EHR Privacy Auditing and Monitoring Policy

Policy Level Approval:	Chief Executive Officer
Policy Category:	Corporate Policy
Policy Number:	INF-011.02-P
Sensitivity Level:	Public
Policy Sponsor (or Sponsors):	Chief, Strategy, Planning, Privacy & Analytics
Original Date of Approval:	June 24, 2014
Date of Posting: This Policy is effective on the date of its posting14 or as otherwise noted in the Policy	July 22, 2025
Version Approval Date:	June 10, 2025
Next Scheduled Year Review (MM/YY):	28/29

1 Purpose, Objectives and Scope

1.1 Purpose

This Policy and its procedures address the following:

1.1.1 The process to be followed by Ontario Health (**OH**) as a Prescribed Organization (**PO**) in relation to continuously auditing and monitoring the electronic records the PO is required to keep of all instances where:

- All or part of the Personal Health Information (**PHI**) that is accessible by means of the Electronic Health Record (**EHR**) is viewed, handled or otherwise dealt with;
- In the event that a Health Information Custodian (**HIC**) has requested that the PO transmit to the HIC PHI that is accessible by means of the EHR, PHI is transmitted to the HIC by means of the EHR;
- A Consent Directive is made, withdrawn or modified; and,
- All or part of the PHI that is accessible by means of the EHR is Disclosed under section 55.7 of the *Personal Health Information Protection Act, 2004* (**PHIPA**) (Consent Override).

1.1.2 The responsibilities of HICs under whose authority PHI is Collected by means of the EHR (**Collecting HICs**) in relation to continuously auditing and monitoring their agents' Collection and Use of PHI that is accessible by means of the EHR;

1.1.3 The process to be followed by OH with respect to requests from the Information and Privacy Commissioner of Ontario (**IPC**) for the electronic records kept by OH in accordance with paragraphs 4, 5 and 6 of section 55.3 of PHIPA; and

1.1.4 The process to be followed by OH with respect to requests from HICs for the electronic records kept by OH in accordance with paragraphs 4, 5 and 6 of section 55.3 of PHIPA where the HIC requires the electronic records to audit and monitor its compliance with PHIPA.

1.2 Objectives

1.2.1 To enable OH and Collecting HICs to comply with PHIPA and Ontario Regulation 329/04 (**O. Reg. 329/04**).

1.2.2 To enable OH to comply with the requirements set out in the IPC's *Manual for the Review and Approval of Prescribed Organizations* (**IPC PO Manual**) in relation to auditing and monitoring the electronic records the PO is required to keep pursuant to paragraphs 4, 5 and 6 of section 55.3 of PHIPA, as required by paragraph 7 of section 55.3 of PHIPA.

1.2.3 To facilitate the identification and investigation of Privacy Incidents.

1.3 Scope

1.3.1 This Policy applies to non-union Employees, people leaders, board members, unionized Employees, secondees, consultants, other individuals acting on behalf of OH (**OH Agents**) and Collecting HICs.

1.3.2 OH's policies, procedures and practices with respect to the electronic record keeping requirements in paragraphs 4, 5 and 6 of section 55.3 of PHIPA are outside the scope of this Policy and are set out in the following documents:

- *Information Security Operations Standard*; and,
- *EHR Consent Directive and Consent Override Policy*.

1.3.3 OH's policy and procedure for privacy audits in respect of the following matters is set out in the *Privacy Audit and Compliance Policy*:

- Audits to assess compliance with OH's Privacy Policy Documents;
- Audits of the Employee(s) and other OH Agents permitted to Collect, Use, or Disclose PHI or PI; and
- Audits of the Employee(s) and other OH Agents permitted to Collect, Use, or Disclose PHI or PI that has been De-identified or Aggregated.

This *EHR Privacy Auditing and Monitoring Policy* sets out the policy and procedure for auditing and monitoring the electronic records the PO is required to keep pursuant to paragraphs 4, 5 and 6 of section 55.3 of PHIPA, as required by paragraph 7 of section 55.3 of PHIPA.

1.4 Compliance, Audit and Enforcement

1.4.1 Compliance with this Policy in its entirety is mandatory unless an exception to a specific section is approved by the Chief Privacy Officer (**CPO**) or delegate in writing. Failure to comply with the requirements of this Policy, without a written exception, may result in disciplinary action up to and including revocation of appointment, termination of employment or termination of contract without notice or compensation.

1.4.2 Compliance will be audited in accordance with and as per the frequency outlined in the *Privacy Audit and Compliance Policy*.

1.4.3 At the first reasonable opportunity upon identifying or becoming aware of a breach or a suspected breach of this Policy, Employees and other OH Agents, as well as Collecting HICs, must notify OH's Privacy Office by reporting the breach to the Enterprise Service Desk by Phone: 1-866-250-1554; or Email: oh-servicedesk@ontariohealth.ca

1.4.4 Breaches of this Policy will be managed in accordance with the *Privacy Incident Management Policy and Procedure* and the *EHR Privacy Incident Management Policy and Procedure*, as applicable.

1.4.5 Compliance will be enforced in accordance with the *Progressive Discipline Policy*.

1.5 Terminology

1.5.1 The words "include" and "including" when used are not intended to be exclusive and mean, respectively, "include, without limitation," and "including, but not limited to".

1.5.2 Words and terms in this Policy that have meanings differing from the commonly accepted definitions are capitalized and their meanings are set out in the Definition and Acronyms section (Section 6).

2 Policies

2.1.1 PHIPA requires OH to implement safeguards to protect the integrity, security and confidentiality of the PHI that is accessible by means of the EHR, including protection against unauthorized Collection, Use or Disclosure of the PHI that is accessible by means of the EHR.

2.1.2 OH responds to requests from HICs pursuant to paragraph 9 of section 55.3 of PHIPA related to records the PO is required to keep pursuant to paragraph 4, 5 and 6 of section 55.3 of PHIPA, OH has a program and tools in place to enable OH to satisfy its auditing and monitoring requirements under PHIPA, applicable agreements, and this Policy and its procedures.

2.1.3 OH has in place and maintains policies, procedures and practices in respect of privacy and security that are necessary to enable OH to comply with its obligations under PHIPA, applicable agreements and this Policy and its procedures. OH takes steps that are reasonable in the circumstances to ensure their agents and Electronic Service Providers comply with PHIPA, applicable agreements, and this Policy and its procedures.

2.1.4 Collecting HICs must have in place and maintain policies, procedures and practices in respect of privacy and security that are necessary to enable them to comply with their obligations under PHIPA, applicable agreements and this Policy and its procedures. Collecting HICs must take steps that are reasonable in the circumstances to ensure their agents and Electronic Service Providers comply with PHIPA, applicable agreements, and this Policy and its procedures.

2.2 Electronic Record Keeping by OH

2.2.1 As required by paragraphs 4, 5 and 6 of section 55.3 of PHIPA, OH keeps an electronic record of all instances where:

- All or part of the PHI that is accessible by means of the EHR is viewed, handled or otherwise dealt with;
- A HIC has requested that the PO transmit to the HIC PHI that is accessible by means of the EHR and PHI is transmitted to the HIC by means of the EHR;
- A Consent Directive is made, withdrawn or modified; and
- All or part of the PHI that is accessible by means of the EHR is Disclosed under section 55.7 of PHIPA (Consent Override).

The electronic record keeping requirements set out above are further addressed in the *Information Security Operations Standard* and *EHR Consent Directive and Consent Override Policy*.

2.2.2 OH ensures that the electronic records it is required to keep are securely retained, transferred and disposed of in a manner than enables compliance with PHIPA, the *EHR Retention Policy* and the *Electronic Health Record Information Security Policy* and its associated procedures.

2.3 Auditing and Monitoring by OH

2.3.1 OH audits and monitors the electronic records that it is required to keep under paragraphs 4, 5, and 6 of section 55.3 of PHIPA[1] to ensure compliance with PHIPA, the IPC Manual, applicable agreements, and the policies, procedures and practices implemented by OH with respect to the EHR. OH's auditing and monitoring is:

- In accordance with auditing and monitoring criteria (i.e., threat scenarios) that enable HICs and OH to comply with their obligations under PHIPA, applicable agreements and the policies, procedures and practices implemented in respect of the EHR;
- Consistent with industry standards and good practices;
- Based on an assessment of the threats and risks posed to PHI that is accessible by means of the EHR; and
- Where applicable, in accordance with the security auditing and monitoring requirements specified in the *Information Security Risk Management Standard* and *Information Security Operations Standard.*

2.3.2 OH continually monitors and audits the electronic record of all instances where a Consent Directive is made, withdrawn or modified to ensure that the Consent Directive continues to apply as requested, by conducting the following:

- Reviewing each request for Consent Directive that is received;
- Auditing and testing all Consent Directives after implementation;
- Regularly conducting health system checks on the consent management technology to ensure the continuity of service;
- Conducting ongoing targeted (reactive) and random (proactive) auditing in accordance with this Policy.

2.3.3 OH conducts ongoing targeted (reactive) and random (proactive) auditing and monitoring of the electronic records OH is required to keep under paragraphs 4, 5, and 6 of section 55.3 of PHIPA.

2.3.4 OH conducts targeted auditing and monitoring in response to requests or complaints from individuals regarding the Collection, Use or Disclosure of their PHI by means of the EHR, and whenever a Privacy Incident is identified.

2.3.5 OH maintains a log of all audits conducted on the electronic records it is required to keep pursuant to paragraphs 5 and 6 of section 55.3 of PHIPA of Consent Directives and Consent Overrides in accordance with the requirements set out in Appendix "A" of the *EHR Consent Directive and Consent Override Policy*.

2.3.6 Where the investigation of an auditing or monitoring alert leads to the identification of a Privacy Incident, OH follows the *Privacy Incident Management Policy and Procedure* and the *EHR Privacy Incident Management Policy and Procedure*, as applicable.

[1] As required by paragraph 7 of section 55.3 of PHIPA.

2.4 Auditing and Monitoring by Collecting HICs

2.4.1 Collecting HICs must conduct the auditing and monitoring activities described in this section to ensure compliance of their agents and service providers with PHIPA, applicable agreements, and the policies, procedures and practices implemented in respect of the EHR.

2.4.2 Collecting HICs must audit and monitor all instances where:

- All or part of the PHI in the EHR is viewed, handled or otherwise dealt with by the HIC or its agents or Electronic Service Providers;
- The Collecting HIC has requested that OH as a PO transmit to the Collecting HIC PHI that is accessible by means of the EHR, and PHI is then transmitted to the Collecting HIC by means of the EHR; and
- All or part of the PHI that is accessible by means of the EHR is Disclosed to the Collecting HIC or its agents under section 55.7 of PHIPA (Consent Override).

2.4.3 Collecting HICs must conduct random auditing and monitoring of all Collections, Uses and Disclosures of PHI by their agents that is in accordance with IPC decisions and guidance.

2.4.4 Collecting HICs must conduct targeted auditing and monitoring in response to requests or complaints from individuals regarding the Collection, Use or Disclosure of their PHI by means of the EHR, and whenever a Privacy Incident is identified.

2.4.5 Where an audit by a Collecting HIC leads to the identification of a Privacy Incident, the Collecting HIC must notify OH of the Privacy Incident at the first reasonable opportunity and manage the Privacy Incident in accordance with the *EHR Privacy Incident Management Policy and Procedure*.

2.5 Requests from the IPC for the Electronic Records kept by OH pursuant to paragraphs 4, 5 and 6 of section 55.3 of PHIPA

2.5.1 In accordance with paragraph 8 of section 55.3 of PHIPA, upon the request of the IPC, OH must provide to the IPC for the purposes of Part V.1 of PHIPA, the electronic records kept by OH pursuant to paragraphs 4, 5, and 6 of section 55.3 of PHIPA, as listed in section 2.2.1 of this Policy.

2.6 Requests from HICs for the Electronic Records kept by OH pursuant to paragraphs 4, 5 and 6 of section 55.3 of PHIPA

2.6.1 In accordance with paragraph 9 of section 55.3 of PHIPA, upon the request of a HIC that requires the electronic records to audit and monitor its compliance with PHIPA, OH provides to the HIC or an agent acting on the HIC's behalf, the records kept by OH pursuant to paragraphs 4, 5, and 6 section 55.3 of PHIPA, as listed in section 2.2.1 of this Policy.

3 Process for Privacy Audits of the Electronic Records

3.1 Proactive (Random) Privacy Audits of the Electronic Records

3.1.1 OH conducts automated continuous proactive monitoring of the electronic records OH is required to keep as a PO through privacy information and event management solutions. If an alert is generated through these solutions it is managed in accordance with the process set out in section 3.3 of this Policy.

3.1.2 In addition to the auditing identified in section 3.1.1, the CPO or delegate is responsible for assigning Designated OH Agent to conduct manual random proactive privacy audits of the electronic records OH is required to keep as a PO and determining the parameters of the random audit. The CPO maintains a schedule for auditing and monitoring of these records. OH conducts manual proactive, random audits of EHR at a minimum, annually.

3.1.3 Upon being assigned by the CPO or delegate to conduct a random privacy audit, the Designated OH Agent contacts Application Management Support, Product Management, and/or SQL Operations, as applicable, in the Digital Excellence in Health Portfolio and requests the relevant electronic records kept by OH pursuant to paragraph 4, 5 and 6 of section 55.3 of PHIPA in accordance with the parameters determined by the CPO or delegate.

3.1.4 Upon request from the Designated OH Agent, Application Management Support, Product Management, and/or SQL Operations is responsible for preparing and providing the electronic records to the Designated Member of the Privacy Team as soon as reasonably possible.

3.1.5 Upon receipt of the relevant electronic records, the Designated OH Agent is responsible for working with the relevant manager or people lead to conduct a review of the electronic records and preparing and submitting a report of the audit results to the CPO or delegate for review and consideration.

3.1.6 At the earliest opportunity, and no later than 2 business days after the Designated OH Agent completes the audit, the Designated Member of the Privacy Team provides a report of the audit results and any recommendations to the CPO or delegate and save the report and any related documentation in the secure drive.

3.1.7 Where the audit leads to the identification of a Privacy Incident, the Designated Member of the Privacy Team is responsible for managing the Privacy Incident in accordance with the *EHR Privacy Incident Management Policy and Procedure*.

3.1.8 The CPO or delegate is responsible for ensuring that all audits are documented in accordance with this Policy and ensuring that audit-related documentation is retained in accordance with the *EHR Retention Policy*.

3.2 Reactive (Targeted) Privacy Audits of the Electronic Records

3.2.1 Where OH receives an EHR Privacy Inquiry or EHR Privacy Complaint from an individual regarding the Collection, Use or Disclosure of their PHI by means of the EHR, the CPO or delegate is responsible for assigning a Designated Member of the Privacy Team to conduct a targeted audit of the related electronic records kept by OH as PO if required as part of the incident, inquiry or complaint investigation.

3.2.2 The Designated Member of the Privacy Team contacts Application Management Support, Product Management, and/or SQL Operations, as applicable, to request the relevant electronic records kept by OH pursuant to paragraph 4, 5 and 6 of section 55.3 of PHIPA.

3.2.3 Upon request from the Designated Member of the Privacy Team, Application Management Support, Product Management, and/or SQL Operations is responsible for preparing and providing the electronic records to the Designated Member of the Privacy Team as soon as reasonably possible.

3.2.4 Upon receipt of the relevant electronic records, the Designated Member of the Privacy Team is responsible for conducting a detailed review of the electronic records and preparing and submitting a report of the audit results to the CPO or delegate for review and consideration.

3.2.5 At the earliest opportunity, and no later than 2 business days after the Designated Member of the Privacy Team completes the audit, the Designated Member of the Privacy Team provides a report of the audit results and any recommendations to the CPO or delegate and save the report and any related documentation in the secure drive.

3.2.6 Where the audit leads to the identification of a Privacy Incident, the Designated Member of the Privacy Team is responsible for managing the Privacy Incident in accordance with the *EHR Privacy Incident Management Policy and Procedure*.

3.2.7 The CPO or delegate is responsible for ensuring that all targeted audits are documented in accordance with this Policy and ensuring that audit-related documentation is retained in accordance with the *EHR Retention Policy*.

3.3 Targeted Privacy Audits as a result of Monitoring Alerts

3.3.1 Where the Privacy Office receives an auditing and monitoring alert (i.e. an audit report triggered by OH's electronic monitoring of the electronic records through pre-determined threat scenarios), the CPO or delegate is responsible for assigning a Designated Member of the Privacy Team to conduct a detailed review of the relevant electronic records to determine if a Privacy Incident has occurred.

3.3.2 If the audit event relates to the activities of a HIC or a HIC's agent, the Designated Member of the Privacy Team completes an initial review of the audit report, and if appropriate, is responsible for providing the audit report to the relevant HIC for further review.

3.3.3 The relevant HIC is responsible for reviewing the audit report and notifying the OH Privacy Office at the first reasonable opportunity if a Privacy Incident is identified. Privacy Incidents will be managed in accordance with the *EHR Privacy Incident Management Policy and Procedure.*

3.3.4 If the audit event relates to the activities of OH, an OH Agent, or an unauthorized third party that is not a HIC, OH reviews the audit report. If upon review of the audit report a Privacy Incident is identified, the Privacy Incident will be handled in accordance with OH's *Privacy Incident Management Policy and Procedure*.

3.4 Logging Audits of Electronic Records of Consent Directives and Consent Overrides

3.4.1 Where an audit is conducted on the electronic records OH is required to maintain of Consent Directives and Consent Overrides pursuant to paragraphs 5 and 6 of section 55.3 of PHIPA, the Designated Member of the Privacy Team logs the audit in accordance with the requirements set out in Appendix "A" to the *EHR Consent Directive and Consent Override Policy*.

4 Process for Responding to Requests for Electronic Records kept by OH

4.1 Requests from the IPC for Electronic Records kept by OH

4.1.0 This section sets out the process that is followed by OH in responding to requests from the IPC pursuant to paragraph 8 of section 55.3 of PHIPA for the electronic records that OH is required to keep pursuant to paragraphs 4, 5, and 6 of section 55.3 of PHIPA.[2]

4.1.1 Upon receipt of a request from the IPC for electronic records kept by OH, the CPO or delegate is responsible for assigning Designated Members of the Privacy Team to manage the request in accordance with the responsibilities assigned in this Policy.

4.1.2 The Designated Member of the Privacy Team is responsible for receiving requests for electronic records from the IPC, recording each request in the tracking log in accordance with the requirements set out in Appendix "A," and saving documentation related to the request in the secure drive.

4.1.3 Upon request from the Designated Member of the Privacy Team, Application Management Support and/or Product Management is responsible for preparing the electronic records requested by the IPC and providing the electronic records to the Designated Member of the Privacy Team as soon as reasonably possible.

4.1.4 The Designated Member of the Privacy Team is responsible for reviewing the electronic records to confirm that they are responsive to the IPC's request and providing the electronic records to the CPO or delegate for further review and approval.

4.1.5 The CPO or delegate is responsible for reviewing the electronic records to ensure that they are responsive to the IPC's request and include the content required pursuant to PHIPA and must provide approval before the records are sent to the IPC.

4.1.6 Prior to providing the electronic records to the IPC, the CPO or delegate notifies the HIC(s) that are named in the electronic records, or whose agent or Electronic Service Provider is named in the electronic records, that OH will be providing the electronic records to the IPC.

4.1.7 The CPO or delegate is responsible for providing the requested information to the IPC as soon as reasonably possible. The electronic records must be in written form and provided to the IPC by the means specified by the IPC.

---

[2] The process for responding to requests from the IPC and HICs for the electronic records kept by OH pursuant to paragraphs 5 and 6 of section 55.3 of PHIPA is also addressed in the *EHR Consent Directive and Consent Override Policy*.

4.2 Requests from HICs for Electronic Records kept by OH

4.2.1 This section sets out the process that is followed by OH in responding to requests from HICs pursuant to paragraph 9 of section 55.3 of PHIPA for the electronic records that OH is required to keep pursuant to paragraphs 4, 5, and 6 of section 55.3 of PHIPA.[3]

4.2.2 Upon receipt of a request from a HIC for the electronic records kept by OH, the CPO or delegate is responsible for assigning Designated Members of the Privacy Team to manage the request in accordance with the responsibilities assigned in this Policy.

4.2.3 The Designated Member of the Privacy Team is responsible for receiving requests for electronic records from HICs, recording each request in the tracking log in accordance with the requirements set out in Appendix "B," and saving documentation related to the request in the secure drive.

4.2.4 The Designated Member of the Privacy Team is responsible for contacting Application Management Support and/or Product Management to prepare the electronic records requested by the HIC.

4.2.5 Upon request from the Designated Member of the Privacy Team, Application Management Support and/or Product Management is responsible for preparing the electronic records requested by the HIC, and providing the electronic records to the Designated Member of the Privacy Team as soon as reasonably possible.

4.2.6 The Designated Member of the Privacy Team is responsible for reviewing the electronic records to ensure that they are responsive to the HIC's request and include the content required in accordance with PHIPA.

4.2.7 The Designated Member of the Privacy Team is responsible for providing the requested information to the HIC. As soon as reasonably possible but no later than 14 business days, Privacy Operations provides the electronic records to the HIC either as an encrypted document sent by email or make the electronic records available to the HIC through a secure portal.

4.2.8 The Designated Member of the Privacy Team is responsible for recording the request in the tracking log in accordance with the requirements set out in Appendix "B" and saving documentation related to the request in the secure drive.

5 Responsibilities

5.1 Chief Privacy Officer or delegate

5.1.1 Responsible for assigning Designated Members of the Privacy Team to conduct audits.

5.1.2 Responsible for receiving and reviewing audit reports prepared by Designated Members of the Privacy Team.

[3] The process for responding to requests from the IPC and HICs for the electronic records kept by OH pursuant to paragraphs 5 and 6 of section 55.3 of PHIPA is also addressed in the *EHR Consent Directive and Consent Override Policy*.

5.1.3 Responsible for ensuring that all audits are documented in accordance with this Policy, and that audit-related documentation is retained in accordance with the *EHR Retention Policy*.

5.1.4 Responsible for reviewing the electronic records to ensure that they are responsive to the IPC's request and include the content required pursuant to PHIPA and approving and sending the electronic records to the IPC.

5.2 Employees and Other OH Agents

5.2.1 Where assigned by the CPO or delegate, Designated Members of the Privacy Team are responsible for conducting audits in accordance with this Policy.

5.2.2 Designated Members of the Privacy Team are responsible for receiving requests for electronic records from HICs and the IPC and responding to such requests in accordance with this Policy.

5.2.3 Upon request, Application Management Support, Product Management, and/or SQL Operations in the Digital Excellence in Health Portfolio are responsible for preparing and providing the electronic records to the Designated Members of the Privacy Team as soon as reasonably possible in accordance with this Policy.

5.3 Collecting HICs

5.3.1 Responsible for conducting auditing and monitoring in accordance with this Policy.

6 Definitions and Acronyms

Defined terms are capitalized throughout this document.

Term / Acronym	Definition
CEO	Chief Executive Officer
Collect	Has the meaning set out in section 2 of PHIPA with respect to PHI; and in respect of PI has the same meaning. "Collect" means to gather, acquire, receive, or obtain the information by any means from any source, and "Collection" and "Collected" has a corresponding meaning.
Collecting HIC	A HIC under whose authority PHI is Collected by means of the EHR.
Consent Directive	Means a directive, made in accordance with s. 55.6 of PHIPA, that withholds or withdraws, in whole or in part, an individual's consent to the Collection, Use and Disclosure of their PHI by means of the EHR by a HIC for the purposes of providing or assisting in the provision of health care to the individual.
Consent Override	Means the permitted Disclosures described in section 55.7 of PHIPA.

CPO	Chief Privacy Officer
Disclose	Has the meaning set out in s. 2 of PHIPA with respect to PHI in the control of a HIC or a person; and in respect of PI has the same meaning. "Disclose" means to make the information available or to release it to another HIC or to another person, but does not include to Use the information, and "Disclosure" has a corresponding meaning.
EHR or Electronic Health Record	Has the meaning set out in s. 55.1 of PHIPA and generally means the electronic systems that are developed and maintained by OH pursuant to Part V.1 of PHIPA for the purpose of enabling HICs to Collect, Use and Disclose PHI by means of the systems.
EHR Privacy Complaint	Concerns or complaints related to compliance of a HIC or OH with the privacy policies, procedures, and practices implemented by the PO or with PHIPA and its regulations in respect of PHI that is accessible by means of the EHR developed or maintained by OH.
EHR Privacy Inquiry	Inquiries related to compliance of a HIC or OH with the privacy policies, procedures, and practices implemented by the PO or with PHIPA and its regulations in respect of PHI that is accessible by means of the EHR developed or maintained by OH and the privacy policies, procedures and practices put in place by HICs or OH in relation to PHI that is accessible by means of the EHR developed or maintained by OH.
Electronic Service Provider	A Third-Party Service Provider contracted or otherwise engaged to provide services for the purpose of enabling the use of electronic means to Collect, Use, modify, Disclose, retain or dispose of records of PHI.
Employee	A person employed and compensated by OH as an Employee, and is classified as either permanent full-time, permanent part-time, temporary full-time, temporary part-time, paid student or casual, as set out in the *Employee Classification Guideline*. A consultant or contractor is not an Employee.
End User	An individual or organization that uses the EHR developed or maintained by Ontario Health.
HIC or Health Information Custodian	Has the meaning set out in s. 3 of PHIPA and generally means a person or organization that has custody or control of personal health information for the purpose of health care or other health-related duties. Examples include physicians, hospitals, pharmacies, laboratories and the MOH, but does not include OH.
IPC	Information and Privacy Commissioner of Ontario
IPC PO Manual	IPC Manual for the Review and Approval of Prescribed Organizations
Minister	Minister of Health
OH	Ontario Health, the agency of the Government of Ontario to which this Policy applies.

OH Agent	A person that acts for or on behalf of OH for the purposes of OH, and not for the Agent's own purposes, whether or not the Agent has the authority to bind OH, whether or not the Agent is employed by OH, and whether or not the Agent is being remunerated.
O. Reg. 329/04	Ontario Regulation 329/04 made under PHIPA
PHI or Personal Health Information	Has the meaning set out in section 4 of PHIPA. Specifically, it is "identifying information" in oral or recorded form about an individual that: • Relates to the physical or mental health of the individual, including information that consists of the health history of the individual's family; • Relates to the provision of health care to the individual, including the identification of a person as a provider of health care to the individual; • Is a plan that sets out the home and community care services for the individual to be provided by a health service provider or Ontario Health Team pursuant to funding under section 21 of the Connecting Care Act, 2019; • Relates to payments or eligibility for health care or eligibility for coverage for health care in respect of the individual; • Relates to the donation by the individual of any body part or bodily substance of the individual or that is derived from the testing or examination of any such body part or bodily substance; • Is the individual's health number; and/or • Identifies an individual's substitute decision-maker. PHI also includes identifying information about an individual that is not PHI listed above but that is contained in a record that includes PHI listed above. Information is "identifying" when it identifies an individual or when it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify the individual.
PHIPA or *Personal Health Information Protection Act, 2004*	The Ontario health privacy law. It establishes rules for the management of PHI and the protection of the confidentiality of that information, while facilitating the effective delivery of healthcare services. References to PHIPA include the regulation made thereunder, as may be amended or replaced from time to time.
Prescribed Organization or PO	The organization prescribed in Ontario Regulation 329/04 as the organization for the purposes of Part V.1 of PHIPA. The Prescribed Organization has the power and the duty to develop and maintain the EHR in accordance with Part V.1 of PHIPA and the regulations made thereunder.

Privacy Breach	A Privacy Breach includes: 1) Privacy Breach of PHI or PI (Privacy PHI/PI Breach) means an event where: • The Collection, Use, or Disclosure of PHI or PI is not in compliance with PHIPA or its regulation, or with FIPPA or its regulations (i.e., without legal authority); and/or • The Viewing, handling or otherwise dealing with PHI provided to OH is not in compliance with PHIPA, or its regulation; • PHI or PI is stolen, lost or subject to unauthorized Collection, Use or Disclosure or where records of PHI or PI are subject to unauthorized copying, modification, or disposal. **Note:** A Privacy PHI/PI Breach does not include a breach of De-identified Information, or Business Identity Information, if the event does involve PI or PHI. 2) Privacy Breach of Privacy Policy or Agreement (Privacy Policy/Agreement Breach) means an event where: • There is a contravention of OH's privacy policies, procedures, or practices; and/or • There is a contravention of a privacy-related[4] term or condition in a: ○ data sharing agreements, ○ research agreements, ○ confidentiality agreements, or, ○ agreements with third-party service providers retained by OH to handle PHI or PI, ○ written acknowledgements acknowledging and agreeing not to use PHI or PI which has been de-identified and/or aggregated, to identify an individual; and • Does not include a privacy breach of PHI or PI **Note:** A Privacy Policy/Agreement Breach may include a breach that involves De-identified Information or Business Identity Information, if the breach relates to privacy controls in an agreement or a privacy policy, procedure or practice related to handling of De-identified Information or Business Identity Information.
Privacy Incident	Any event where the Privacy Office is notified or becomes aware that a Privacy Breach may have occurred. This includes events that are reviewed/investigated and: 1. confirmed to be a Privacy Breach 2. confirmed not to be a Privacy Breach 3. it cannot or has not been determined if a Privacy Breach occurred (Suspected Privacy Breach).

[4] A privacy-related term or condition, includes terms or conditions that relate to privacy requirements from law (including, for example, FIPPA, PHIPA and GOLA), the IPC PP/PE Manual, the IPC PO Manual, IPC guidelines and orders, OH's privacy information practices or other controls to protect the privacy of individuals or the confidentiality of their PI and PHI.

	Note: Privacy Incidents include events involving PI and PHI, as well as De-identified Information and Business Identity Information as these events require investigation in accordance with this Policy to confirm if they are Privacy Breaches as defined below. OH shall investigate these incidents involving De-identified Data and Business Identity Information, considering factors such as the 1) risk of re-identification and related de-identification guidelines for De-identified Data, as well as 2) the context for handling data that OH received as Business Identity Information, to confirm that it does not constitute PI, respectively.
Third-Party Service Provider	A third-party contracted or otherwise engaged to provide services, including Electronic Service Providers.

7 Review Cycle

This Policy is to be reviewed by Ontario Health at least within 3 years of its effective date or earlier if required in accordance with the *Privacy Audit and Compliance Policy.*

8 References and/or Key Implementation Documents

- PHIPA and O. Reg. 329/04
- IPC PO Manual
- EHR Consent Directive and Consent Override Policy
- EHR Privacy Incident Management Policy and Procedure
- EHR Retention Policy
- Privacy Incident Management Policy and Procedure
- Privacy Audit and Compliance Policy
- Information Security Operations Standard
- Information Security Risk Management Standard

9 Appendices

- Appendix “A”: Minimum Content Required in Log of Requests for Electronic Records from the IPC
- Appendix “B”: Minimum Content Required in Log of Requests for Electronic Records from HICs

10 Policy Consultations

The following were consulted in the development of this Policy:

- Staff from the Privacy Office and other OH Agents responsible for drafting, maintaining, and/or reviewing the privacy policies in reference to OH's privacy requirements; and
- Working Group members of the Privacy Program Advisory Committee (version 1 of Policy)

11 Policy Review History

Date of Review MM/YYYY	Itemize section changed and description of change (if no changes made, indicate N/A	New policy number	Date of Approval DD/MM/YYYY	Approver
1/7/2025	• Updated IT contact information. • Updated roles and responsibilities to reflect changes in organizational structure. • Added/edited information throughout Policy as per the updated IPC Manuals; • Revised definitions of Personal Health Information, Personal Information, Privacy Breach, and Privacy Incident • Updated compliance will be enforced in accordance with the *Progressive Discipline Policy*	INF-011.02-P	10/06/2025	CEO

12 Policy Repeal

1) Date of Repeal:
2) Reason for Repeal:
3) Date of Approval of Repeal:
4) Approver:

Appendix A: Content for Log of Requests for Electronic Records from the IPC

OH maintains a log of the electronic records that are provided to the IPC pursuant to paragraph 8 of s. 55.3 of PHIPA.

For each request for electronic records received from the IPC, the log sets out the following:

- The employee(s) or other OH Agent(s) who received the request for electronic records;
- The date the request was received;
- The employee(s) or other person(s) acting on behalf of the IPC who submitted the request;
- The types of electronic records that were requested by the IPC;
- The employee(s) or other OH Agent(s) who responded to the request;
- The types of electronic records that were provided to the IPC;
- The employee(s) or other person(s) acting on behalf of the IPC to whom the electronic records were provided;
- The form in which the electronic records were provided to the IPC;
- The manner in which the electronic records were provided to the IPC; and
- The date when the electronic records were provided to the IPC.

Appendix B: Content of Log of Requests for Electronic Records from HICs

OH maintains a log of the electronic records that are provided to HICs pursuant to paragraph 9 of s. 55.3 of PHIPA.

For each request for electronic records received from a HIC, the log sets out the following:

- The Employee(s) or other OH Agent(s) who received the request for electronic records;
- The date the request for electronic records was received by OH;
- The HIC who made the request for electronic records;
- The types of electronic records that were requested by the HIC;
- The employee(s) or other OH Agent(s) who responded to the request;
- The types of electronic records that were provided to the HIC;
- The agent of the HIC to whom the electronic records were provided;
- The form the electronic records were provided to the HIC;
- The manner the electronic records were provided to the HIC; and
- The date the electronic records were provided to the HIC.