical Analysis (Analytics)
 - (A) In accordance with s.45(1) of *PHIPA*, ICES may use of PHI for the purpose of analysis or compiling statistical information with respect to the management of, evaluation or monitoring of, the allocation of resources to or planning for all or part of the health system, including the delivery of services.
 - (ii) Research
 - (A) Pursuant to s.18(3) of Ontario Regulation 329/04 to *PHIPA*, and s.37(1)(j) of *PHIPA*, ICES may use PHI to conduct **Research**.

4.1.3 Coroners Act

- (a) As a Prescribed Entity under the *Coroners Act*, ICES may use PI in the following circumstances:
 - (i) Statistical Analysis (Analytics)
 - (A) In accordance with s.52.1(1) of the *Coroners Act*, ICES may use PI for the purpose of data analysis or the compilation of statistical information related to the health or safety of the public, or any segment of the public.
 - (ii) Research
 - (A) Pursuant to s.3 and s.4 of Ontario Regulation 523/18 to the *Coroners Act*, ICES may use PI to conduct Research.

4.1.4 CYFSA

- (a) As a Prescribed Entity under the *CYFSA*, ICES may use PI in the following circumstances:
 - (i) Statistical Analysis (Analytics)
 - (A) In accordance with s.293(1) of the *CYFSA*, ICES may use PI for the purpose of analysis or compiling statistical information with respect to the management of, evaluation or monitoring of services (as defined in the *CYFSA*), the allocation of resources to or planning for those services, including their delivery.
 - (ii) Research
 - (A) Pursuant to s.4 of Ontario Regulation 191/18 to the *CYFSA*, ICES may use PI to conduct Research.

Use of ICES Data Policy

4.1.5 Multi-purpose use of Identifiable Information as a Prescribed Entity

- (a) When using linked PHI/PI for Statistical Analysis (Analytics), the use of the PHI/PI must meet the purposes relevant to that specific PHI and PI. Therefore use of linked PHI/PI for Statistical Analysis (Analytics) requires two or more purposes to be met concurrently.
- (b) A **Privacy Impact Assessment (“PIA”)** regarding the planned activity assesses whether the above requirement is met.

4.1.6 Other applicable laws and legal agreements

- (a) ICES may use Other Identifiable Data if such use is permitted by:
 - (i) Any applicable laws governing the Other Identifiable Data; and
 - (ii) Any applicable legal agreements between ICES and the **Data Provider** that governs ICES’ permitted collection, use, and disclosure of the Other Identifiable Data.

4.1.7 Consent

- (a) As a not-for-profit, ICES may use Identifiable Information with consent of the individual to whom the Identifiable Information relates.
- (b) ICES’ use of the Identifiable Information must be consistent with the purposes that the individual consented to.

4.2 Lawful authority to use Non-Identifiable Data

4.2.1 ICES may use Non-Identifiable Data provided:

- (a) As a not-for-profit, if it is in accordance with any applicable laws, legal agreements, and/or associated terms and conditions; and
- (b) The use is in accordance with ICES’ authority as a not-for-profit corporation and, specifically, as permitted by ICES’ Corporate Objects.

4.3 Use of ICES Data by Third Party Service Providers

4.3.1 **Third Party Service Provider (“TPSP”)** use of ICES Data, including access to ICES Data, must be assessed and approved in accordance with the *Third Party Service Provider Policy*.

4.4 ICES Agent obligations and data minimization principles

4.4.1 ICES Agents must sign an **ICES Agent and Confidentiality Agreement (“ICES Agent CA”)** prior to use of ICES Data, in accordance with the *ICES Agent Policy*.

4.4.2 ICES Agents must only use ICES Data in accordance with:

- (a) ICES’ policies, standards, and procedures;
- (b) Applicable laws;
- (c) Legal agreements or other terms and conditions requirements, if applicable; and
- (d) **Research Ethics Board (“REB”)** approval, if applicable.

4.4.3 ICES adheres to **Data Minimization** principles when using Identifiable Information, including:

Use of ICES Data Policy

- (a) ICES Agents must not use Identifiable Information if other information, such as De-Identified Information, will serve the purpose; and
 - (b) ICES Agents must not use more Identifiable Information than is reasonably necessary to meet the purpose.
- 4.4.4 ICES Agents must only use Identifiable Information for the specified period set out in applicable PIAs and legal agreements. Use beyond the permitted period may be subject to amendment and/or extension approvals. ICES Agent access to Identifiable Information may be terminated in accordance with the *Access to ICES Data Standard* and applicable procedures.
- 4.4.5 ICES Agents must only use Identifiable Information if permitted in this policy and permitted for their role, in accordance with the *Access to ICES Data Standard*. If not permitted, then ICES Agents must only access and use De-Identified Information.
- 4.4.6 Except for limited circumstances of permitted re-identification set out in the *De-Identification and Aggregation Policy*, ICES Agents are prohibited from using De-Identified Information to identify an individual. This includes:
- (a) Attempting to decrypt information that is encrypted for the purpose of re-identification;
 - (b) Attempting to identify an individual based on unencrypted information; and
 - (c) Relying on prior knowledge in combination with De-Identified Information in order to re-identify an individual.
- 4.5 ICES Data Repository
- 4.5.1 Any use of ICES Data must be consistent with the purpose(s) for which the ICES Data was collected and in accordance with any applicable legal agreements governing the ICES Data.
- 4.5.2 ICES Data available for use is categorized based, in part, on conditions that a Data Provider may place on ICES when using the data:
- (a) **General Use Data (“GUD”)**
 - (i) An **ICES Data Holding** that is GUD may be used by ICES Agents in accordance with ICES’ policies, standards, and procedures. There are no additional specific and ongoing compliance obligations unique to the data.
 - (b) **Controlled Use Data (“CUD”)**
 - (i) An ICES Data Holding that is CUD may be used by ICES Agents subject to specific and ongoing compliance obligations as set out in the applicable legal agreement between ICES and the Data Provider. These obligations are in addition to any requirements set out in ICES’ policies, standards, and procedures that must be met.
 - (ii) Examples of ongoing compliance obligations are additional approval requirements prior to using the data or notifications to the Data Provider when the data is used.
 - (c) **Project-Specific Data (“PSD”)**
 - (i) ICES Data that is PSD was initially disclosed to ICES for a specific ICES Project or a series of related projects conducted by a **Principal Investigator**. Use of PSD by ICES Agents is only permitted if in accordance with:

Use of ICES Data Policy

- (A) The legal agreement between ICES and the Data Provider; and
 - (B) The PIA contemplating the use of PSD.
 - (ii) PSD may not be used to create an **ICES Derived Data Holding**.
- 4.5.3 Further information regarding GUD and CUD requirements for specific ICES Data Holdings, including ICES Derived Data Holdings, are set out on the Data Holdings Obligations (“**DHO**”) page of the **Data Dictionary** (available on the **ICES Intranet**)
- 4.5.4 Permitted disclosure of ICES Data is not informed or determined by whether the ICES Data is GUD, CUD, or PSD. Any disclosures of ICES Data must be in accordance with the *Disclosure of ICES Data Policy*.
- 4.6 Oversight of use of ICES Data
- 4.6.1 Uses of ICES Data in ICES Projects are managed through the designated research program, department, or ICES Site, and through the Project Team. They are responsible for:
- (a) Oversight of the ICES Project to ensure all applicable requirements set out in section 4.7 below are addressed prior to use; and
 - (b) Retaining relevant documentation about the ICES Project, including but not limited to:
 - (i) Review and approval requests;
 - (ii) Research ethics materials, if applicable; and
 - (iii) Copies of completed PIAs.
- 4.6.2 All other uses of ICES Data are managed by the **Requestor** and their department. They are responsible for:
- (a) Oversight of the planned activity to ensure all applicable requirements set out in this section 4.7 below are addressed prior to use; and
 - (b) Retaining relevant documentation about the planned activity, including but not limited to:
 - (i) Review and approval requests; and
 - (ii) Copies of completed PIAs.
- 4.6.3 In addition to the above, ICES Agents in Privacy Services and other impacted departments retain documentation related to their applicable processes for these activities. For instance, retention of PIAs.
- 4.7 Requirements for use of Identifiable Information
- 4.7.1 Use of Identifiable Information is subject to the following requirements being met prior to use:
- (a) For ICES Projects that are Research:
 - (i) Additional requirements for ICES Agents conducting Research, as set out below in section 4.8 below;
 - (ii) REB approval of a written research plan, if the use is for Research; and
 - (iii) For PI initially collected by ICES under the *Coroners Act*, consent from the Chief Coroner may be required;
 - (b) For all ICES Projects and other uses of Identifiable Information

Use of ICES Data Policy



- (i) Completion of a PIA; and
- (ii) Management of any identified risks.

4.8 Additional ICES Agent obligations when using PHI/PI for Research

- 4.8.1 ICES Agents may have additional obligations when using Identifiable Information for Research depending on the PHI/PI being used. The ICES Agent must agree to these obligations prior to use of the PHI/PI, and this consent is confirmed by ICES as part of the PIA process.
- 4.8.2 ICES Agents must retain PHI/PI in compliance with the written research plan, as approved by the REB, and in accordance with ICES' *Information Handling Standard*.
- 4.8.3 ICES Agents must comply with ICES' policies, standards, and procedures regarding return, destruction, and de-identification of PHI/PI used for Research, including but not limited to the *Information Handling Standard, De-Identification and Aggregation Policy*, and applicable procedures regarding use of ICES Data. :
- 4.8.4 If using PHI for Research, ICES Agents must comply with s.44(6)(a) to (f) of *PHIPA*, meaning:
 - (a) Comply with the conditions, if any, specified by the REB with respect to the written research plan;
 - (b) Use the PHI only for the purposes set out in the written research plan, as approved by the REB;
 - (c) Not publish PHI in a form that could reasonably enable a person to ascertain the identity of the individual;
 - (d) Not disclose the PHI except as required by law;
 - (e) Not make contact or attempt to make contact with the individual to whom the PHI belongs, either directly or indirectly, unless ICES first obtains the individual's consent to be contacted;
 - (f) Notify ICES immediately if becoming aware of non-compliance with the above requirements.
- 4.8.5 If using PI initially collected by ICES under the *Coroners Act*, ICES Agents must comply with s.52.1(6) of the *Coroners Act* and s.3(4), (5), and s4 of Ontario Regulation 523/18, meaning:
 - (a) Use of the PI in Research is related to the health or safety of the public, or any segment of the public.
 - (b) Comply with the conditions, if any, specified by the REB with respect to the written research plan;
 - (c) Use the PI only for the purposes set out in the written research plan, as approved by the REB;
 - (d) Must not directly or indirectly make contact, or directly or indirectly attempt to make contact, with individuals to whom the PI relates unless ICES confirms the Chief Coroner has obtained consent from the individual to be contacted.
 - (e) Notify ICES immediately if the ICES Agent becomes aware of non-compliance with the above requirements so that ICES can notify the Chief Coroner.

Use of ICES Data Policy



- 4.8.6 If using PI initially collected by ICES under the *CYFSA*, ICES Agents must comply with the following requirements:
- (a) Use PI only for the purposes set out in the written research plan, as approved by the REB;
 - (b) Not publish PI in a form that could reasonably enable a person to ascertain the identity of the individual;
 - (c) Not disclose the PI except as required by law;
 - (d) Not make contact, or attempt to make contact, directly or indirectly, with any individual to whom the PI belongs; and
 - (e) Notify ICES immediately if becoming aware of non-compliance with the above requirements.
- 4.9 Research ethics approval
- 4.9.1 The ICES Project must have a written research plan that was approved by an REB and complies with requirements of applicable law governing the Identifiable Information.
- 4.9.2 The approving REB must meet any membership requirements or other criteria set out for it in applicable law governing the Identifiable Information intended for use, including but not limited to *PHIPA*, *Coroners Act*, and the *CYFSA*.
- 4.9.3 REB approval is reviewed and confirmed by ICES as part of the PIA process and further requirements related to REB approval are set out in the *Privacy Impact Assessment Policy*.
- 4.10 Chief Coroner's consent for use of PI for Research
- 4.10.1 For PI that ICES initially collected under the *Coroners Act*, ICES requires the consent of the Chief Coroner for use of that PI in Research that is outside the scope of the purpose set out in s.52.1(1) of the *Coroners Act*.
- 4.10.2 The Chief Coroner must consent to the use for the specific ICES Project and the purpose must relate to the health or safety of the public or any segment of the public.
- 4.10.3 The consent from the Chief Coroner is reviewed and confirmed by ICES as part of the PIA process.
- 4.11 Privacy Impact Assessments
- 4.11.1 All uses of Identifiable Information must be assessed in a PIA in accordance with the *Privacy Impact Assessment Policy*.
- 4.11.2 The PIA determines if:
- (a) ICES has lawful authority to use the information by law and legal agreements;
 - (b) Any and all conditions or restrictions set out in applicable laws and their regulations have been satisfied; and
 - (c) The use is in accordance with ICES' policies, standards, and procedures.
- 4.12 Risk management



Use of ICES Data Policy

- 4.12.1 Any unaddressed conditions, restrictions, or unresolved risks identified in a PIA or another ICES process, such as a **Threat Risk Assessment (“TRA”)**, must be addressed through ICES’ Enterprise Risk Management (“ERM”) program and in accordance with the *Risk Management Policy*.
- 4.12.2 Decisions to move forward with a particular use of ICES Data must be made taking into consideration the *Risk Management Policy*.
- 4.13 Logging use of Identifiable Information for Research
 - 4.13.1 ICES maintains information regarding approved uses of Identifiable Information in ICES Projects for Research purposes. At minimum, the log includes the information set out in Appendix A.
 - 4.13.2 This information is logged as part of the PIA process and managed by Privacy Services in accordance with the *Privacy Impact Assessment Policy*.
- 4.14 Use of De-Identified Information for Research
 - 4.14.1 Use of De-Identified Information for Research only occurs at ICES when the De-Identified Information is created from de-identification of Identifiable Information also used for Research. As such, all requirements set out in ICES’ policies, standards, and procedures for use and de-identification of Identifiable Information must be met first.
- 4.15 Secure retention and destruction of ICES Data
 - 4.15.1 ICES Data is retained in accordance with the *ICES Data Retention Schedule Standard* and the *Destruction of ICES Data Procedure*.
 - 4.15.2 ICES Data is disposed of in accordance with the *Secure Disposal Standard* and the *Destruction of ICES Data Procedure*.

5.0 RELATED DOCUMENTATION

- 5.1 Policies
 - 5.1.1 *De-Identification and Aggregation Policy*
 - 5.1.2 *Disclosure of ICES Data Policy*
 - 5.1.3 *ICES Agent Policy*
 - 5.1.4 *Privacy Impact Assessment Policy*
 - 5.1.5 *Risk Management Policy*
 - 5.1.6 *Third Party Service Provider Policy*
- 5.2 Standards
 - 5.2.1 *Access to ICES Data Standard*
 - 5.2.2 *ICES Data Retention Schedule Standard*
 - 5.2.3 *Information Classification Standard*
 - 5.2.4 *Information Handling Standard*
 - 5.2.5 *Record Linkage and Data Linking Standard*



Use of ICES Data Policy

5.2.6 *Secure Disposal Standard*

5.3 Procedures

5.3.1 *Destruction of ICES Data Procedure*

5.3.2 *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 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:

Use of ICES Data Policy

- 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
2025-07-31	<ul style="list-style-type: none"> ■ Reviewed for compliance with ICES' obligations as a Prescribed Entity: <ul style="list-style-type: none"> ○ IPC Manual: <ul style="list-style-type: none"> ▪ 01-08: Policy, Procedures, and Practices for Limiting Agent Access to and Use of Personal Health Information ▪ 01-09: Log of Agents Granted Approval to Access and Use Personal Health Information ▪ 01-10: Policy, Procedures, and Practices for the Use of Personal Health Information for Research ▪ 01-11: Log of Approved Uses of Personal Health Information for Research ▪ 01-22: Policy, Procedures, and Practices for the Linkage of Records of Personal Health Information ○ Coroners Addendum: <ul style="list-style-type: none"> ▪ 05-09: Policy, Procedures and Practices for Limiting Agent Access to and Use of Personal information ▪ 05-10: Log of Agents Granted Approval to Access and Use Personal information ▪ 05-14: Policy, Procedures and Practices for the Use of Personal information for Research ▪ 05-15: Log of Approved Uses of Personal information for Research ▪ 05-23: Policy, Procedures and Practices for the Linkage of Records of Personal Information ■ Updated to reflect: <ul style="list-style-type: none"> ○ 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	<ul style="list-style-type: none"> ■ Substantially revised to re-distribute content previously in this policy to the <i>Access to ICES Data Standard</i> (previously titled the <i>Use of ICES Data Standard</i>) and the new <i>Record Linkage and Data Linking Standard</i>. Overall re-distribution to make content clearer to ICES Agents regarding use, access, and linkages. ■ Revised to incorporate CYFSA-related information ■ Revised to reflect the updated ICES Information classification terms

Use of ICES Data Policy



Appendix A

Use of Identifiable Information for Research – Log Requirements	
	At minimum, the log must include the following information regarding ICES' approved uses of Identifiable Information for Research:
1.	The name of the research study
2.	The ICES Agent(s) to whom the approval is granted
3.	The date REB approval was granted
4.	The date of PIA approval for the ICES Project, as date of approval for use of Identifiable Information for Research
5.	The ICES Data Holdings and, if applicable, Project-Specific Data used for the ICES Project
6.	The purpose of the research study
For ICES Projects using Personal Information collected by ICES under the <i>Coroners Act</i>	
7.	Confirmation that the purpose of the research study is related to the health or safety of the public or any segment of the public
8.	Whether the research study is using the Personal Information in accordance with s.52.1(1) of the <i>Coroners Act</i> or s.4 of its regulation
9.	For research conducted under s.4 of the regulation, the date the Chief Coroner approved the use of Personal Information for research
If the Identifiable Information is being used by the ICES Agent outside the secure ICES Data Environment	
10.	The date the Identifiable Information was provided to the ICES Agent
11.	The retention period of the Identifiable Information, as set out in the written research plan approved by the REB
12.	Whether the Identifiable Information will be securely returned to ICES, securely disposed of, or de-identified following the retention period.
13.	The date the Identifiable Information must be returned or destroyed
14.	The date the Identifiable Information is returned or a certificate of destruction is received