Use of ICES Data Policy

Department	Reference Number	Organizational Scope	ICES Site	IPC Scope
R&A	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)
September 2022	N/A	Triennial	September 2025	PO.014-NPR.01

Authority (Title)	Chief Privacy and Legal Officer
Policy Owner (Title)	Director, Privacy and Legal Office
Required Reviewers (Titles)	Senior Director, Researcy, Data & Financial Services
	Director, Data & Analytics Services
	Director, Data Quality & Information Management
	Director, Research & Analysis

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

1.0 PURPOSE

1.1 The purpose of this Policy is to:

1.1.1 Define the rules for the use of ICES Data by ICES Agents to ensure consistency with the mandate of ICES, in accordance with applicable laws and other legal requirements in respect of:

(a) Limiting use of Personal Health Information (“PHI”) and Personal Information (“PI”) based on the “need to know” principle to ensure ICES Agents use both the least identifiable information possible and the minimum amount of identifiable information necessary for carrying out their day-to-day employment, contractual or other responsibilities;

(b) Linking ICES Data; and

(c) Use of ICES Data for Research.

2.0 SCOPE

2.1 This Policy applies to all ICES Agents who use ICES Data.

3.0 ROLES AND RESPONSIBILITIES

3.1 ICES Chief Privacy and Legal Officer (“CPLO”) is accountable for this Policy to ensure that all uses of ICES Data are in compliance with applicable laws and any other legal requirements.

3.2 ICES Senior Director for the platform of Research and Data is responsible for ensuring that all uses of ICES Data are in compliance with this Policy and as set out in ICES’ Use of ICES Data Standard and any associated Procedures.

3.3 ICES Directors for the platforms of Research & Analysis ("R&A"), Data Quality and Information Management ("DQIM"), and Data & Analytic Services ("DAS") are responsible for ensuring that all Procedures and Practices relating to the uses of ICES Data are in compliance with this Policy and ICES' Use of ICES Data Standard.

4.0 DETAILS

4.1 Forms of ICES Data

4.1.1 To facilitate Data Minimization and reflect gradients of identifiability, PHI/PI consists of the following subsets:

(a) Fully Identifiable Data;

(b) Coded Data; and

(c) Risk Reduced Coded Data ("RRCD").

4.1.2 Fully Identifiable Data, Coded Data, and RRCD must be treated as PHI/PI for the purposes of ICES' Policies, Procedures, and Practices.

4.1.3 The specific Procedures relating to the use of ICES Data will depend on the type of ICES Data being used in the circumstances.

4.2 General Principles

4.2.1 Use of PHI/PI by ICES is authorized to ICES Agents only. Any viewing of PHI/PI by an individual who is not an ICES Agent constitutes a disclosure of PHI/PI by ICES, which requires a corresponding authority to disclose the PH/PI.

4.2.2 ICES Agents must use ICES Data only in accordance with ICES' Policies, Procedures, and Practices, applicable laws and other legal requirements, including, where applicable, Research Ethics Board ("REB") approval and contractual arrangements.

4.2.3 ICES Agents may only use PHI/PI if De-identified Data will not serve the identified purposes, and the use of PHI/PI must be limited to that which is reasonably necessary to meet the identified purposes.

4.2.4 ICES Agents must sign an ICES Agent and Confidentiality Agreement ("ICES Agent CA") before using PHI/PI.

4.2.5 The ICES Agent CA as set out in the ICES Agent Policy, requires that ICES Agents:

(a) Adhere to Policies, Procedures, and Practices,

(b) Be informed about consequences of breach of contract; and

(c) Use, including access, ICES Data only in order to perform their employment, contractual or other responsibilities on behalf of ICES, based on the "need to know" principle.

4.2.6 ICES Agents shall not use ICES Data, either alone or in combination with other information, including any unencrypted information or an ICES Agent's prior knowledge of an individual, to identify an individual, except whereas permitted under applicable laws.

4.2.7 ICES Agents, other than Data Covenantors in the course of their duties, are prohibited from attempting to decrypt PHI/PI provided in an encrypted form.

4.2.8 ICES must conduct audits in accordance with its privacy and security audit program to demonstrate compliance with its Practices as a Prescribed Entity.

4.2.9 Practices with respect to use of ICES Data must be audited as set out in ICES' Privacy and Security Audit Policy and associated Procedures.

4.2.10 The specific mechanisms and details implemented by ICES with respect to following activities are set out in the *Use of ICES Data Standard:*

(a) Limiting ICES Agent use of PHI/PI;

(b) Linking records of ICES Data; and

(c) Use of ICES Data for ICES Projects

4.3 Authority to Use PHI/PI

4.3.1 ICES shall use PHI/PI, and permit access and use of PHI/PI by ICES Agents, only as set out in ICES' incorporating documents as a not-for-profit corporation and as permitted or required by law, including but not limited to Ontario's Personal Health Information Protection Act ("PHIPA"), the Coroners Act, and their applicable regulations.

4.3.2 Authority as a Corporation

(a) ICES can use PHI/PI only for the purposes set out in ICES' Corporate Objects.

4.3.3 Authority as Permitted or Required by Law

(a) ICES is designated a Prescribed Entity under s.18(1) of O. Reg. 329/04 for the purposes of s.45 of PHIPA. As such, ICES has legal authority to use PHI disclosed by Health Information Custodians ("HIC"), Prescribed Entities ("PE"), and/or Prescribed Persons ("PP") 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;

(b) ICES is designated a Prescribed Entity under s.2 of O. Reg. 523/18 to the Coroners Act, for the purposes of s.52.1 of the Coroners Act and, as such, ICES has legal authority to use PI disclosed by the Chief Coroner of Ontario for the purpose of research, data analysis or the compilation of statistical information related to the health or safety of the public, or any segment of the public; and

(c) Any use of PHI/PI by ICES that involves linking PHI with PI collected under the Coroners Act must be for a purpose that falls within the narrower scope of statistical analysis permitted under PHIPA.

4.3.4 Authority for Research

(a) ICES, as a Prescribed Entity, has legal authority pursuant to s.18(3) of O. Reg. 329/04 to PHIPA, and s.37(1)(j) of PHIPA, to use PHI to conduct Research;

(b) PHI may be used by ICES for Research purposes only when such Research:

(i) Is conducted by an ICES Agent;

(ii) Supports ICES' Corporate Objects; and

(iii) Has an ICES Agent named on the written research plan and application approved by an REB,

(c) PHI used by ICES for Research must be supervised by a Responsible ICES Scientist ("RIS") if the ICES Project's Principal Investigator is not an ICES Scientist;

(d) Use of PHI for Research remains subject to the general principle that ICES will not use PHI for Research if other information will serve the Research purpose, nor will it use more PHI than is necessary for the Research purpose;

(e) ICES, as a Prescribed Entity, is permitted under s.3 and s.4 of O. Reg. 523/18 to the Coroners Act to use PI to conduct Research; and

(f) ICES can use PHI and/or PI with consent for Research or non-research purpose.

4.3.5 Authority Under Contracts Research

(a) Any use of ICES Data must be consistent with the purpose(s) for which the ICES Data was collected and in accordance with the applicable Data Sharing Agreement ("DSA");

(b) The terms General Use Data ("GUD"), Controlled Use Data ("CUD"), and Project-Specific Data ("PSD") describe the conditions that the Data Provider places on use of the ICES Data by ICES as follows:

(i) GUD is considered an ICES Data Holding that may be used by ICES Agents for any ICES Project, as set out in a Privacy Impact Assessment ("PIA");

(ii) CUD is considered an ICES Data Holding that may be used by ICES Agents for any ICES Project (as set out in a PIA), but is subject to additional conditions and compliance requirements as directed by the Data Provider in a DSA; and

(iii) PSD is disclosed by Data Providers to ICES for a specific ICES Project or a series of related projects conducted by a Principal Investigator and can be used by ICES Agents only as set out in the PIA and applicable DSA.

4.3.6 Authority for Third Party Service Providers

(a) Use, including access, to ICES Data by Third Party Service Providers must be assessed and approved in accordance with ICES' Third Party Service Provider Policy.

4.3.7 Authority for other Purposes

(a) For all other purposes and in all other circumstances, ICES Agents must use De-Identified Data as set out in ICES' De-Identification and Aggregation Policy.

4.4 Limiting Use of PHI/PI

4.4.1 Access Privileges

(a) All ICES Agents who seek use of PHI/PI must be formally approved and given Access Privileges, and such approval must be monitored, controlled, and audited;

(b) All ICES Agents with Access Privileges must be assigned a level of access based on their role in the organization;

(c) To facilitate and demonstrate compliance with this Policy, the ICES Senior Director for the platform of Research and Data is responsible for ensuring that all ICES Agents have the level of access appropriate for each role at ICES as set out in ICES' Use of ICES Data Standard and any associated Procedures;

(d) ICES Senior Director for the platform of Research and Data may delegate day-to-day responsibility for operationalizing Access Privileges pursuant to this Policy to ICES' Directors of DQIM, R&A, or DAS, as applicable, and as further set out in ICES' Use of ICES Data Standard and any associated Procedures; and

(e) ICES aims, to the extent possible, to segregate duties of ICES Agents to avoid a concentration of Access Privileges that would enable a single ICES Agent to compromise ICES Data.

4.4.2 Default Access Privileges

(a) ICES permits certain roles at ICES to have access to PHI/PI on an ongoing basis through Default Access;

(b) Any approval of Default Access must be in accordance with this Policy and as set out in ICES' Use of ICES Data Standard and any associated Procedures; and

(c) ICES Agents with Default Access also may be granted additional Access Privileges where needed in order to perform their work, in accordance with this Policy, ICES' Use of ICES Data Standard, and any associated Procedures.

4.4.3 Project Specific Access

(a) Access to ICES Data also may be granted to ICES Agents as Project-Specific Access; and

(b) Access Privileges must be assessed and approved in accordance with this Policy, ICES' Use of ICES Data Standard, and any associated Procedures.

4.4.4 Review and Approval Process

(a) The ICES Agent responsible and the process to be followed in receiving, reviewing, and determining whether to approve or deny a request by an ICES Agent for use of ICES Data shall be set out in ICES' Use of ICES Data Standard and associated Procedures, along with the Access Privileges that may be granted;

(b) To satisfy and fulfill lawful authority to use PHI/PI, the following details must be set out in ICES' Use of ICES Data Standard:

(i) The requirements to be satisfied in requesting, reviewing, and determining whether to approve or deny a request by an ICES Agent for use of ICES Data;

(ii) The documentation that must be completed, provided and/or executed, and its required content;

(iii) The ICES Agent responsible for completing, providing and/or executing the documentation; and

(iv) The ICES Agent to whom the documentation must be provided,

(c) The criteria that must be considered by the ICES Agent responsible for determining whether to approve or deny a request for and use of ICES Data, including the criteria considered when determining the appropriate level of access if approved, is set out below:

(i) The ICES Agent making the request routinely requires use of ICES Data on an ongoing basis or for a specified period of their employment, contractual, or other responsibilities;

(ii) The identified purpose for which use of ICES Data is requested is permitted under this Policy, including permitted under PHIPA (for PHI), the Coroners Act (for PI), and their applicable regulations;

(iii) The identified purpose for which use of PHI/PI is requested cannot be reasonably accomplished without PHI/PI;

(iv) De-Identified Data will not serve the identified purpose;

(v) No more PHI/PI will be used than is reasonably necessary to meet the identified purpose;

(vi) The ICES Agent has completed all applicable privacy and cybersecurity awareness and training as set out in ICES' Privacy and Security Awareness and Training Policy and Procedures;

(vii) The ICES Agent has signed an ICES Agent CA as set out in the ICES Agent Policy;

(viii) To the best of their knowledge, the ICES Agents granted Access Privileges to ICES Data have a record of complying with all Policies, Procedures, Practices, and applicable agreements;

(ix) Any restrictions or conditions set out in applicable PIAs, DSAs, Policies, Procedures, Disciplinary Findings, and/ or Risks; and

(x) Whether the appropriate level of access (if the request is approved) is associated with the least identifiable level of PHI/PI necessary for the purpose,

(d) The manner in which the decision approving or denying the request for use of ICES Data, the reasons for the decision, and details around the supporting documentation must be set out in ICES' Use of ICES Data Standard and associated Procedures;

(e) The method by which and the format in which the decision will be communicated (and to whom) must be set out in ICES' Use of ICES Data Standard and associated Procedures;

(f) ICES' Use of ICES Data Standard further reinforces the requirement that use of ICES Data is permitted only for the specified time period as set out in the PIA and DSA, and that this information is captured accordingly as set out in ICES' Use of ICES Data Standard and associated Procedures; and

(g) ICES does not automatically terminate Access Privileges annually, but rather requires that all ICES Agents sign an ICES Agent CA, which mandates that ICES Agents use ICES Data only for the specified time period set out in a PIA and DSA and in accordance with ICES' Use of ICES Data Standard and any associated Procedures. Where there are no automatic expiry dates with an approved use of ICES Data, regular audits of ICES Agents must take place.

4.4.5 Audit of ICES Agents Granted Approval Use ICES Data

(a) To ensure that ICES' Practices align with its lawful authority to use ICES Data, ICES must conduct regular audits of ICES Agents with Access Privileges;

(b) Audits must be conducted in accordance with ICES' Privacy and Security Audit Policy and associated Procedures, such that ICES can confirm that:

(i) ICES Agents with Access Privileges continue to be employed or retained by ICES;

(ii) ICES Agents with Access Privileges continue to require access to the same amount and type of ICES Data; and

(iii) ICES Agents with Access Privileges continue to access ICES Data only for the time needed to conduct the applicable ICES Project as set out in the PIA and DSA,

(c) ICES Director, Privacy and Legal Office ("PLO") is responsible for conducting the audit and ensuring that it conforms to the requirements set out in ICES' Privacy and Security Audit Policy; and

(d) All audits with respect to Access Privileges must be conducted, at minimum, on an annual basis.

4.4.6 Tracking approved use of ICES Data

(a) As set out in ICES' Use of ICES Data Standard, a log must be maintained that sets out those ICES Agents granted approval to use ICES Data;

(b) Such log must be maintained by ICES' Director, DQIM;

(c) All documentation related to the receipt, review, approval, denial or termination of use of ICES Data is retained as set out in the Use of ICES Data Standard and any associated Procedures; and

(d) Such documentation must be maintained by ICES' Director, PLO.

4.5 Data Linkages

4.5.1 ICES permits records of PHI/PI to be linked to facilitate permissible uses as set out in this Policy.

4.5.2 The purposes for all Data Linkages must be set out in PIAs as required under ICES' Privacy Impact Assessment Policy.

4.5.3 All contemplated Data Linkages must be set out in DSAs as required under ICES' Execution of Data Sharing Agreement Standard.

4.5.4 Any ICES Data that is not PHI but is then linked to PHI becomes subject to PHIPA as a Mixed Record, unless an Act of the Provincial Legislature or Federal Parliament states otherwise.

4.5.5 Record Linkages

(a) In accordance with ICES' Use of ICES Data Standard, DQIM personnel are permitted to conduct Record Linkages and coding, the latter of which involves removal of some or all Direct Personal Identifiers and Indirect Personal Identifiers and assignment of a unique identifier to ICES Data;

(b) All details surrounding the review and approval of Record Linkages are set out in ICES' Use of ICES Data Standard and any associated Procedures;

(c) All details regarding the conditions or restrictions on the approval of Record Linkages are set out in ICES' Use of ICES Data Standard and any associated Procedures;

(d) All details regarding the process of Record Linkages are set out in any Procedures aligned with this Policy and ICES' Use of ICES Data Standard and any associated Procedures; and

(e) ICES Director, PLO is responsible for ensuring that a log is maintained to capture the Record Linkages of PHI/PI as set out in ICES' Use of ICES Data Standard.

4.5.6 Project-Based Linking

(a) Project-Based Linking of PHI/PI is permitted for the purpose of creating Project Datasets to support the conduct of Analytics and Research in accordance with ICES' Use of ICES Data Standard;

(b) Project Datasets created through Project-Based Linking must be converted to De-identified Data as soon as practicable after the purpose of the linkages has been fulfilled, pursuant to ICES' De-Identification and Aggregation Policy;

(c) All details surrounding the review and approval of Project-Based Linking are set out in ICES' Use of ICES Data Standard and any associated Procedures;

(d) All details regarding the conditions or restrictions on the approval of Project-Based Linking are set out in ICES' Use of ICES Data Standard and any associated Procedures;

(e) All details regarding the process for Project-Based Linking are set out in any Procedures aligned with this Policy and ICES' Use of ICES Data Standard;

(f) All Project Datasets created through Project-Based Linking must be retained in compliance with the ICES Data Retention Schedule Standard until it becomes De-Identified Data pursuant to ICES' De-Identification and Aggregation Policy;

(g) All Project Datasets created through Project-Based Linking must be securely disposed of in compliance with ICES' Secure Disposal Standard;

(h) ICES Director, PLO is responsible for ensuring that a log is maintained to capture the Project-Based Linking of PHI/PI as set out in ICES' Use of ICES Data Standard and any associated Procedures; and

(i) All details regarding the log, whether to review, approve or deny requests for Project-Based Linking are set out in ICES' Use of ICES Data Standard.

4.6 Notification and Termination of use of PHI/PI

4.6.1 Access to PHI/PI must terminate when no longer required.

4.6.2 ICES Agents granted approval to use PHI/PI must remove themselves from the Project Data Folder when use of PHI/PI is no longer required for their ICES Project.

4.6.3 When an ICES Agent is no longer employed or retained by ICES, the individual's access to PHI/PI must be terminated in accordance with ICES' Use of ICES Data Standard and associated Procedures.

4.6.4 The following details are set out in the Use of ICES Data Standard

(a) The time frame within which the notification must be provided;

(b) The format of the notification;

(c) The documentation that must be completed, provided and/or executed, if any;

(d) The ICES Agent responsible for completing, providing, and/or executing the documentation;

(e) The ICES Agent to whom the notification and documentation must be provided;

(f) The required content of the documentation; and

(g) The ICES Agent responsible for terminating use of PHI/PI, including all associated Procedures, and the time frame within which access must be terminated.

4.6.5 Any Procedures implemented to satisfy the requirements in this Policy must be consistent with ICES' Termination or Cessation of Employment or Contractual Relationship in Relation to ICES Data Policy.

4.7 Use of PHI/PI for Research

4.7.1 ICES permits use of ICES Data, including PHI/PI, for Research as determined by the analysis set out in the PIA, pursuant to ICES' Privacy Impact Assessment Policy.

4.7.2 All ICES Projects for Research must have valid REB approval as set out in s.44(1) of PHIPA and/or s.3(1) of O. Reg 523/18 to the Coroners Act.

4.7.3 PHI/PI may not be used for a Research purpose if there is no valid REB approval of the written research plan.

4.7.4 The criteria utilized by ICES Agents in determining when a use of PHI/PI is for Research purposes and when a use is for Statistical Analysis (also called Analytics) is set out in ICES' Privacy Impact Assessment Policy.

4.7.5 The ICES Agent responsible for reviewing and determining whether to approve or deny a request for the use of PHI/PI for Research purposes in relation to an ICES Project is the ICES Manager, Privacy. The process to be followed in this review and determination, including any documentation that must be completed, is set out in ICES' Privacy Impact Assessment Policy.

4.7.6 The requirements that must be satisfied and the criteria that must be considered by the ICES Manager, Privacy in determining whether to approve the request to use PHI/PI for Research purposes is set out in ICES' Privacy Impact Assessment Policy. The requirements and criteria shall have regard to PHIPA and its regulation to ensure the request is in compliance.

4.7.7 ICES Manager, Privacy must ensure that the PHI/PI being requested is consistent with the PHI/PI identified in the written research plan approved by the REB, as further set out in ICES' Privacy Impact Assessment Policy.

4.7.8 ICES Manager, Privacy must ensure that other information, namely De-Identified Data, will not serve the Research purpose and that no more PHI/PI is being requested than is reasonably necessary to meet the Research purpose, as set out in ICES' De-Identification and Aggregation Policy and ICES' Privacy Impact Assessment Policy.

4.7.9 All conditions or restrictions for the use of PHI/PI for Research are set out in ICES' Privacy Impact Assessment Policy.

4.7.10 All PHI/PI used for Research purposes as set out in ICES' Privacy Impact Assessment Policy must be retained and used only during the time frame and retention period identified in the written research plan, unless a REB approves amendments to the research plan's time frame and/or retention period, and these changes are in compliance with ICES' Information Security Policy.

4.7.11 The location for the written research plans, copies of the decisions of REBs, certificates of data destruction, and other documentation related to the receipt, review, or denial of requests for the use of PHI/PI for Research purposes will be retained as set out in ICES' Privacy Impact Assessment Policy and associated Procedures.

4.8 Use of Non-PHI/PI for Research

4.8.1 ICES Agents are permitted to use Non-PHI/PI for Research purposes.

4.8.2 The requirements to be satisfied and the criteria that must be considered by the ICES Manager, Privacy in determining whether to approve or deny the request to use Non-PHI/PI for Research purposes must be in accordance with ICES' Privacy Impact Assessment Policy and ICES' De-Identification and Aggregation Policy.

4.8.3 Any conditions or restrictions for the use of Non-PHI/PI for Research purposes are set out in ICES' Privacy Impact Assessment Policy and ICES' De-Identification and Aggregation Policy.

4.9 Logging

4.9.1 If a collection and use of PHI/PI is for Research purposes, the Log of Approved Uses of PHI/PI for Research must capture the following information:

(a) Name of the research study;

(b) Name of the ICES Agent(s) using, including accessing, the PHI/PI;

(c) The date of the decision of the REB approving the written research plan;

(d) The date that the PIA was finalized and approved to grant the use of PHI/PI;

(e) The date that the PHI/PI was provided to the ICES Agent;

(f) The nature of the PHI/PI provided to the ICES Agent;

(g) The retention period for the PHI/PI identified in the written research plan approved by the REB;

(h) Whether the PHI/PI will be securely returned, securely disposed of, or De-Identified and retained following the retention period; and

(i) The date the PHI/PI is securely returned or a certification of destruction is received or the date by which they must be returned or disposed of, if applicable.

4.10 Secure Retention

4.10.1 ICES Director, DQIM is responsible for ensuring that PHI/PI approved for the uses of Record Linkages, Project-Specific Linkages, Statistical Analyses (also called Analytics), or Research must be securely retained in accordance with compliance with ICES' Information Security Policy.

4.10.2 ICES Agents granted approval to use PHI/PI must securely retain the records of PHI/PI in compliance with ICES' ICES Data Retention Schedule Standard.

4.11 Secure Disposal

4.11.1 ICES Director, DQIM is responsible for ensuring that PHI/PI approved for the uses of Record Linkages, Project-Specific Linkages, Statistical Analyses (also called Analytics), and Research are securely disposed of in accordance with ICES' Secure Disposal Standard.

4.11.2 ICES Agents granted approval to use PHI/PI must securely dispose PHI/PI in compliance with ICES' Secure Disposal Standard.

5.0 RELATED DOCUMENTATION

5.1 Policies

5.2 Standards

5.3 Procedures

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

Change Date (YYYY-MM-DD)	**Change Notes**