



**Ontario  
Health**

## **EHR Inquiries and Complaints Policy and Procedures**

<b>Policy Level Approval:</b>	Chief Executive Officer
<b>Policy Category:</b>	Corporate Policy
<b>Policy Number:</b>	INF-004.02-PP
<b>Sensitivity Level:</b>	Public
<b>Policy Sponsor (or Sponsors):</b>	Chief, Strategy, Planning, Privacy & Analytics
<b>Original Date of Approval:</b>	June 26, 2014
<b>Date of Posting:</b> This Policy is effective on the date of its posting or as otherwise noted in the Policy	July 22, 2025
<b>Version Approval Date:</b>	June 10, 2025
<b>Next Scheduled Year Review (MM/YY):</b>	28/29

### **Copyright Notice**

Copyright © 2021, Ontario Health

### **All rights reserved**

No part of this document may be reproduced in any form, including photocopying or transmission electronically to any computer, without prior written consent of Ontario Health. The information contained in this document is proprietary to Ontario Health and may not be used or disclosed except as expressly authorized in writing by Ontario Health.

### **Trademarks**

Other product names mentioned in this document may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

# 1 Purpose, Objectives, and Scope

---

## 1.1 Purpose

- 1.2.1 This Policy and its procedures address the process to be followed in receiving, documenting, tracking, and responding to EHR Privacy Inquiries and EHR Privacy Complaints in respect of Personal Health Information (PHI) that is accessible by means of the Electronic Health Record (EHR) developed or maintained by Ontario Health (OH).

## 1.2 Objectives

- 1.2.2 To support an individual in exercising their right to make an EHR Privacy Inquiry or EHR Privacy Complaint in respect of the EHR developed or maintained by OH.
- 1.2.3 To enable Health Information Custodians (**HICs**) and OH to meet their obligations under the *Personal Health Information Protection Act, 2004 (PHIPA)* and its regulations in relation to EHR Privacy Inquiries and EHR Privacy Complaints in respect of the EHR developed or maintained by OH.
- 1.2.4 This Policy and its procedures support OH's management of EHR Privacy Inquiries and EHR Privacy Complaints in compliance with the requirements set out in the Information and Privacy Commissioner's (**IPC**) *Manual for the Review and Approval of Prescribed Organizations (IPC PO Manual)*.

## 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 HICs who access or contribute PHI that is accessible by means of the EHR.
- 1.3.2 This Policy and its procedures apply to Privacy Inquiries and Privacy Complaints in respect of PHI accessible by means of the EHR developed or maintained by OH. For more information on the scope of the EHR, please see the [EHR Plain Language Description and List of Repositories](#).
- 1.3.3 OH's *Privacy Complaints and Inquiries Policy and Procedures* complements this Policy and assists OH Employees and other OH Agents in managing all Privacy Inquiries and Privacy Complaints relating to OH.

## 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 of this Policy, employees, or other OH Agents, as well as HICs must notify OH's Privacy Office by reporting the breach to 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*.
- 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 5).

## 2 Policy

---

### 2.1 General

- 2.1.1 OH will handle real and suspected Privacy Breaches identified during the investigation of an EHR Privacy Inquiry or an EHR Privacy Complaint in accordance with the *Privacy Incident Management Policy and Procedure* or *EHR Privacy Incident Management Policy and Procedure*, as applicable.
- 2.1.2 PHIPA requires a HIC that is not an individual, such as a HIC that is a corporation or partnership, to designate a contact person to respond to Privacy Inquiries about the HIC's information practices, to receive Privacy Complaints about the HIC's alleged contravention of PHIPA and to ensure all agents of the HIC are appropriately informed of their duties under PHIPA.
- 2.1.3 PHIPA permits a HIC that is an individual to designate a contact person to respond to Privacy Inquiries about the HIC's information practices, to receive Privacy Complaints about the HIC's alleged contravention of PHIPA and to ensure all agents of the HIC are appropriately informed of their duties under PHIPA. Where a HIC that is an individual does not designate a contact person to perform these functions, the HIC is required to perform these functions on their own.
- 2.1.4 An individual who has reasonable grounds to believe that a HIC, OH or one of their agents or Electronic Service Providers (**ESP**) has contravened or is about to contravene PHIPA may also make a complaint to the IPC.
- 2.1.5 This Policy and its procedures will support an individual in exercising their right to make an EHR Privacy Inquiry or EHR Privacy Complaint and will enable HICs and OH to meet their obligations under PHIPA in this regard.
- 2.1.6 HICs and OH has 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 associated procedures.

- 2.1.7 HICs and OH have in place and maintain policies, procedures and practices in respect of privacy and security that comply with PHIPA and inform their agents and ESPs on the policies, procedures and practices as required by PHIPA.
- 2.1.8 OH has a program in place to enable HICs and OH to satisfy their obligations in receiving, documenting, tracking, addressing and responding to EHR Privacy Inquiries and EHR Privacy Complaints in respect of PHI accessible by means of the EHR developed or maintained by OH that is in accordance with PHIPA, applicable agreements, and this Policy.
- 2.1.9 Where OH directly receives a Privacy Inquiry or Privacy Complaint related solely to OH or an unauthorized person, OH receives, document, track, address and respond directly to the individual making the Privacy Inquiry or Privacy Complaint as soon as possible, but in any event no later than 30 calendar days following receipt of the Privacy Inquiry or Privacy Complaint by OH, in accordance with the *Privacy Complaints and Inquiries Policy and Procedures* and this Policy, as applicable.

## 3 Procedures

---

### 3.1 How to make an EHR Privacy Inquiry or EHR Privacy Complaint

- 3.1.1 Individuals may direct EHR Privacy Inquiries and EHR Privacy Complaints directly to OH where the inquiry, concern or complaint is related to:
  - The compliance of a HIC or OH 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.
- 3.1.2 EHR Privacy Inquiries and EHR Privacy Complaints may be made directly to OH verbally or in writing. Individuals should include their contact information, including their name, mailing address, phone number or email address if they would like OH to respond to their inquiry, concern, or complaint.
- 3.1.3 EHR Privacy Inquiries and EHR Privacy Complaints may be directed to OH's CPO in the following manner:

**Email:** [privacy@ontariohealth.ca](mailto:privacy@ontariohealth.ca)

**Phone:** 1-877-280-8538

**Mail:**

Chief Privacy Officer  
525 University Avenue, 5th Floor  
Toronto, ON M5G 2L3
- 3.1.4 Individuals may direct Privacy Complaints regarding the compliance of OH or one or more HICs who Collect, Use or Disclose PHI by means of the EHR with PHIPA and its regulations to the IPC.

3.1.5 The mailing address and contact information for the IPC is as follows:

**Mail:** Registrar  
Information and Privacy Commissioner of Ontario  
2 Bloor Street East, Suite 1400  
Toronto, ON M4W 1A8

**Email:** info@ipc.on.ca

**Telephone: Toronto Area:** 416-326-3333

**Toll Free:** 1-800-387-0073

**TDD/TTY:** 416-325-7539

3.1.6 The OH website includes a privacy page with the mailing address, email address, telephone, and fax number to which individuals may direct an EHR Privacy Inquiry or EHR Privacy Complaint to OH, as well as contact information for the IPC.

3.1.7 Individuals may obtain further information about the privacy policies, procedures and practices put in place by OH by visiting OH's website.

3.1.8 Individuals may obtain further information about the privacy policies, procedures and practices put in place by HICs that contribute PHI to the EHR or HICs that Collect PHI accessible by means of the EHR by contacting the HIC directly.

## **3.2 Process for Receiving EHR Privacy Inquiries and EHR Privacy Complaints**

3.2.1 OH's Privacy Office acts as the first point of contact for responding to EHR Privacy Inquiries and EHR Privacy Complaints.

3.2.2 Any Employee or other OH Agent that directly receives an EHR Privacy Inquiry or EHR Privacy Complaint must immediately forward the EHR Privacy Inquiry or EHR Privacy Complaint to OH's Privacy Office.

3.2.3 Once an EHR Privacy Inquiry or EHR Privacy Complaint is received by the Privacy Office, the CPO or delegate is responsible for designating a member of the Privacy team ("Designated Member of the Privacy Team") to document, track, investigate and respond to the EHR Privacy Inquiry or EHR Privacy Complaint, as applicable.

3.2.4 Information requested from the individual making an EHR Privacy Inquiry or EHR Privacy Complaint may include their name and contact information, including their mailing address, phone number or email address, if the individual would like OH to respond to their inquiry, concern, or complaint.

3.2.5 OH may request additional information and/or documentation (e.g. privacy complaint form) from an Individual where reasonably necessary for the purposes of receiving and responding to an EHR Privacy Inquiry or an EHR Privacy Complaint.

## **3.3 Procedures related to EHR Privacy Inquiries**

3.3.1 The Designated Member of the Privacy Team as soon as possible, reviews the EHR Privacy Inquiry and determine whether it relates to OH or an unauthorized person, or one or more HICs.

- Where the EHR Privacy Inquiry relates to OH or an unauthorized person, the Designated Member of the Privacy Team follows the procedure set out the *OH Privacy Complaints and Inquires Policy and Procedure*.
- Where the EHR Privacy Inquiry relates to one or more HICs, the Designated Member of the Privacy Team follows the procedure beginning in 3.3.13.

3.3.2 The Designated Member of the Privacy Team records all steps taken in relation to the EHR Privacy Inquiry in the tracking log.

### ***EHR Privacy Inquiry Relates to One or More HICs***

3.3.3 Where OH receives an EHR Privacy Inquiry related to one or more HICs, the Designated Member of the Privacy Team:

- Logs receipt of the EHR Privacy Inquiry in the tracking log;
- Forwards the EHR Privacy Inquiry to the HIC(s) to whom the EHR Privacy Inquiry relates as soon as possible, and in any event no later than 4 business days following receipt of the EHR Privacy Inquiry by OH;
- Uses the method of communication preferred by the individual making the EHR Privacy Inquiry to respond to the individual as soon as possible, and in any event no later than 4 business days following receipt of the EHR Privacy Inquiry by OH:
  - Acknowledging receipt of the EHR Privacy Inquiry;
  - Advising that the EHR Privacy Inquiry has been forwarded to one or more HICs;
  - Advising that the HIC(s) to whom the EHR Privacy Inquiry has been forwarded will provide a response to the individual making the EHR Privacy Inquiry as soon as possible, and in any event no later than 30 days following receipt of the EHR Privacy Inquiry by OH;
  - Advising that the HIC(s) to whom the EHR Privacy Inquiry has been forwarded will provide a revised date for response if the EHR Privacy Inquiry cannot be responded to within 30 days following receipt of the EHR Privacy Inquiry by OH; and
  - Providing contact information for the HICs to whom the EHR Privacy Inquiry was forwarded.

3.3.4 Upon receiving a forwarded EHR Privacy Inquiry from OH, the HIC must:

- Receive, document, track, address and respond directly to the individual making the EHR Privacy Inquiry as soon as possible, but in any event no later than 30 days following receipt of the EHR Privacy Inquiry by OH, in accordance with its internal policies, procedures and practices;
- Provide the individual making the EHR Privacy Inquiry with a revised date for response as soon as possible, but in any event no later than 30 days following receipt of the EHR Privacy Inquiry by OH, if the EHR Privacy Inquiry cannot be responded to within 30 days following receipt of the EHR Privacy Inquiry by OH; and

- 3.3.5 Record that the EHR Privacy Inquiry was responded to by maintaining a copy of the response or logging that the EHR Privacy Inquiry was responded to in accordance with its internal policies, practices, and procedures.

### ***Minister Request or Direction regarding EHR Privacy Inquiries***

- 3.3.6 When requested to do so or directed to do so by the Minister of Health (**Minister**), OH assists HICs in:
- Developing a policy and procedures to respond to EHR Privacy Inquiries in circumstances where the EHR Privacy Inquiries relate to one or more HICs; and
  - Responding to EHR Privacy Inquiries.

## **3.4 Procedures related to EHR Privacy Complaints**

- 3.4.1 The Designated Member of the Privacy Team, as soon as possible, reviews the EHR Privacy Complaint and determines whether it relates to OH or an unauthorized person, or one or more HICs.
- 3.4.2 Where the EHR Privacy Complaint relates to OH or an unauthorized person, the Member of the Privacy Team follows the procedure set out in the OH Privacy Complaints and Inquiries Policy and Procedure. Where the EHR Privacy Complaint relates to one or more HICs, the Designated Member of the Privacy Team follows the procedure beginning in section 3.4.15.
- 3.4.3 The Designated Member of the Privacy Team logs all steps taken in relation to the EHR Privacy Complaint in accordance with the requirements set out in Appendix “A.”

### ***EHR Privacy Complaint Relates to One or More HICs***

- 3.4.4 Where OH receives an EHR Privacy Complaint related to one or more HICs or to an agent or ESP of one or more HICs, the Designated Member of the Privacy Team:
- Logs receipt of the EHR Privacy Complaint in the EHR Privacy Complaints Log;
  - Forwards the EHR Privacy Complaint to the HIC(s) to whom the EHR Privacy Complaint relates as soon as possible, and in any event no later than 4 business days following receipt of the EHR Privacy Complaint by OH;
  - Responds in writing to the individual making the EHR Privacy Complaint as soon as possible, and in any event no later than 4 business days following receipt of the EHR Privacy Complaint by OH:
    - Acknowledging receipt of the EHR Privacy Complaint;
    - Advising that the EHR Privacy Complaint has been forwarded to one or more HICs;
    - Advising that the HIC(s) to whom the EHR Privacy Complaint has been forwarded will provide a response to the individual making the EHR Privacy Complaint as soon as possible, and in any event no later than 30 days following receipt of the EHR Privacy Complaint by OH;

- Advising that the HIC(s) to whom the EHR Privacy Complaint has been forwarded will provide a revised date for response if the EHR Privacy Complaint cannot be responded to within 30 days following receipt of the EHR Privacy Complaint by OH; and
  - Providing contact information for the HIC(s) to whom the EHR Privacy Complaint was forwarded.
- 3.4.5 Upon receiving a forwarded EHR Privacy Complaint from OH, the HIC must:
- 3.4.6 Receive, document, track, investigate, remediate, and respond directly to the individual making the EHR Privacy Complaint as soon as possible, but in any event no later than 30 days following receipt of the EHR Complaint by OH, in accordance with its internal policies, procedures and practices;
- 3.4.7 Provide the individual making the EHR Privacy Complaint with a revised date for response as soon as possible, but in any event no later than 30 days following receipt of the EHR Privacy Complaint by OH, if the EHR Privacy Complaint cannot be responded to within 30 days following receipt of the EHR Privacy Complaint by OH; and
- 3.4.8 Record that the EHR Privacy Complaint was responded to by maintaining a copy of the response or logging that the EHR Privacy Complaint was responded to in accordance with its internal policies, practices, and procedures.

### ***Minister Request or Direction related to EHR Privacy Complaints***

- 3.4.9 When requested to do so or directed to do so by the Minister, OH assists HICs in:
- Developing a policy and procedures to make a determination of whether to **investigate an EHR Privacy Complaint and if so, to investigate and remediate** the EHR Privacy Complaint in circumstances where the EHR Privacy Complaint relates to more than one HIC or to an agent or ESP of more than one HIC.
  - Making a determination of whether to investigate an EHR Privacy Complaint and if so, to assist in investigating and remediating the EHR Privacy Complaint in circumstances where the EHR Privacy Complaint relates to one or more HICs or to an agent or ESP of one or more HICs.

## **3.5 Tracking and Logging EHR Privacy Inquiries and EHR Privacy Complaints**

- 3.5.1 OH maintains a log of all EHR Privacy Complaints (EHR Privacy Complaints Log) in respect of PHI accessible by means of the EHR developed or maintained by OH, but is not required to maintain a log of EHR Privacy Inquiries.
- 3.5.2 Designated Members of the Privacy Team, with the oversight of the CPO or delegate, are responsible for maintaining the EHR Privacy Complaints Log and tracking whether OH has addressed the recommendations arising from an investigation within the identified timelines.

- 3.5.3 Documentation related to the receipt, investigation, notification, and remediation of Privacy Complaints will be retained in the secure drive, and the CPO or delegate is responsible for retaining this documentation.
- 3.5.4 The EHR Privacy Complaints Log sets out the information listed in “**Appendix A**” to this document with respect to each EHR Privacy Complaint received by OH.

## **4 Responsibilities**

---

### **4.1 Chief Privacy Officer (CPO) or delegate**

- Overseeing OH’s management of EHR Privacy Inquiries and EHR Privacy Complaints.
- Designating a member of the Privacy Office to manage each EHR Privacy Inquiry and EHR Privacy Complaint and designating members of OH to address and remediate related privacy risks.
- Determining if an EHR Privacy Complaint should be investigated and if the findings of an investigation should be communicated to the CEO or another organization or individual.

### **4.2 SVP, Digital Excellence in Health**

- The SVP, Digital Excellence in Health has been delegated day-to-day authority to manage OH’s security program.

### **4.3 Designated Member of Privacy Office**

- Documenting, tracking, investigating, responding, and remediating the EHR Privacy Inquiry or EHR Privacy Complaint in accordance with this Policy and OH’s internal policies and procedures, as applicable.

### **4.4 Applicable Health Information Custodian (HIC)**

- Notifying OH of EHR Privacy Inquiries and EHR Privacy Complaints that relate to another HIC or OH in accordance with this Policy.
- Documenting, tracking, investigating, responding, and remediating the EHR Privacy Inquiry or EHR Privacy Complaint in accordance with this Policy and the HIC’s internal policies and procedures, as applicable.
- At the first reasonable opportunity upon identifying or becoming aware of a breach of this Policy, notifying OH’s Privacy Office.

### **4.5 Employees and other OH Agents**

- At the first reasonable opportunity upon identifying or becoming aware of a breach of this Policy, notifying OH’s Privacy Office.

- Immediately forwarding any EHR Privacy Inquiries or EHR Privacy Complaints to OH's Privacy Office.

## 4 Definitions and Acronyms

Defined terms are capitalized throughout this document.

Term / Acronym	Definition
<b>CEO</b>	Chief Executive Officer
<b>Collect</b>	<p>Has the meaning set out in section 2 of PHIPA with respect to PHI; and in respect of PI has the same meaning.</p> <p>“Collect” means to gather, acquire, receive, or obtain the information by any means from any source, and “Collection” and “Collected” has a corresponding meaning.</p>
<b>CPO</b>	Chief Privacy Officer
<b>Disclose</b>	<p>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.</p> <p>“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.</p>
<b>EHR or Electronic Health Record</b>	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.
<b>EHR Privacy Complaint</b>	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.
<b>EHR Privacy Inquiry</b>	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.
<b>Employee</b>	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 <i>Employee Classification Guideline</i> . A consultant or contractor is not an Employee.

Term / Acronym	Definition
<b>ESP or Electronic Service Provider</b>	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.
<b>HIC or Health Information Custodian</b>	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.
<b>IPC</b>	Information and Privacy Commissioner of Ontario
<b>IPC PO Manual</b>	IPC Manual for the Review and Approval of Prescribed Organizations
<b>Minister</b>	Minister of Health
<b>O. Reg. 329/04</b>	Ontario Regulation 329/04 made under PHIPA
<b>OH</b>	Ontario Health, the agency of the Government of Ontario to which this Policy applies.
<b>OH Agent</b>	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.
<b>PHI or Personal Health Information</b>	<ul style="list-style-type: none"> <li>• Has the meaning set out in section 4 of PHIPA. Specifically, it is “identifying information” in oral or recorded form about an individual that:</li> <li>• Relates to the physical or mental health of the individual, including information that consists of the health history of the individual’s family;</li> <li>• 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;</li> <li>• 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;</li> <li>• Relates to payments or eligibility for health care or eligibility for coverage for health care in respect of the individual;</li> <li>• 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;</li> <li>• Is the individual’s health number; and/or</li> <li>• Identifies an individual’s substitute decision-maker.</li> </ul> <p>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.</p>

Term / Acronym	Definition
<b>PHIPA or Personal Health Information Protection Act, 2004</b>	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.
<b>Prescribed Organization or PO</b>	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.
<b>Privacy Incident</b>	<p>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:</p> <ol style="list-style-type: none"> <li>1. confirmed to be a Privacy Breach</li> <li>2. confirmed not to be a Privacy Breach</li> <li>3. it cannot or has not been determined if a Privacy Breach occurred (Suspected Privacy Breach).</li> </ol> <p><b>Note:</b> 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.</p>

Term / Acronym	Definition
<p><b>Privacy Breach</b></p>	<p>A Privacy Breach includes:</p> <ol style="list-style-type: none"> <li>1) Privacy Breach of PHI or PI (Privacy PHI/PI Breach) means an event where: <ul style="list-style-type: none"> <li>• 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</li> <li>• The Viewing, handling or otherwise dealing with PHI provided to OH is not in compliance with PHIPA, or its regulation;</li> <li>• 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.</li> </ul> <p><b>Note:</b> 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.</p> </li> <li>2) Privacy Breach of Privacy Policy or Agreement (Privacy Policy/Agreement Breach) means an event where: <ul style="list-style-type: none"> <li>• There is a contravention of OH’s privacy policies, procedures, or practices; and/or</li> <li>• There is a contravention of a privacy-related<sup>1</sup> term or condition in a: <ul style="list-style-type: none"> <li>○ data sharing agreements,</li> <li>○ research agreements,</li> <li>○ confidentiality agreements, or,</li> <li>○ agreements with third-party service providers retained by OH to handle PHI or PI,</li> <li>○ written acknowledgements acknowledging and agreeing not to use PHI or PI which has been de-identified and/or aggregated, to identify an individual; and</li> </ul> </li> <li>• Does not include a privacy breach of PHI or PI</li> </ul> <p><b>Note:</b> 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.</p> </li> </ol>
<p><b>Use</b></p>	<p>In relation to PHI or PI in the custody or under the control of a HIC or a person, “Use” means to view, handle or otherwise deal with the information, but does not include to Disclose the information, and “Use,” as a noun, has a corresponding meaning. For the purposes of PHIPA, the providing of PHI between a HIC and an agent of the HIC is a Use by the HIC, and not a Disclosure by the person providing the information or a Collection by the person to whom the information is provided.</p>

<sup>1</sup> 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.

## 5 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*.

## 6 References and/or Key Implementation Documents

---

- PHIPA and O. Reg. 329/04
- IPC PO Manual
- Privacy Audit and Compliance Policy
- Privacy Incident Management Policy and Procedure
- EHR Privacy Incident Management Policy and Procedure

## 7 Appendices

---

- Appendix “A”: Minimum Content Required in EHR Privacy Complaints Log

## 8 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.

## 9 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
7/2025	<ul style="list-style-type: none"><li>• Updated IT contact information.</li><li>• Updated roles and responsibilities to reflect changes in organizational structure.</li><li>• Added/edited information throughout Policy as per the updated IPC Manuals; Updated contact information for making a complaint to OH;</li><li>• Revised definitions of Personal Health Information, Privacy Breach, and Privacy Incident</li></ul>	INF-004.02-PP	10/06/2025	CEO

	<ul style="list-style-type: none"><li>Updated compliance will be enforced in accordance with the <i>Progressive Discipline Policy</i>.</li></ul>			
--	--	--	--	--

## 10 Policy Repeal

---

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

## Appendix A: Complete Content Required in EHR Privacy Complaints Log

The EHR Privacy Complaints Log sets out each of the following, to the extent they are known to OH:

- The date that the EHR Privacy Complaint was received by OH;
- The nature of the EHR Privacy Complaint;
- The HICs to whom the EHR Privacy Complaint was forwarded and the date the EHR Privacy Complaint was forwarded, if applicable;
- The date the individual was advised that the EHR Privacy Complaint was forwarded to one or more HICs, if applicable;
- The determination as to whether or not the EHR Privacy Complaint will be investigated by OH;
- The Employee(s) or other OH Agent(s) and/or the agent(s) of a HIC who made the determination as to whether the EHR Privacy Complaint would be investigated;
- Where the determination was made that the EHR Privacy Complaint will not be investigated, the date that the individual making the Complaint was advised that the EHR Privacy Complaint will not be investigated and was provided a response to the EHR Privacy Complaint and informed of their right to file their complaint with the IPC;
- Where the determination is made that the EHR Privacy Complaint will be investigated:
  - The date that the individual making the EHR Privacy Complaint was advised that the EHR Privacy Complaint will be investigated;
  - The date that the investigation was commenced;
  - The date that the investigation was completed;
  - The employee(s) or other OH Agent(s) and/or the agent(s) of a HIC responsible for conducting the investigation;
  - The findings and recommendations arising from the investigation;
  - The date that the Chief Executive Officer or Executive Director (or equivalent position) and senior management were notified of the findings and other relevant recommendations arising from the investigation, if applicable;
  - The Employee(s) or other OH Agent(s) and/or agent(s) of a HIC responsible for addressing each recommendation;
  - The date each recommendation was or is expected to be addressed;
  - The manner in which each recommendation was or is expected to be addressed; and
  - The date that the individual making the EHR Privacy Complaint was advised of the findings of the investigation, of the measures taken, if any, in response to the privacy complaint, and of their right to file a complaint with the IPC.