Electronic Health Record Privacy Incidents & Privacy Breaches Policy

Policy Level Approval:	Chief Privacy Officer
Policy Category:	EHR Privacy Program
Cross Reference to Other policies/legislations/regulations/directives:	*The Personal Health Information Protection Act, 2004 (PHIPA); Ontario Regulation, 329/04*
Original Date of Approval:	September 30, 2020

Policy Applies to:

☒ Health information custodians that collect, use and disclose personal health information that is accessible by means of the electronic health record

☒ Health information custodians that contribute personal health information that is accessible by means of the electronic health record

☒ Employees of Ontario Health

1. Purpose

This policy defines Ontario Health (Digital Services)' policy and procedures for detection and handling of Privacy Incidents and Privacy Breaches that involve PHI held within the EHR. Capitalized words, including acronyms, have the meanings set out in section 5, Definitions.

2. Scope

This policy applies to the electronic health record (EHR) that is developed and maintained by Ontario Health (Digital Services), under its authority as the Prescribed Organization under s.45(1) of PHIPA . For more information on the scope of the EHR, please see the Plain Language Description of the Electronic Health Record.

This policy and supporting procedures apply to Privacy Incidents and Privacy Breaches that involve PHI held within the EHR.

3. Policy

Privacy Incidents and Privacy Breaches

As the Prescribed Organization and in accordance with PHIPA, Ontario Health (Digital Services) has procedures in place to identify, report, contain, investigate, remediate and provide notice of Privacy Incidents and Privacy Breaches in accordance with its obligations under PHIPA.

Ontario Health (Digital Services) monitors the EHR for suspicious collection, use or disclosure of PHI held within the EHR.

A suspicious collection, use or disclosure of PHI held within the EHR is, and is handled as, a Privacy Incident until it is determined to be a Privacy Breach.

As a Prescribed Organization, Ontario Health (Digital Services) is responsible for notifying the IPC of breaches it is responsible for causing. The HICs are responsible for notifying the IPC of a Privacy Breach they are responsible for causing.

HICs are responsible for notifying individuals in all instances of a Privacy Breach, regardless of the source or cause of the Privacy Breach.

HICs who provide PHI to Ontario Health (Digital Services), by means of the EHR, that they are authorized to provide, are not responsible for:

i. Any unauthorized viewing or handling of the PHI, or any unauthorized dealing with the PHI, by Ontario Health (Digital Services), its employees or Agents; or

ii. Any unauthorized collection of the PHI by another HIC.

4. Process for Managing and Responding to Privacy Incidents and Privacy Breaches

4.1 Identification and Notification

i. HICs will ensure that their Agents and Electronic Service Providers (ESPs) notify them of actual or suspected Privacy Incidents and Privacy Breaches, at the first reasonable opportunity, in accordance with PHIPA.

ii. Ontario Health (Digital Services) will ensure that its Agents and service providers notify Ontario Health (Digital Services) of actual or suspected Privacy Incidents and Privacy Breaches, at the first reasonable opportunity, in accordance with PHIPA and Ontario Health (Digital Services)' internal policies, procedures and practices.

4.2 Reporting and Containment

i. Ontario Health (Digital Services) or any Agent of Ontario Health (Digital Services) who suspects or detects a Privacy Incident or Privacy Breach is required to report it immediately to the Ontario Health (Digital Services)' Privacy Department at 416-946-4767 or via email at OH-DS_privacyoperations@ontariohealth.ca.

ii. Where Ontario Health (Digital Services) has determined that a Privacy Breach has occurred and is responsible for the Privacy Breach, Ontario Health (Digital Services) will follow its internal policies, procedures and practices to contain the Privacy Breach and, where required, request assistance from other HICs in containing the Privacy Breach.

iii. Any HIC that suspects or detects a Privacy Incident or Privacy Breach is required to engage their own internal privacy department to address and contain the incident or breach in accordance with the HIC's internal policies and procedures.

iv. The HIC's internal Privacy Designate must report the Privacy Breach to Ontario Health (Digital Services)' privacy department as soon as possible, but in any event no later than the end of the next business day after it is determined that the privacy breach has occurred.

4.3 Investigation

i. Ontario Health (Digital Services) or the HIC or HICs that created and contributed the PHI to the EHR that was subject to the Privacy Breach must, as soon as possible, but in any event no later than seven (7) days after the determination that a Privacy Breach has occurred, identify a Breach Investigator within their organization to lead the Privacy Breach investigation.

ii. The Breach Investigator must provide Ontario Health (Digital Services) with a written report of the investigation, no later than seven (7) days after the breach investigator has been identified. (See Appendix A: Privacy Breach Report Form).

4.4 Notification

i. Responsibility for notifying individuals of Privacy Breaches will be the responsibility of the HIC who collected the PHI without authority. If the Privacy Breach is caused by Ontario Health (Digital Services), the HIC who contributed the PHI to the EHR is responsible for notifying the impacted individuals. If the PHI has been contributed by more than one HIC, the HICs in collaboration with Ontario Health (Digital Services) will determine the most appropriate HIC to notify the individual.

ii. The HIC will notify the IPC in writing, of a Privacy Breach that the HIC is responsible for causing.

iii. Ontario Health (Digital Services) will notify the IPC in writing, immediately after becoming aware that PHI held within the EHR,

   i. Has been viewed, handled or otherwise dealt with by Ontario Health (Digital Services), its Agents or service providers, other than in accordance with its obligations set out in PHIPA, or

   ii. Has been made available or released by Ontario Health (Digital Services), its Agents or service providers, other than in accordance with its obligations set out in PHIPA.

iv. Ontario Health (Digital Services) is responsible for notifying, at the first reasonable opportunity, each HIC that contributed the PHI to the EHR, if the PHI that the HIC provided is stolen or lost or if it is collected, used or disclosed without authority.

5. Definitions

Agent: An entity, who, with the authorization of the HIC, acts for or on behalf of the HIC in respect of personal health information for the purposes of the HIC, and not its own purposes as defined by section 2 of PHIPA.

Breach Investigator: The party assigned to the breach file to gather relevant facts and help resolve the issues under dispute.

CPO: Ontario Health (Digital Services)'s Chief Privacy Officer.

EHR: The electronic health record, as defined by section 55.1(1) of PHIPA, and further detailed in the Plain Language Description of the EHR available on Ontario Health's website.

ESP: Electronic Service Provider, as defined by section 54.1 (1) of PHIPA.

HIC: Heath information custodian, as defined by section 3(1) of PHIPA.

IPC: The Information and Privacy Commissioner of Ontario.

Ontario Health: A corporation under the *Connecting Care Act, 2019*, and a Crown agent, which, among other things, is charged with managing health service needs across Ontario in a manner consistent with the health system strategies of the Ministry of Health (as further detailed in section 6 of the Act) and has assumed the operations, activities and affairs of eHealth Ontario.

PHI: Personal health information, as defined by section 4(1) of PHIPA.

PHIPA: The *Personal Health Information Protection Act*, 2004, and supporting regulations as amended from time to time.

Prescribed Organization: The organization prescribed by Ontario Regulation 329/04 as the organization for the purposes of Part V.1 of PHIPA.

Privacy Breach: A collection, use or disclosure of PHI held within the EHR that is not authorized by: PHIPA; policies or procedures implemented by Ontario Health; or an agreement that governs handling of the PHI held within the EHR by Ontario Health. This includes circumstances where PHI that is held within the EHR is stolen, lost or subject to unauthorized collection, use or disclosure, including unauthorized copying, modification or disposal.

Privacy Designate: The person listed in the matrix of privacy contacts that is maintained by Ontario Health (Digital Services) Privacy Operations team.

Privacy Incident: A collection, use or disclosure of PHI held within the EHR, that does not, or has not yet been determined to, constitute a Privacy Breach that contravenes an agreement that governs handling of that PHI by Ontario Health or by an Agent on its behalf.

6. Responsibilities

ROLE	RESPONSIBILITY
Ontario Health Chief Privacy Officer:	Responsible for approving this policy and its associated processes
Ontario Health (Digital Services) Privacy Office:	Responsible for authoring and maintaining this policy and its associated processes
Ontario Health (Digital Services) Legal Counsel:	Responsible for reviewing and providing input into this policy and its associated processes
Ontario Health Employees:	Responsible for complying with this policy and its associated processes
Health Information Custodians who contribute to or access the EHR:	Responsible for complying with this policy and its associated processes in relation to PHI held within the EHR

7. Review

This policy is reviewed and updated in accordance with all applicable laws.

8. Appendices

Appendix A: Breach Report Form

Form 1:

Breach Notification Form

Overview

A Privacy Breach must be reported to Ontario Health (Digital Services) as soon as possible, **but in any event no later than the end of the next business day** after making the determination that a Privacy Breach has occurred or has reasonable suspicion that a Privacy Breach has occurred by contacting the **Ontario Health (Digital Services)' Privacy Office**.

Instructions

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

DATE FORM COMPLETED:	
SECTION 1: SUBMITTER CONTACT INFORMATION	
ORGANIZATION NAME:	
SUBMITTER FIRST NAME:	SUBMITTER BUSINESS TELEPHONE NO.:
SUBMITTER LAST NAME:	SUBMITTER BUSINESS EMAIL:
SUBMITTER JOB TITLE:	SUBMITTER IS PRIVACY OFFICER: YES ☐
REQUIREMENT	**RESPONSE**

1. An acknowledgement that the HIC or the Agents or ESPs of the HIC caused the Privacy Breach	
2. The name of each Agent and Electronic Service Provider of the HIC that caused the Privacy Breach, whether intentional or not.	
3. The name of each HIC that created and contributed the PHI to the EHR	
4. The date and time of the Privacy Breach	
5. A description of the nature and scope of the Privacy Breach	
6. A description of the PHI in the EHR that was subject to the Privacy Breach	
7. The individuals who whom the PHI in the EHR relates	
8. The measures implemented to contain the Privacy Breach	
9. Any request for assistance from Ontario Health (Digital Services) and/or other HICs in containing the Privacy Breach	
10. Sufficient information to assist with the notification of the individuals to whom the PHI relates in accordance with PHIPA	

Form 2:

PRIVACY BREACH REPORT
Date report last updated: Version number of report: Is this the final version of the report?
1. 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 (Critical, Severe, Moderate, Minor, Near Miss):

Person responsible for causing the Privacy Breach (if relevant and known):
Does the breach involve a shared system? If so, please identify which one(s).

Breach Type	Was the Breach? *
☐ Collection ☐ Use ☐ Disclosure ☐ Retention ☐ Destruction ☐ Mishandling ☐ Other, explain:	☐ Unintentional ☐ Intentional

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 *

9. Policy Change History

Revision Number:	1
Date of Approval:	September 30, 2020
Replaces Policy:	Electronic Health Record Privacy Incidents and Privacy Breaches Policy, March 26, 2018
Description of Change:	N/A