Privacy Policy

Department	Reference Number	Organizational Scope	ICES Site	IPC Scope
PLO	001-00-00	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)
2014-01-01	2025-10-31	Annual	October 2026	2025-07-30

Authority (Title)	Chief Privacy and Legal Officer
Policy Owner (Title)	Director, Privacy and Legal Office
Required Reviewers (Titles)	N/A

Please refer to the **glossary** for terms and 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 provides the general principles that form the lawful basis for ICES' collection, use, disclosure, and **Processing** of **Identifiable Information**.

1.1.1 Identifiable Information is **ICES Data** or **Corporate Information** that identifies an individual or it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify an individual.

1.1.2 The following types of ICES Data are considered Identifiable Information:

(a) **Personal Health Information ("PHI")**;

(b) **Personal Information ("PI")**; and

(c) **Other Identifiable Data**.

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

1.1.3 Identifying information about **ICES Employees** and other **ICES Agents** are examples of Corporate Information considered Identifiable Information.

(a) Further details regarding Identifiable Information about ICES Employees are set out in the *Employee Privacy Policy*.

1.2 This policy supports a clear mandate for ICES' robust compliance regime in relation to Identifiable Information.

1.3 This policy identifies the primary roles and responsibilities for ICES' privacy program.

1.4 This policy sets out ICES' approach to protection of Identifiable Information.

2.0 SCOPE

2.1 This policy applies to all activities of ICES involving Identifiable Information collected, used, disclosed or otherwise Processed by ICES.

2.2 For ICES Data, this policy applies to PHI, PI, and Other Identifiable Data, as well as any derivatives of that ICES Data.

3.0 ROLES AND RESPONSIBILITIES

3.1 Chief Executive Officer ("**CEO**")

3.1.1 Ultimate responsibility for ensuring that ICES complies with:

(a) Applicable laws and other legal requirements, including ICES' obligations as a **Prescribed Entity** under:

(i) *Personal Health Information Protection Act* ("***PHIPA***") and its regulation;

(ii) *Coroners Act* and its applicable regulations*;* and

(iii) *Child, Youth and Family Services Act* ("***CYFSA***") and its applicable regulations.

(b) This policy and all other privacy and security policies, standards, and procedures implemented by ICES.

3.1.2 At a minimum, the CEO's responsibilities include:

(a) Seeking and implementing the policies, standards, and procedures necessary to maintain ICES' Prescribed Entity designation under *PHIPA*, the *Coroners Act* and the *CYFSA*, and complying with such statutes and their applicable regulations, as amended from time to time.

(b) Appointing and overseeing a Chief Privacy and Legal Officer ("**CPLO**").

(c) Ensuring the necessary budgets and agreements are in place to maintain a team of Privacy **Subject Matter Experts ("SMEs")**, reporting to the CPLO or their delegate, and located across the **ICES Network**.

(d) Taking the steps necessary to ensure reporting of **Privacy Breaches** and **Privacy Complaints**.

(e) Final signing-off approval on **In-Depth Audits**.

(f) Ensuring there are written updates on the status of ICES' privacy program to the Finance, Audit & Risk Committee ("**FAR**") of the Board of Directors, which may include information regarding:

(i) Privacy training;

(ii) The development and implementation of privacy policies, standards, and procedures;

(iii) **Compliance Audits**, including recommendations and the implementation status of the recommendations, in accordance with the *Privacy and Security Audit Policy*; and

(iv) **Privacy Impact Assessments ("PIAs")**, including recommendations and the implementation status of the recommendations, in accordance with the *Privacy*

Impact Assessment Policy.

(g) Fostering a privacy-minded culture and promoting awareness of and compliance with policies, standards, and procedures.

3.2 Chief Privacy and Legal Officer

3.2.1 Reports directly to the CEO and is delegated authority for executive oversight of ICES' Privacy and Cybersecurity programs, including:

(a) The design and oversight of ICES' **Key Control** environment, with consideration of ICES' obligations as a Prescribed Entity, and including responsibility for the development, revision, approval, communication and implementation of required policies, standards, and procedures for the effective prevention, detection, and response to Privacy Breaches and **Security Incidents**.

(b) The oversight of a team of Privacy SMEs, distributed across the ICES Network, responsible for ensuring compliance with policies, standards, and procedures, and delivering a range of privacy services, including but not limited to:

(i) Privacy awareness;

(ii) Privacy training;

(iii) Conducting PIAs;

(iv) Supporting the development of **Data Sharing Agreements ("DSAs")** and other legal agreements;

(v) Addressing **Compliance Breaches** and Privacy Breaches;

(vi) Performing or supporting Compliance Audits; and

(vii) Responding to a variety of privacy-related consultations.

(c) This includes oversight of the Privacy and Legal Office ("**PLO**") and Cybersecurity department, in accordance with the *Privacy and Security Governance and Accountability Policy*; and

(d) Ensuring all ICES committees involving discussion, decision, or actions in relation to PHI/PI include representation of Privacy SMEs.

(i) The current list of all ICES committees that include Privacy SME representation is set out on the **ICES Intranet**..

4.0 DETAILS

4.1 Legal Authorities

4.1.1 *PHIPA*

(a) ICES is designated a Prescribed Entity under s.18(1) of Ontario Regulation 329/04 under *PHIPA* for the purposes of s.45 of *PHIPA*.

(b) As a Prescribed Entity under *PHIPA*, ICES has the legal authority to collect, use, and disclose PHI for the purpose of analysis or compiling statistical information with respect to the management of, evaluation or monitoring of, or the allocation of resources to or planning for all or part of the health system, including the delivery of services.

4.1.2 *Coroners Act*

(a) ICES is designated a Prescribed Entity under s.2 of Ontario Regulation 523/18 under the *Coroners Act,* for the purposes of s.52.1 of the *Coroners Act*.

(b) As a Prescribed Entity under the *Coroners Act*, ICES has legal authority to collect, use, and disclose PI as defined under the *Coroners Act* 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.

4.1.3 *CYFSA*

(a) ICES is designated as a Prescribed Entity under s.1 of Ontario Regulation 191/18 under the *CYFSA* for the purposes of s.293 of the *CYFSA*.

(b) As a Prescribed Entity under the *CYFSA*, ICES has legal authority to collect, use, and disclose PI as defined under the *CYFSA* for the purpose of analysis or compiling statistical information with respect to the management of, evaluation or monitoring of services, the allocation of resources to or planning for those services, including their delivery.

4.1.4 Not-for-profit corporation

(a) ICES is a not-for-profit corporation incorporated in 1992 under the laws of Ontario.

(b) As a not-for-profit corporation, ICES has legal authority to collect and use Identifiable Information pursuant to its **Corporate Objects**.

(i) For PHI/PI, ICES may only collect and use PHI/PI if its Corporate Objects align with the intended purposes for the collection and use set out in *PHIPA*, the *Coroners Act*, the *CYFSA*, and their applicable regulations.

4.1.5 Indigenous Data

(a) ICES respects the principle of **Indigenous Data Sovereignty** and aims to incorporate the principle in ICES' approach to data governance, including the collection, use, and disclosure of **Indigenous Data**.

(b) The First Nations principles of OCAP® (Ownership, Control, Access, and Possession) also form part of ICES' approach to data Processing practices.

4.1.6 Data Sharing Agreements

(a) ICES enters into DSAs with respect to the collection, use, and disclosure of PHI/PI and such DSAs outline the terms and conditions for ICES lawfully collecting, using, and/or disclosing the PHI/PI governed by the DSAs.

4.1.7 Research

(a) To rely on a **Research** legal authority for the collection, use, and disclosure of Identifiable Information, ICES must be specifically named in a written research plan approved by a **Research Ethics Board ("REB")**, and such research plan must clearly articulate the data flow to ICES and ICES' role(s) in Processing the Identifiable Information in the planned Research.

4.1.8 Other authorities

(a) ICES may collect and use Other Identifiable Data in instances where ICES'

designations as a Prescribed Entity under *PHIPA,* the *Coroners* Act, and the *CYFSA* are not applicable. ICES must ensure it has lawful authority to collect and use the Other Identifiable Data, which may or may not be subject to other privacy legislation.

(b) ICES may collect and use **Non-Identifiable Data** subject to the requirements and obligations set out in this policy, the *Collection of ICES Data Policy,* and the *Use of ICES Data Policy*.

4.2 Compliance

4.2.1 ICES implements privacy and security policies, standards, and procedures required to protect the privacy of individuals whose Identifiable Information it receives and to maintain the confidentiality of that Identifiable Information.

4.2.2 ICES is committed to complying with the provisions of *PHIPA*, the *Coroners Act,* the *CYFSA*, and their regulations applicable to Prescribed Entities and as it relates to PHI/PI.

4.2.3 With regards to PHI/PI, ICES' policies, standards, and procedures are written to ensure compliance with the following documents:

(a) **IPC Manual**;

(b) **Coroners Addendum**; and

(c) **CYFSA Addendum**.

4.2.4 As a Prescribed Entity, policies, standards, and procedures are subject to review by the Information and Privacy Commissioner of Ontario ("**IPC**") every three years.

4.2.5 ICES is responsible for the Identifiable Information collected, used, and disclosed by ICES Agents.

4.2.6 ICES is responsible for ICES Agents' compliance with ICES' policies, standards, and procedures.

4.2.7 ICES ensures compliance by ICES Agents with *PHIPA*, the *Coroners Act* and the *CYFSA* through:

(a) Policies, standards, and procedures;

(b) Privacy awareness and training; and

(c) Contractual agreements.

4.3 Identifiable Information collected and used by ICES for Statistical Analysis (Analytics) and Research

4.3.1 Most of ICES' scientific programs and services involve the collection and use of Identifiable Information that is subject to privacy law, including but not limited to:

(a) PHI as defined under *PHIPA;*

(b) PI collected from the Chief Coroner under the *Coroners Act;* and

(c) PI collected from **Service Providers** under the *CYFSA*.

4.3.2 ICES collects and uses Identifiable Information for the purpose of the administration of its scientific programs and services, including:

(a) **Statistical Analysis (Analytics)**; and/or

(b) Research

4.3.3 ICES may only collect and use Identifiable Information that is permitted by law and aligns with its Corporate Objects.

4.3.4 ICES collects the following types of Identifiable Information for Statistical Analysis (Analytics) and Research:

(a) PHI originally collected by **Health Information Custodians ("HICs")** and Prescribed Entities or **Prescribed Persons**;

(b) PHI and Other Identifiable Data collected as part of a **Third Party Research Project ("TPR Project")**;

(c) Other Identifiable Data that was originally collected by other organizations in the public and private sectors and are not governed by *PHIPA*, the *Coroners Act*, or the *CYFSA*;

(d) PI collected from the Chief Coroner under the *Coroners Act*;

(e) PI collected from Service Providers under the *CYFSA*; and

4.4 Identifiable Information collected and used by ICES for business operations

4.4.1 ICES collects Identifiable Information to manage its relationships with ICES Employees, other ICES Agents, affiliated individuals, and others who interact with ICES.

4.5 Protection principles when collecting and using Identifiable Information

4.5.1 ICES recognizes that Identifiable Information is inherently sensitive and ICES is responsible for ensuring that Identifiable Information is processed in accordance with the following:

(a) ICES' policies, standards, and procedures

(i) For PHI/PI, more specifically ICES' policies, standards, and procedures as a Prescribed Entity under *PHIPA, Coroners Act*, the *CYFSA*, and their applicable regulations;

(b) Other applicable law;

(c) Contractual obligations; and

(d) REB approvals, as applicable

4.5.2 ICES adopts the following key principles, which guides its collection, use, disclosure, and other processing of Identifiable Information:

(i) ICES collects and uses Identifiable Information only when:

(A) Permitted by *PHIPA*, the *Coroners Act* and/or the *CYFSA*, and their applicable regulations, with regards to PHI/PI;

(B) In accordance with applicable law; and

(C) REB approvals, when necessary.

(b) ICES adheres to **Data Minimization** principles, including:

(i) Not collecting or using Identifiable Information if other information will serve the purpose; and

(ii) Not collecting or using more Identifiable Information than is reasonably necessary to meet the purposes identified.

(c) ICES implements policies, standards, and procedures to ensure that both the amount and the type of Identifiable Information collected and used is limited to that which is reasonably necessary for its purposes. Examples of these policies, standards, and procedures include:

(i) *Collection of ICES Data Policy;*

(ii) *Privacy Impact Assessment Policy;*

(iii) *Use of ICES Data Policy*; and

(iv) *Dataset Creation Plan Procedure*

(d) For Identifiable Information collected as ICES Data, ICES ensures that upon collection of it, ICES assigns a confidential **ICES Key Number ("IKN")** to individual-level Identifiable Information and removes the **Direct Personal Identifiers ("DPI")** before making available for use by ICES Agents.

(e) ICES maintains a list of its **ICES Data Holdings** containing Identifiable Information, as currently listed in Appendix A.

(i) The **Data Dictionary**, available through ICES' website, sets out further information related to the purposes, data variables, and data sources for each ICES Data Holding containing Identifiable Information.

4.6 Privacy Impact Assessments

4.6.1 For ICES Data that is Identifiable Information, ICES distinguishes in each PIA if the purpose for the use of the Identifiable Information is for Statistical Analysis (Analytics) or Research, in accordance with the following:

(a) With respect to PHI that was collected by ICES as a Prescribed Entity under *PHIPA*, ICES distinguishes between:

(i) Uses for Statistical Analysis (Analytics) purposes in accordance with s.45 of *PHIPA;* and

(ii) Uses for Research in accordance with s.37 of *PHIPA*.

(b) With respect to PI that was collected by ICES as a Prescribed Entity under the *Coroners Act*, ICES distinguishes between:

(i) Uses for Statistical Analysis (Analytics) in accordance with s.52.1(1) of the *Coroners Act;*

(ii) Uses for Research in accordance with s.52.1(1) of the *Coroners Act*; and

(iii) Uses for Research in accordance with s.4 of Ontario Regulation 523/18.

(c) With respect to PI that was collected by ICES as a Prescribed Entity under the *CYFSA,* ICES distinguishes between:

(i) Uses for Statistical Analysis (Analytics) in accordance with s.293 of the *CYFSA;* and

(ii) Uses for Research in accordance with s.4 of Ontario Regulation 191/18.

4.6.2 All requests to conduct Statistical Analysis (Analytics) or Research require a PIA by ICES to ascertain legal authority and compliance with its policies, standards, and procedures,

Corporate Objects, applicable legal agreements, and REB approvals.

4.6.3 PIAs must set out findings, risks, and recommendations, if applicable, associated with the requests outlined in the PIAs.

4.6.4 PIAs must be conducted by an appropriate Privacy SME.

4.6.5 PIAs must clearly distinguish between the use of Identifiable Information and the use of **De-Identified Information**, either in the form of **Aggregate Data (Summary Output)** or **Publishable Data**.

4.6.6 When ICES collects PHI/PI as a Prescribed Entity, PIAs must ensure that each use of PHI/PI is consistent with the uses of PHI/PI permitted by applicable statute governing it, including but not limited *PHIPA,* the *Coroners Act*, and/or the *CYSFA*, and their regulations.

4.6.7 All PIAs must articulate a commitment that the use of Identifiable Information by ICES Agents is only in support of and in alignment with ICES' Corporate Objects.

4.7 Use of Identifiable Information by ICES Agents

4.7.1 ICES remains responsible for the Identifiable Information used by any ICES Agents, as set out in the **ICES Agent and Confidentiality Agreement ("ICES Agent CA")**.

4.7.2 ICES Agents must only collect, use, disclose, and otherwise process Identifiable Information in accordance with:

(a) ICES policies, standards, and procedures;

(b) The ICES Agent CA and the *ICES Agent Policy*; and

(c) Applicable statute that may govern the Identifiable Information, including but not limited to PHI/PI collected by ICES as a Prescribed Entity under *PHIPA*, *Coroners Act*, and/or *CYFSA*.

4.8 Disclosure of PHI/PI

4.8.1 PHI initially collected under *PHIPA*

(a) For PHI that was initially collected by ICES as a Prescribed Entity under *PHIPA*, ICES may only disclose PHI for one of the following purposes set out below. Otherwise ICES does not disclose this PHI.

(i) Disclosure of PHI to Prescribed Entities and Prescribed Persons for their prescribed purposes, as permitted by s.18(4) of Ontario Regulation 329/04 to *PHIPA,* with respect to s.39 (1)(c) and s.45 of *PHIPA*, and verified through a PIA conducted by ICES;

(ii) Disclosure of PHI for TPR Projects, only in the form of **Risk Reduced Coded Data ("RRCD")** on a secure **ICES Data Environment**, for the purposes of publicly or privately funded research, as permitted by s.18(4) of Ontario Regulation 329/04 to *PHIPA*, with respect to s.44 of *PHIPA*, and verified through a PIA conducted by ICES; and

(iii) Disclosure of PHI for TPR Projects in the form of a **Cohort Disclosure List**, for the purposes of publicly funded research that cannot be reasonably conducted within ICES, as permitted by s.44 of *PHIPA* and verified through a PIA conducted by ICES; and

(iv) Disclosure of PHI as otherwise permitted under *PHIPA*.

4.8.2 PI initially collected under the *Coroners Act*

(a) For PI that was initially collected by ICES as a Prescribed Entity under the *Coroners Act*, ICES may only disclose this PI for one of the following purposes set out below. Otherwise ICES does not disclose this PI.

(i) Disclosure of PI for TPR Projects in accordance with s.5 of Ontario Regulation 523/18 to the *Coroners Act* and verified through a PIA conducted by ICES;

(ii) Disclosure of PI to the Chief Coroner in accordance with s.6 of Ontario Regulation 523/18 to the *Coroners Act*, and verified through a PIA conducted by ICES; and

(iii) Disclosure of PI as otherwise permitted under the *Coroners Act*.

4.8.3 PI initially collected under the *CYFSA*

(a) ICES does not disclose PI that was initially collected by ICES as a Prescribed Entity under the *CYFSA*, however ICES may disclose De-Identified Information derived from use of this PI.

4.9 Protection principles when disclosing Identifiable Information

4.9.1 ICES adheres to Data Minimization principles when disclosing Identifiable Information, including:

(a) Not disclosing Identifiable Information if other information, such as De-Identified Information, will serve the purpose; and

(b) Not disclosing more Identifiable Information than is reasonably necessary to meet the purpose.

4.9.2 ICES implements policies, standards, and procedures to ensure that both the amount and the type of Identifiable Information disclosed is limited to that which is reasonably necessary for its purposes. Examples of these policies, standards, and procedures include:

(a) *Disclosure of ICES Data Policy;* and

(b) *Dataset Creation Plan Procedure*.

4.9.3 Excluding disclosure of Cohort Disclosure Lists, **Third Party Researchers** conducting TPR Projects are only permitted to access RRCD on a secure ICES Data Environment.

4.9.4 ICES does not disclose Identifiable Information to any **Knowledge User**.

4.10 Disclosure of De-Identified Information

4.10.1 Excluding disclosure of Cohort Disclosure Lists, only De-Identified Information may be released from a secure ICES Data Environment to Third Party Researchers.

4.10.2 Only De-identified Information may be disclosed to Knowledge Users.

4.10.3 In accordance with the *De-Identification and Aggregation Policy,* a **Re-Identification Risk Assessment ("RIRA")** must be conducted prior to disclosure of De-Identified Information to ensure that it is not reasonably foreseeable in the circumstances that any De-identified Information could be used, either alone or with other information, to identify an individual.

4.11 Secure transfer of Identifiable Information

4.11.1 ICES takes steps to transfer Identifiable Information securely, as set out in the *Secure Collection, Disclosure, and Transfer of PHI/PI Procedure* and the *Information Handling Standard*.

4.11.2 ICES does not transfer paper records that include PHI/PI.

4.12 Secure retention and destruction of Identifiable Information

4.12.1 Identifiable Information is retained in accordance with the *ICES Data Retention Schedule Standard* and the *Information Handling Standard.*

4.12.2 Identifiable Information is disposed of in accordance with the *Secure Disposal Standard* and the *Destruction of ICES Data Procedure*.

4.13 Implementation of administrative, technical, and physical safeguards

4.13.1 ICES implements a range of administrative, technical, and physical safeguards to protect Identifiable Information. More specifically, these safeguards protect the privacy of individuals whose Identifiable Information that ICES receives and to maintain the confidentiality of that Identifiable Information.

4.13.2 ICES assesses the range of administrative, technical, and physical safeguards in PIAs and **Threat Risk Assessments ("TRAs").**

4.13.3 The administrative, technical, and physical safeguards implemented by ICES are set out in more detail in ICES' privacy and security policies, standards, and procedures, including but not limited to the safeguards set out in Appendix B. These are steps ICES takes to protect Identifiable Information against theft, loss, and unauthorized collection, use, or disclosure, and to protect Identifiable Information against unauthorized copying, modification, or disposal.

4.14 Privacy Inquiries and Privacy Complaints

4.14.1 ICES ensures individuals can make **Privacy Inquiries** and Privacy Complaints regarding:

(a) ICES' privacy policies, standards, and procedures; and/or

(b) ICES' compliance with *PHIPA*, the *Coroners Act*, and/or the *CYFSA* as a Prescribed Entity.

4.14.2 Individuals may direct Privacy Inquiries and Privacy Complaints, either verbally or in writing, to the CPLO at ICES:

Institute for Clinical Evaluative Sciences
Attn: Chief Privacy and Legal Officer
V Wing, V1-06
2075 Bayview Avenue
Toronto, Ontario M4N 3M5
Telephone: 416-480-4055
Email: privacy@ices.on.ca

4.14.3 Individual may obtain further information about ICES' privacy policies, standards, and procedures on ICES' website or by contacting the CPLO, including further information about ICES' *Privacy Inquiries and Privacy Complaints Policy*.

4.14.4 Individuals may also direct to the IPC any Privacy Complaints about ICES compliance as a Prescribed Entity under:

(a) *PHIPA* and its regulation;

(b) Section 52.1 of the *Coroners Act* and its regulations; and/or

(c) Section 293 of the *CYFSA* and its regulations.

4.14.5 Individuals may contact the IPC at the below mailing address and contact details:

Office of the Information and Privacy Commissioner of Ontario
Suite 1400 – 2 Bloor Street East
Toronto, Ontario M4W 1A8
Telephone: 1-800-387-0073
Email: info@ipc.on.ca
Website: www.ipc.on.ca/en/contact-us

5.0 RELATED DOCUMENTATION

5.1 Policies

5.1.1 *Collection of ICES Data Policy*

5.1.2 *De-Identification and Aggregation Policy*

5.1.3 *Disclosure of ICES Data Policy*

5.1.4 *Employee Privacy Policy*

5.1.5 *ICES Agent Policy*

5.1.6 *Privacy and Security Governance and Accountability Policy*

5.1.7 *Privacy and Security Audit Policy*

5.1.8 *Privacy Impact Assessment Policy*

5.1.9 *Privacy Inquiries and Privacy Complaints Policy*

5.1.10 *Use of ICES Data Policy*

5.2 Standard

5.2.1 *ICES Data Retention Schedule Standard*

5.2.2 *Information Classification Standard*

5.2.3 *Information Handling Standard*

5.2.4 *Secure Disposal Standard*

5.3 Procedures

5.3.1 *Dataset Creation Plan Procedure*

5.3.2 *Destruction of ICES Data Procedure*

5.3.3 *Secure Collection, Disclosure, and Transfer of PHI/PI Procedure*

5.4 Tools

5.4.1 Data Dictionary

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**
2025-07-30	■ Reviewed for compliance with ICES' obligations as a **Prescribed Entity**: ○ **IPC Manual:** Privacy Policy in Respect of its Status as a Prescribed Person or Prescribed Entity ○ **Coroners Addendum:** Privacy Policy in Respect of its Status as a Prescribed Entity ○ **CYFSA Addendum:** Privacy Policy in Respect of its Status as a Prescribed Entity ■ Added content regarding ICES' role as a *Prescribed Entity* under *CYFSA* ■ Revised to reflect updated template and standardized language in Sections 6.0 to 9.0 ■ Revised to reflect updated glossary terms and titles of ICES policies, standards, and procedures ■ Removed content where it is already more suitably addressed in other ICES policies, standards, and procedures.
2025-10-31	■ Revised to reflect updated ICES Information classification; general revisions for clarity; added Appendix A and Appendix B

Appendix A

ICES Data Holdings

- Some ICES Data Holdings listed may not contain Identifiable Information
- Some ICES Data Holdings listed may not currently be available for use and/or disclosure

Short Title	Full Title
ADP	Assistive Devices Program
ALR	Cancer Activity Level Reporting
ASTHMA	Ontario Asthma dataset
BORN	Better Outcomes Registry and Network
BRTRC	Bariatric Registry
C19INTGR	COVID19 Integrated Testing Data
CAPE	Client Agency Program Enrolment
CBI	Community Business Intelligence
CCHS	Canadian Community Health Survey
CCIS	Critical Care Information System
CCM	Case and Contact Management System
CCN	Cardiac Care Network
CCRS	Continuing Care Reporting System
CENSUS	Ontario Census Area Profiles
CENSUSCA	Canada Census Area Profiles
CERNER	Laboratory Data from South-Western Ontario Hospitals
CHC	Community Health Centre
CHF	Congestive Heart Failure
CIC	IRCC Permanent Residents database
CJRR	Canadian Joint Replacement Registry
CLD	Clinical Liver Database
CLSA	Canadian Longitudinal Study on Aging
CONTACT	Yearly Health Services Contact
COPD	Chronic Obstructive Pulmonary Disease
CORR	Canadian Organ Replacement Registry
COVAXON	Ontario COVID-19 Vaccine Data
CPDB	Corporate Provider Database
CPRO	Client Profile Database
DAD	Discharge Abstract Database DAD
DATIS	Drug and Alcohol Treatment Information System

Short Title	Full Title
DDARD	Drug and Drug/Alcohol-related Deaths
DEMENTIA	Ontario Dementia Database
DIN	Drugs List
DPD	Drug Product Database
EFFECT	Enhanced Feedback for Effective Cardiac Treatment
EMRPC	Electronic Medical Records Primary Care – Master Linking Crosswalk
ERCLAIM	OHIP's Emergency Claims Database
ESAS	Symptom Management Database
ESTSOB	Estimated Schedule of Benefits (SOB) price associated with each OHIP feecode and suffix.
GAPP	GAPP Decision Support Systems (Physician Payments)
GDML	Gamma Dynacare Medical Laboratories
GEMINI	GEMINI Study
HCD	Home Care Database
HCDMOH	Home Care Database (Alternate Source: MOHLTC)
HCES	Health Care Experience Survey
HIV	Ontario HIV Database
HIVOHTN	Ontario HIV Treatment Network
HLINK	Health Links Datasets
HLINKSEL	Health Links for Southeast LHIN
HOBIC	Health Outcomes for Better Information and Care
HSU	High Service User
HYPER	Ontario Hypertension dataset
INST	Information about Ontario health care institutions funded by the Ministry of Health and Long-Term Care (MOHLTC)
IPDB	ICES Physician Database
LHIN	Local Health Integration Network
LOC	Levels of Care Classification System
MIS	Management Information System
MOMBABY	Linked Delivering Mother and Newborns
MOSHIP	McMaster Outcome Study of Hypertension in Pregnancy
NACRS	National Ambulatory Care Reporting System
NDFP	New Drug Funding Program
NMS	Narcotics Monitoring System
NPHS	National Population Health Survey

Short Title	Full Title
NRS	National Rehabilitation Reporting System
NSO	Newborn Screening Ontario
OBI	Ontario Brain Institute Crosswalk (Backbone linkage of OBI ID and IKN)
OBSP	Ontario Breast Screening Program
OCCC	Ontario Crohn's and Colitis Cohort dataset
OCCI	Ontario Case Costing Initiative
OCP	Ontario College of Pharmacists
OCR	Ontario Cancer Registry
ODB	Ontario Drug Benefit Claims
ODD	Ontario Diabetes Dataset
ODR	Organ Donor Registry
OHCAS	Ontario Home Care Administrative System
OHIP	Ontario Health Insurance Plan Claims Database
OHS	Ontario Health Study
OHSURVEY	Ontario Health Survey
OLIS	Ontario Laboratories Information System
OLISC19	OLIS COVID-19 Laboratory Data
OMHRS	Ontario Mental Health Reporting System
OMID	Ontario Myocardial Infarction Dataset
ONMARG	Ontario Marginalization Index
ORAD	Ontario Rheumatoid Arthritis Database
ORGD	Vital Statistics - Deaths
ORNGE	Ontario Patient Transport Database
ORRS	Ontario Renal Reporting System
OSR	Ontario Stroke Registry
OTR	Ontario Trauma Registry
PCAS	Primary Care Access Survey
PCCF	Postal Code Conversion File
PCPOP	Primary Care Population
PHYSNET	Ontario Multispecialty Physician Network dataset
PIBD	Ontario Paediatric Inflammatory Bowel Disease dataset
POGONIS	The Pediatric Oncology Group of Ontario Networked Information System
POP	Ontario Inter-censal Population Estimates and Projections

Short Title	Full Title
POPCAN	Canada Inter-censal Estimates
PROMS	Patient-reported outcome measures (PROMs) collection in Ontario
RAICA	Resident Assessment Instrument (RAI) - Contact Assessment
RAIHC	inter Resident Assessment Instrument (RAI) - Home Care
RAIHCMOH	Resident Assessment Instrument (RAI) - Home Care (MOHLTC)
RAIPC	inter Resident Assessment Instrument (RAI) - Palliative Care
REF	Reference Files (Look-up Tables)
RHRA	Retirement Homes Regulatory Authority
RPDB	Registered Persons Database
SDS	Same Day Surgery Database (Annual)
SURNAMES	Surname-based Ethnicity Group
TARGET	The Applied Research Group for Kids
TGLN	Trillium Gift of Life Network (Organ/Tissue Donation Ontario)
WTIS	Wait Time Information System

Appendix B

Administrative, Technical, and Physical Safeguards

Administrative	• Project-specific data cuts • All projects subject to privacy approval • Mandatory privacy and cybersecurity training • Confidentiality Agreements • Incident response process • Monthly awareness campaigns
Technical	• Secure portal with multi-factor authentication for electronic transfer of data to and from ICES, with network restrictions controlling connectivity • Data encrypted in transit • Segregation of operational and analytic environments • Segregation of analytic environment prevents communication to resources such as the Internet and those located in the operational network • Role-based access • Password-protected screensavers • Analytic environments accessible using multi-factor authentication and only through a “thin client” environment, restricting the ability to transfer data • Controls, including logging, of all transfers from the analytic environment • Threats (e.g., malicious and mobile code) detected using a defense in depth architecture that includes host, network and perimeter-based controls • TRAs routinely performed on material changes to the analytic environment • Vulnerability scans performed monthly on all assets in both the operational and analytic environments, and penetration tests performed annually.
Physical	• ID badges • Visitor access controls • Security zones, subject to role-based access • Locked offices • Security cameras 24/7/365 • “Glass break” detectors and “security windows” • Fireproof data safe • Emergency response service • Physical security patrols