Electronic Health Record Privacy Incident Management Policy and Procedure

Policy Level Approval:	Chief Executive Officer
Policy Category:	Corporate Policy
Policy Number:	INF-006.02-PP
Sensitivity Level:	Public
Policy Sponsor (or Sponsors):	Chief, Strategy, Planning, Privacy & Analytics
Original Date of Approval:	September 30, 2020
Date of Posting: This Policy is effective on the date of its posting 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

1.1.1 To provide guidance to Health Information Custodians (**HICs**) and Coroners with respect to their obligations for the identification, reporting, containment, notification, investigation and remediation of Privacy Incidents related to Personal Health Information (**PHI**) received by Ontario Health (**OH**) as a Prescribed Organization (**PO**) for the purpose of developing or maintaining the Electronic Health Record (**EHR**).

1.2 Objectives

1.2.1 To enable OH, HICs and Coroners to comply with the Privacy Incident management requirements set out in the following, as applicable:

- The *Personal Health Information Protection Act, 2004* (**PHIPA**) and its regulations;
- The Information and Privacy Commissioner of Ontario's (**IPC**) *Manual for the Review and Approval of Prescribed Organizations* (**IPC PO Manual**);
- Guidelines issued by the IPC, including *Responding to a Health Privacy Breach: Guidelines for the Health Sector;* and
- Any directions issued by the Minister of Health (**Minister**).

1.2.2 To protect the privacy of individuals and the confidentiality of their PHI.

1.3 Application and Scope

1.3.1 This Policy applies to HICs that provide PHI to OH as a PO for the purpose of developing or maintaining the EHR, HICs that Collect PHI by means of the EHR, and Coroners to whom the PO provides PHI by means of the EHR.

1.3.2 This Policy applies to OH in its capacity as a PO, specifically: non-union Employees, people leaders, board members, unionized Employees, secondees, consultants, and other individuals acting on behalf of OH collectively referred to as (**OH Agents**).

1.3.3 OH Employees and other OH Agents must also comply with the OH *Privacy Incident Management Policy and Procedure* when managing Privacy Incidents, including those related to PHI received by OH as a PO for the purpose of developing or maintaining the EHR.

1.4 Compliance and Exemptions

1.4.1 Compliance with this Policy in its entirety is mandatory unless an exception to a specific section is approved by OH's 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 the roles, process and frequency outlined in the *Privacy Audit & Compliance Policy.*

1.4.3 At the first reasonable opportunity upon identifying or becoming aware of a breach of this Policy, OH Employees and other OH Agents, as well as HICs and Coroners 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 Compliance will be enforced in accordance with the *Progressive Discipline Policy.*

1.5 Terminology

1.5.0 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".

1.5.1 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 General

2.1 Background

2.1.1 In accordance with this Policy and OH's *Privacy Incident Management Policy and Procedure*, OH's Privacy Office, led by the CPO, is responsible for the management of OH's privacy program including procedures addressing identification, reporting, containment, notification, investigation and remediation of suspected and actual Privacy Breaches related to the EHR.

2.1.2 OH has systems and processes in place to audit and monitor the EHR for suspicious Collection, Use and Disclosure of PHI accessible by means of the EHR.

- If OH becomes aware of a Privacy Incident related to the EHR, at the first reasonable opportunity and to the extent reasonably known, OH notifies:
  - The HIC(s) or Coroner(s) that caused the Privacy Incident; and
  - The HIC(s) that provided the PHI to OH as a PO for the purpose of developing or maintaining the EHR.

2.1.3 OH's Privacy Office investigates, tracks, and logs Privacy Incidents in accordance with the OH *Privacy Incident Management Policy and Procedure*.

2.2 Policy

2.2.1 HICs and Coroners must implement and adhere to their own internal Privacy Incident management policies for the identification, reporting, containment, notification, investigation and remediation of Privacy Incidents in respect of PHI accessible by means of the EHR and are responsible for ensuring their own compliance with PHIPA, O. Reg. 329/04, OH Policies, and applicable legal agreements.

2.2.2 HICs and Coroners that Collect, Use or Disclose PHI by means of the EHR must ensure that their internal policies and procedures impose mandatory reporting requirements that ensure the HIC or Coroner's compliance with PHIPA, O. Reg.329/04, and this Policy.

2.2.3 HICs that provide PHI to the PO for the purpose of developing or maintaining the EHR, HICs that Collect PHI by means of the EHR, and Coroners to whom the PO provides PHI by means of the EHR must notify OH at the first reasonable opportunity upon identifying or becoming aware of a Privacy Incident related to PHI accessible by means of the EHR.

Notice should be provided to OH's Privacy Office by reporting the Privacy Incident to Enterprise Service Desk by Phone: 1-866-250-1554; or Email: oh-servicedesk@ontariohealth.ca.

2.2.4 All findings that are identified through the management and investigation of a Privacy Breach under this Policy must be communicated in writing (may include email or hardcopy i.e. letter)

HICs who provide PHI to the PO for the purpose of developing or maintaining the EHR

2.2.5 PHIPA establishes that when a HIC provides PHI to the PO, the HIC is considered not to be Disclosing the information to the PO, and the PO is considered not to be Collecting the information from the HIC.[1]

2.2.6 PHIPA requires HICs with custody or control of PHI about an individual to notify the individual to whom the PHI relates at the first reasonable opportunity if the PHI is stolen or lost or if it is Used or Disclosed without authority, and include in the notice a statement that the individual is entitled to make a complaint to the IPC under Part VI of PHIPA.[2] This includes Privacy Breaches related to the EHR which are caused by the PO or an Unauthorized Person.

2.2.7 If the circumstances surrounding a theft, loss or unauthorized Use or Disclosure meet the requirements prescribed in Ontario Regulation 329/04 made under PHIPA (**O.Reg.329/04**), the HIC must notify the IPC of the theft or loss or of the unauthorized Use or Disclosure.[3]

HICs who Collect PHI by means of the EHR

2.2.8 If PHI about an individual is Collected without authority by means of the EHR, in addition to any notice that is required to be given in the case of an unauthorized Use or Disclosure under subsections 12 (2) and (3) of PHIPA, the HIC who is responsible for the unauthorized Collection must:

- Notify the individual at the first reasonable opportunity of the unauthorized Collection, and include in the notice a statement that the individual is entitled to make a complaint to the IPC under Part VI; and

[1] Subsection 55.1(3) of PHIPA.

[2] Subsection 12(2) of PHIPA.

[3] Subsection 12(3) of PHIPA.

- If the circumstances surrounding the unauthorized Collection meet the prescribed requirements, notify the IPC of the unauthorized Collection.[4]

Coroners to whom the PO provides PHI by means of the EHR

2.2.9 O. Reg. 329/04 establishes that a Coroner to whom the PO provides PHI under subsection 55.9.1 (1) of PHIPA must, with respect to that PHI, comply with section 11.1, subsections 12 (1), (2) and (3), subsection 13 (1) and sections 17, 17.1, 30 and 31 of PHIPA as if the Coroner were a HIC.[5]

2.2.10 A Coroner to whom the PO provides PHI under subsection 55.9.1 (1) of PHIPA may only Use or Disclose the PHI for the purpose for which the PHI was provided or for the purpose of carrying out a statutory or legal duty.[6]

2.2.11 If a Coroner requests that the PO transmit PHI to the Coroner by means of the EHR and the PO transmits the PHI as requested, the Coroner must comply with the obligations set out in subsection 12 (1) of PHIPA with respect to the transmitted PHI, regardless of whether the Coroner has viewed, handled or otherwise dealt with the PHI.[7]

Specifically, in accordance with subsection 12(1) of PHIPA, the Coroner must take steps that are reasonable in the circumstances to ensure that PHI in its custody or control is protected against theft, loss and unauthorized Use or Disclosure and to ensure that the records containing the PHI are protected against unauthorized copying, modification or disposal.[8]

2.2.12 If PHI about an individual is Collected without authority by a Coroner by means of the EHR, the Coroner must:

(a) Notify the individual at the first reasonable opportunity of the unauthorized Collection and include in the notice a statement that the individual is entitled to make a complaint to the IPC under Part VI of PHIPA; and

(b) Notify the IPC of the unauthorized Collection at the first reasonable opportunity, if any circumstance exists where the Coroner would be required to notify the Commissioner if the Coroner were a HIC to which subsection 18.3 (1) of O.Reg. 329/04 applied.[9]

2.2.13 *Annual report re: theft, loss, etc.:* A Coroner to whom the PO provides PHI under subsection 55.9.1 (1) of PHIPA must, in respect of that PHI, comply with section 6.4 of O.Reg.329/04, with any necessary modification, as if the Coroner were a HIC.[10]

---

[4] Subsection 55.5(7) of PHIPA.

[5] Subsection 18.10(1) of O. Reg. 329/04.

[6] Subsection 18.10(2) of O. Reg. 329/04.

[7] Subsection 18.10(3) of O. Reg. 329/04.

[8] Subsection 12(1) of PHIPA.

[9] Subsection 18.10(4) of O. Reg. 329/04.

[10] Subsection 18.10(5) of O. Reg. 329/04.

3 Process for Managing Privacy Incidents

3.1 Identification of Privacy Incidents by HIC or Coroner

3.1.1 HICs and Coroners may identify a Privacy Incident through a combination of formal and informal processes, including the following:

- Reports by their employees or other agents;
- Reports by other HICs or Coroners;
- Reports by members of the public;
- Privacy audits, Privacy Complaints and Privacy Inquiries.

3.1.2 Where a HIC or Coroner becomes aware of a Privacy Incident related to the EHR, the HIC or Coroner must notify OH at the first reasonable opportunity in writing by sending the *Appendix A: Breach Notification Form* by email to: oh-servicedesk@ontariohealth.ca. Notice may also be provided to OH verbally by telephone at: 1-866-250-1554.

3.1.3 Upon receiving notice of a Privacy Incident, OH Employees and other OH Agents will follow the OH *Privacy Incident Management Policy and Procedure*.

3.2 Identification of Privacy Incidents by Ontario Health

3.2.1 Where OH identifies a Privacy Incident that was caused by one or more HICs or Coroners, OH reports the Privacy Incident to the HIC(s) or Coroner(s) in accordance with the OH *Privacy Incident Management Policy and Procedure*.

3.3 Privacy Incidents Caused by One or More HICs or Coroners

3.3.1 Where it is confirmed that a HIC or Coroner has caused a Privacy Incident involving unauthorized Collection of PHI by means of the EHR, the HIC or Coroner must appoint an investigator no later than 7 days after becoming aware of the Privacy Incident. The investigator appointed by the HIC or Coroner must, as soon as reasonably possible, submit a written report of the investigation to OH as outlined in *Appendix B: Breach Notification Form.*

3.2.2 Upon receipt of the written report of the investigation, OH Employees and other OH Agents follow the OH *Privacy Incident Management Policy and Procedure*.

3.2.3 In addition to any notice that is required to be given in the case of an unauthorized Use or Disclosure by a HIC under subsections 12 (2) and (3) of PHIPA, if PHI about an individual is Collected without authority by means of the EHR, the HIC who is responsible for the unauthorized Collection must,

(a) notify the individual at the first reasonable opportunity of the unauthorized Collection, and include in the notice a statement that the individual is entitled to make a complaint to the IPC under Part VI of PHIPA; and

(b) if the circumstances surrounding the unauthorized Collection meet the prescribed requirements, notify the IPC of the unauthorized Collection.[11]

3.2.4 If PHI about an individual is Collected without authority by a Coroner by means of the EHR, the Coroner must:

- Notify the individual at the first reasonable opportunity of the unauthorized Collection and include in the notice a statement that the individual is entitled to make a complaint to the IPC under Part VI of PHIPA; and
- Notify the IPC of the unauthorized Collection at the first reasonable opportunity, if any circumstance exists where the Coroner would be required to notify the IPC if the Coroner were a HIC to which subjection 18.3 (1) of O. Reg. 329/04 applied.[12]

3.2.5 When requested or directed by the Minister, OH fulfills the following in accordance with the OH *Privacy Incident Management Policy and Procedure*:

- Cooperates with the HICs in developing a policy and procedure to make a determination of whether a Privacy Breach has in fact occurred and if so, to contain, investigate and remediate the Privacy Breach, and to notify individuals in circumstances where the Privacy Breach or Privacy Incident was caused by one or more HICs;

3.2.6 Assists HICs in making a determination of whether a Privacy Breach has in fact occurred and if so, assist in containing, investigating and remediating the Privacy Breach and notifying individuals in circumstances where the Privacy Breach or Privacy Incident was caused by one or more HICs; and

- Assists HICs in fulfilling their obligations to notify individuals under subsections 12(2) and 55.5(7) of PHIPA and takes into consideration any directions issued by the Minister.

3.2.7 OH's CPO or designate is responsible for appointing members of the OH Privacy Office or other designated program area/business unit to assist the HIC(s) upon request or direction by the Minister.

3.2.8 In addition to any requests or directions issued by the Minister, OH may assist the HICs in fulfilling their obligation to notify individuals of a Privacy Breach. OH's role in assisting a HIC may include:

- Collating a list of individuals impacted by the Privacy Incident;
- Drafting the notice to affected individual(s); and
- Supporting any other requests or directions issued by the Minister.

3.3 Privacy Incidents Caused by OH or an Unauthorized Person

3.3.1 OH follows the steps outlined in the OH *Privacy Incident Management Policy and Procedure* to manage Privacy Incidents caused by:

[11] Subsection 55.5(7) of PHIPA.

[12] Subsection 18.10(4) of O. Reg. 329/04.

- OH Employees or other OH Agents;
- A system that retrieves, processes or integrates PHI accessible by means of the EHR;
- An unauthorized person who is not an OH Employee or other OH Agent; and
- An unauthorized person who is not an agent of a HIC.

Note: *OH Privacy Incident Management Policy and Procedure* stipulates the process to be followed for determining whether an event constitutes a Privacy Incident or Breach, as well as the process for containment, investigation and notification, and the documentation that must be completed, provided and/or executed by the OH Employee or other OH Agent responsible and the required content of the documentation.

4 Responsibilities

4.1 Ontario Health Chief Privacy Officer

4.1.1 Ensures compliance with FIPPA and PHIPA and ensures relevant OH policies and procedures are put in place.

4.1.2 Responsible for the overall accountability and the day-to-day operations of the Privacy Program.

4.2 Ontario Health Privacy Office

4.2.1 Responsible for authoring and maintaining this Policy and its associated processes.

4.2.2 Receives and manages notifications of Privacy Incidents.

4.2.3 Manages Privacy Incidents and Breaches in accordance with this Policy and the OH *Privacy Incident Management Policy*.

4.3 HICs that provide PHI to OH as a PO

4.3.1 Manage Privacy Incidents in accordance with this Policy, PHIPA, O. Reg. 329/04 and the HIC's internal Privacy Incident Management policies, procedures and practices.

4.3.2 Responsible for notifying individuals of a Privacy Breach that relates to PHI the HIC provided to OH as a PO for the purpose of developing or maintaining the EHR in accordance with PHIPA.

4.4 Coroners to whom PHI is provided by means of the EHR

4.4.1 Manage Privacy Incidents in accordance with this Policy, PHIPA, O. Reg. 329/04 and the Coroner's internal Privacy Incident Management policies, procedures and practices.

4.4.2 Responsible for notifying individuals and the IPC in accordance with PHIPA where the Coroner Collects PHI by means of the EHR without authority.

4.5 HICs that Collect PHI by means of the EHR

4.5.1 Manage Privacy Incidents in accordance with this Policy, PHIPA, O. Reg. 329/04 and the HIC's internal Privacy Incident Management policies, procedures and practices.

4.5.2 Responsible for notifying individuals and the IPC in accordance with PHIPA where the HIC Collects PHI by means of the EHR without authority.

5 Definitions and Acronyms

Defined terms are capitalized throughout this document.

Term / Acronym	Definition
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.
Coroner	Means the Chief Coroner for Ontario, a Deputy Chief Coroner for Ontario, a regional coroner or a coroner appointed under section 5 of the *Coroners Act*, as set out in section 1 of the *Coroners Act.*
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.
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.
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.

Term / Acronym	Definition
IPC	Information and Privacy Commissioner of Ontario
IPC PO Manual	IPC Manual for the Review and Approval of Prescribed Organizations
Minister	Minister of Health
MOH	Ontario Ministry of Health
O. Reg. 329/04	Ontario Regulation 329/04 made under PHIPA
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.
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.

Term / Acronym	Definition
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.
PI or Personal Information	Has the meaning set out in section 2 of FIPPA. Specifically, it means recorded information about an identifiable individual, including: • information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual; • information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved; • any identifying number, symbol or other particular assigned to the individual; • the address, telephone number, fingerprints or blood type of the individual; • the personal opinions or views of the individual except where they relate to another individual; • correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence; • the views or opinions of another individual about the individual; and • the individual's name where it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual. Personal Information also includes information that is not recorded and that is otherwise defined as Personal Information when considering the manner of collection, notice to public, privacy impact assessments and safeguards.[13]
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.

[13] Section 38 (1) FIPPA

Term / Acronym	Definition
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[14] 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 Complaint	Concerns or complaints relating to: • The privacy policies, procedures and practices implemented by OH and OH's compliance under PHIPA, FIPPA and associated regulations; and • Compliance of a HIC with PHIPA and its regulation in respect of PHI that is accessible by means of the EHR developed or maintained by OH.

[14] 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.

Term / Acronym	Definition
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). **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.
Privacy Inquiry	Inquiries relating to: • The privacy policies, procedures and practices implemented by OH and OH's compliance under PHIPA, FIPPA and related regulations; and • Inquiries relating to the privacy policies, procedures, and practices of a HIC, or the compliance of a HIC with PHIPA and its regulation, in respect of PHI that is accessible by means of the EHR developed or maintained by OH.
Use	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.

6 Review Cycle

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

7 References and/or Key Implementation Documents

- Privacy Incident Management Policy and Procedure
- Information Security Incident Management Standard
- Electronic Health Record Logging and Auditing Policy

- Electronic Health Record Privacy Breach Report Form
- Electronic Health Record Retention Policy
- Privacy Audit and Compliance Policy
- IPC's Responding to a Health Privacy Breach: Guidelines for the Health Sector
- Any directions issued by the Minister of Health

8 Appendices

- *Appendix A: Privacy Breach Severity Report Form*
- *Appendix B: Privacy Breach Notification Form*

9 Policy Consultations

The following were consulted in the development of this Policy:

- Managers and responsible staff members of OH business units responsible for implementing and/or complying with this Policy.

10 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
01/07/2025	• 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-006.02-PP	10/06/2025	CEO

11 Policy Repeal

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

Appendix A: Privacy Breach Severity Levels:

High Severity:

- Significant number or volume of individuals are impacted
- Information could be used to commit identify theft or gain unauthorized access to computer systems and other sources of PHI
- Significant risk of media attention
- Will cause significant reputation harm to OH
- May cause significant harm to individuals or stakeholders
- Containment requires shutting down systems
- Information at issue is considered highly sensitive
- Information may have been disclosed in error to the public at large
- Recurring Privacy Incident

Medium Severity:

- A relatively small number of individuals are impacted
- Moderate risk of harm to individual
- Moderate risk of media attention
- Moderate risk that the information could be used to commit identify theft or gain unauthorized access to computer systems and other sources of PHI
- Containment requires shutting down some minor systems
- Information disclosed to a known individual not authorized by OH to view PHI
- A breach caused by incorrect access permissions either due to human error or technological error; access permissions are assigned incorrectly

Low Severity:

- A single record of misdirected outgoing correspondence containing PHI caused by a factor such as an incorrect address
- Unlikely to cause harm to the individual
- Unlikely risk of media attention
- Unlikely risk that the information could be used to commit identify theft or gain
- Not recurring or widespread
- No harm to OH or Division's systems or information
- Information disclosed to a known individual authorized by OH to view PHI

- A policy breach where the Collection, use or disclosure is in contravention of an Ontario Health policy, but does not constitute an unauthorized Collection, use or disclosure as per *PHIPA* (e.g. PHI sent in an email to an authorized OH recipient) and including passive Privacy Breaches.

Appendix B: Privacy Breach Notification Form

Privacy Breach Notification Form

Overview

A Privacy Breach must be reported to **Ontario Health's Privacy Office** as soon as possible, after making the determination that a Privacy Breach has occurred or where there is a reasonable suspicion that a Privacy Breach has occurred.

Do NOT include any Personal Information (PI) or Personal Health Information (PHI) in this report

Instructions

Complete this form with as much information as is known at the time of reporting and send to OH-DS_privacyoperations@ontariohealth.ca.

Privacy Breach Report	
Date report last updated: Version number of report: Is this the final version of the report?	
2. Privacy Breach Information (Reporter to complete as much as known)	
Time and date Privacy Breach occurred (if known):	
Time and date Privacy Breach identified:	
Breach Severity (High, Medium, Low):	
Person responsible for the Privacy Breach (if relevant and known):	
Does the breach involve a shared system? If so, please identify which one(s).	
Breach Type ☐ Collection ☐ Use ☐ Disclosure ☐ Retention ☐ Destruction ☐ Mishandling	Was the Breach? * ☐ Unintentional ☐ Intentional

☐ Other, explain:	

Description of the nature and scope of the Privacy Breach *****

Include information such as:

- *What activity or activities occurred? When did they occur?*
- *Who was involved?*
- *Why is it a Breach?*
- *What is supposed to happen? What are the standard operating procedures?*
- *How many <<patients/clients>> were affected?*

What PHI was involved in the Breach? *

☐ Demographic Information
☐ Medical
☐ Other

Description of the PHI involved in the Breach:

3. Privacy Breach Containment

Person responsible for containment *****

Description of any containment measures taken *****

4. Privacy Breach Escalation

Identify which if any of the following has been notified about the Privacy Breach *****

Group	*Date of Notification*
☐ Program Office (if shared system)	
☐ Clinic Leadership	
☐ IPC / Ontario	
☐ Law enforcement	
☐ Regulatory College	
☐ Other, explain	

5. Notification to Impacted Individuals

Were the impacted individuals (i.e., <<patients/clients>> or clients) notified? If not, why? *

Describe the manner of the notice *

Include information such as:

- *Who was responsible for the notice?*
- *When was notice provided?*
- *How was notice provided?*

6. Investigation

Breach Investigator (Name) *

Description of investigation activities *

Include information such as:

- *Scope and nature of the investigation*
- *Steps that were followed*

Root cause of the Privacy Breach *

7. Remediation Plan

Identify the remediation activities that have been completed or are recommended to be completed.

Activity	**Owner**	**Status of Completion**	**Expected Date of Completion**