



**Ontario
Health**

Privacy and Security Training and Awareness Policy and Procedure

Policy Level Approval:	Chief Executive Officer
Policy Category:	Corporate Policy
Policy Number:	INF-018.02-PP
Sensitivity Level:	Protected A
Policy Sponsor (or Sponsors):	Chief, Strategy, Planning, Privacy & Analytics and Senior Vice President, Digital Excellence in Health
Original Date of Approval:	November 11, 2021
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

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

1.1.1. The purpose of this policy is to set out:

- The requirement for Employees and other Ontario Health (OH) Agents to complete onboarding, annual and role-based privacy and security training;
- To identify the minimum contents for privacy and security training;
- To document the process, roles and responsibilities for creating, delivering and tracking privacy and security training; and
- Address the responsibilities and mechanisms with respect to fostering a culture of privacy and security and establishing awareness of privacy and security obligations at OH.

1.2. Objectives

1.2.1. To facilitate OH's compliance with:

- *The Personal Health Information Protection Act (PHIPA), Freedom of Information and Protection of Privacy Act (FIPPA), and associated regulations;*
- *The Information and Privacy Commissioner's (IPC's) Manual for the Review and Approval of Prescribed Organizations and Manual for the Review and Approval of Prescribed Persons and Prescribed Entities; and*
- IPC orders, *guidelines* and industry best practices for the protection of privacy.

1.2.2. To raise Employee's and other OH Agent's understanding of their privacy and security obligations to protect privacy and the confidentiality of Personal Health Information (PHI) and Personal Information (PI) that is received or managed by OH.

1.3. Application and Scope

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

1.4. Compliance, Audit, Enforcement and Exemptions

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 & Compliance Policy*.

- 1.4.3. At the first reasonable opportunity upon identifying or becoming aware of a breach of this Policy, Employee(s), or other OH Agents must notify the Privacy Office by reporting the breach to OH Service Desk by phone: 1-866-364-4373; or email: oh-servicedesk@ontariohealth.ca.
- 1.4.4. Breaches of this Policy will be managed in accordance with the OH *Privacy Incident Management Policy and Procedure and the Information Security Incident Management Standard*.
- 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. Policy

2.1. General

- 2.1.1. All Employees and other OH Agents complete:
 - Initial onboarding privacy and security training within 30 days of employment, contractual or other relationship with OH and prior to the Collection, viewing, accessing, Using, handling, Disclosing, or otherwise dealing with any PHI or PI received or managed by OH, including PHI or PI that has been de-identified and/or aggregated (i.e. Aggregated Data and De-identified Data);
 - Ongoing privacy and security training on an annual basis thereafter;
 - Role-based training as directed by the Privacy or Information Security Offices, or the Employee or Agent’s Manager or Director;
 - Ongoing Phishing Campaigns.
- 2.1.2. The privacy and security training includes the content listed in Appendix A.

2.2. Logging

- 2.2.1. A log of all initial and ongoing privacy and security training is maintained by OH.
- 2.2.2. A log of all initial and ongoing privacy and security training that is delivered through the Learning Management System (**LMS**) (including the agency-wide privacy and security training courses that are required to be completed during employee and agent onboarding (“initial” training) and on an annual basis (“ongoing” training), as well as the EHR role-based privacy and security training (also “initial” training)), is maintained within the LMS.

- 2.2.3. All other relevant privacy and security training (additional role-based training and/or communications, for example, to employees who may not access PHI, but have a role in safeguarding PHI, to employees who may investigate a privacy or security breach, to employees who may respond to a privacy inquiry, etc.), is logged in the Privacy Training and Awareness Log or Security Training and Awareness Log, as applicable.
- 2.2.4. A consolidated log for LMS delivered privacy and security training, and a consolidated log for non-LMS delivered privacy and security training, can be produced in a reasonably timely manner if requested.

3. Procedure

3.1. Privacy and Security Training Content

- 3.1.1. The CPO or delegate, and the SVP, Digital Excellence in Health or delegate, are responsible for creating and reviewing the content for all privacy and security training.
 - In creating and reviewing the content, consideration will be given to the minimum contents required for privacy and security training as listed in Appendix A.
- 3.1.2. Initial and ongoing privacy and security training is formalized and standardized and be based on evolving industry privacy standards and best practices.
 - In developing the training content, the CPO or delegate, and the SVP, Digital Excellence in Health or delegate, considers evolving industry privacy and security standards and best practices.
- 3.1.3. The CPO or delegate, and the SVP, Digital Excellence in Health or delegate, reviews all privacy and training content annually at a minimum.

3.2. Training Delivery

Onboarding¹ and Annual² Privacy and Security Training

- 3.2.1. The Privacy and Security onboarding and annual training will be delivered electronically to Employees and other OH Agents, primarily through the LMS managed by Human Resources (HR).
- 3.2.2. Upon receiving the content of the privacy and security training, a designated member of the HR team is responsible for uploading and managing the training content in the LMS.

¹ Onboarding training is considered part of 'initial training', as are role-based training courses that are required to be complete prior to an Employee or OH Agent being permitted to collect, access, view, use, disclose, handle or otherwise deal with PHI or PI.

² Annual training is considered part of 'ongoing training' as are role-based training courses that are provided on a periodic basis after initial training.

- 3.2.3. The designated member of the HR team is responsible for enrolling Employees and OH Agents in the onboarding and annual privacy and security training courses, in accordance with the *Mandatory Training Standard*.
- 3.2.4. The *Mandatory Training Standard* sets out the process for notifying HR when an Employee or other OH Agent has commenced or will commence an employment, contractual or other relationship with the prescribed organization, including:
 - The Employee or other OH Agent responsible for providing this notification to HR;
 - The timeline for which the notification must be provided; and
 - The format of the notification.

Role-based Privacy and Security Training

- 3.2.5. Role-based privacy and security training may be delivered to Employees and other OH Agents *through* a variety of means, including for example, electronically through the LMS, in-person or through virtual presentations made to portfolios or project teams.

3.3. Tracking and Logging Initial and Ongoing Training

Initial and Ongoing Training through LMS:

- 3.3.1. For privacy and security training that is delivered through the LMS, HR is responsible for logging the attendance and completion of the training.
- 3.3.2. HR is responsible for tracking and logging:
 - The name of the Employee or other OH Agent and the date that the Employee or other OH Agent commenced their employment, contractual or other relationship with OH (this is maintained in the HR electronic Workday System);
 - The name of the Employee or other OH Agent and date that the Employee or other OH Agent attended or completed the privacy or security training (this is maintained in the HR electronic LMS); and
 - The nature of the privacy and/or security training delivered.
- 3.3.3. Once an Employee or other OH Agent completes the privacy or security training course, including a quiz and/or knowledge check and a training acknowledgement statement, the LMS automatically tracks that the Employee or other OH Agent has completed the training, including the name of the Employee or other OH Agent, and the date and time that the training is complete.
- 3.3.4. The LMS will provide weekly automatic reminders to Employees and other OH Agents if training is not complete.
- 3.3.5. Course completion and remedial action required with regards to non-completion of the privacy and security training will be done in accordance with the *Mandatory Training Standard* and *Progressive Discipline Policy*.

Initial and Ongoing Training delivered outside of LMS:

- 3.3.6. For privacy and security training that is delivered outside of LMS, the Employee or other OH Agent who provides or delivers the role-based training, is responsible for logging the attendance and completion of the training in the Privacy Training and Awareness Log or Security Training and Awareness Log.

3.3.7. The Privacy Training and Awareness Log or the Security Training and Awareness Log includes the following information:

- The name of the Employee or other OH Agent who completed or attended the training; and
- The nature of the privacy or security training.

3.3.8. The Privacy Training and Awareness Log or the Security Training and Awareness Log will be maintained by the Privacy Office or the Information Security Office, respectively, in the designated shared drive or SharePoint site for Privacy or Information Security.

4. Privacy and Security Awareness

4.1. General Privacy and Security Awareness

4.1.1. The CPO or delegate, and SVP, Digital Excellence in Health or delegate, are accountable for ensuring that OH employs a variety of methods to foster a culture of privacy and security and to raise awareness of PHIPA, FIPPA, the privacy and security programs, and the privacy and security policies, procedures and practices implemented by OH.

4.1.2. The mechanisms used to increase privacy and security awareness include, for example, awareness training campaigns, intranet discussion groups, posters, calendars, presentations in celebration of International Privacy Day and Cyber Security Awareness month, and privacy and security presentations tailored for particular OH portfolios or business units.

4.2. Phishing Campaigns

4.2.1. To enhance information security awareness among OH employees and individuals acting on its behalf, phishing campaigns are conducted monthly by the Information Security Office as part of the Privacy and Security Training and Awareness Program. These campaigns are structured to simulate real-world phishing attempts and assess employees' ability to identify and report suspicious activities.

4.2.2. The following practices support the effective implementation of this mechanism:

- **Frequency:** Phishing campaigns are executed on a monthly basis, ensuring consistent exposure to evolving phishing tactics.
- **Method:** Simulated phishing emails are designed to mimic current phishing trends and are distributed via the organization's email system. These campaigns provide immediate feedback to participants, including educational materials for incorrect responses. These training modules aim to address specific gaps identified during the campaign and are tracked for completion.
- **Nature of Communication:** Post-campaign communications include detailed analyses of results, highlighting organizational performance and areas for improvement. Reports are shared with DXH management and OH board of directors.
- **Responsible Parties:** The Security Awareness and Training team is responsible for designing, implementing, and analyzing phishing campaigns. Oversight is provided by

the Information Security Office, which ensures alignment with organizational policies and objectives.

5. Responsibilities

5.1. Chief Privacy Officer or Delegate and Senior Vice President, Digital Excellence in Health or Delegate

- Ensuring Employees and other OH Agents are aware of the privacy and security policies, procedures and practices implemented by OH and are appropriately informed of their duties and obligations thereunder; and
- Overseeing the development, review and delivery of privacy and security training and awareness.

5.2. Human Resources

- Maintaining the ongoing and initial privacy and security training courses in the LMS;
- Logging the completion of privacy and security courses through the LMS; and
- Enrolling Employees and OH agents in privacy and security training upon the start of their employment, contractual or other relationship with OH.
- Tracking completion of training modules and notifying manager and director of incomplete training in accordance with *Mandatory Training Standard*.

5.3. Privacy Office and Information Security Office

- Creating, delivering, and logging role-based training and other mechanisms to raise privacy and security awareness among Employees and other OH Agents in accordance with this Policy.

6. Definitions and Acronyms

Terms not defined within the body of this Policy and Procedure are set out in OH's Privacy Policy.

Term / Acronym	Definition
Aggregate Data	Data that is summed and/or categorized in a manner that prevents the ability to reveal an individual's identity (individual records cannot be reconstructed). Aggregate data does not include PHI or PI.

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.
CPO	Chief Privacy Officer
De-identified Data	Data which has any information that identifies the individual removed. It is not reasonably foreseeable in the circumstances that the data could be utilized, either alone or with other information, to identify an individual.
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 <i>Employee Classification Guideline</i> . A consultant or contractor is not an Employee.
FIPPA or Freedom of Information and Protection of Privacy Act, 1990	Ontario legislation with two main purposes: 1) to make provincial government institutions more open and accountable by providing the public with a right of access to records; and 2) to protect the privacy of individuals with respect to their Personal Information held by provincial government organizations. References to FIPPA include the regulations made thereunder, as may be amended or replaced from time to time.
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
Minister	Minister of Health
OH	Ontario Health, the agency of the Government of Ontario to which this Policy applies.

Term / Acronym	Definition
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	<p>Has the meaning set out in section 4 of PHIPA. Specifically, it is “identifying information” in oral or recorded form about an individual that:</p> <ul style="list-style-type: none"> • 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. <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.</p> <p>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>
PHIPA or <i>Personal Health Information Protection Act, 2004</i>	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.

Term / Acronym	Definition
PI or Personal Information	<p>Has the meaning set out in section 2 of FIPPA. Specifically, it means recorded information about an identifiable individual, including:</p> <ul style="list-style-type: none"> • 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. <p>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.³</p>
Prescribed Entity or PE	<p>An entity that is prescribed in Ontario Regulation 329/04 for the purposes of s. 45 of PHIPA, to which a HIC is permitted to Disclose PHI, without the consent of the individual to whom the information relates, for the purpose of analysis or compiling statistical information for the management, evaluation, or monitoring of the allocation of resources to, or planning for, all or part of the health system, including the delivery of services.</p>
Prescribed Organization or PO	<p>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.</p>

³ Section 38 (1) FIPPA

Term / Acronym	Definition
Prescribed Person or PP	A person that is prescribed in the regulations for the purposes of s. 39(1)(c) of PHIPA, to which a HIC is permitted to Disclose PHI, without the consent of the individual to whom the information relates, to such person who maintains a registry of PHI for purposes of facilitating or improving the provision of health care or that relates to the storage or donation of body parts or body substances.
Prescribed Registry or PR	A registry of PHI that is prescribed in Ontario Regulation 329/04 maintained for the purpose of enabling or improving the provision of health care or that relates to the storage or donation of body parts or bodily substances.
Privacy Breach	<p>A Privacy Breach includes:</p> <ol style="list-style-type: none"> 1) Privacy Breach of PHI or PI (Privacy PHI/PI Breach) means an event where: <ul style="list-style-type: none"> • 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. <p>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.</p> 2) Privacy Breach of Privacy Policy or Agreement (Privacy Policy/Agreement Breach) means an event where: <ul style="list-style-type: none"> • There is a contravention of OH's privacy policies, procedures, or practices; and/or • There is a contravention of a privacy-related⁴ term or condition in a: <ul style="list-style-type: none"> ○ 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 <p>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.</p>

⁴ A privacy-related term or condition, includes terms or conditions that relate to privacy requirements from law (including, for example, FIPPA, PHIPA and GOLLA), 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
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.

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

- Privacy Incident Management Policy and Procedure
- Privacy Audit and Compliance Policy
- Mandatory Training Standard

9. Appendices

- Appendix A: Required Content of Training

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 and security policies in reference to OH’s privacy and security requirements.
 - Working Group members of the Privacy Program Advisory Committee (Version 1 of the Policy)
 - Information Security Office

Policy Review History

Date of Review DD/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

29-11-2023	<ul style="list-style-type: none"> • Updated to reflect changes of course completion and remedial actions. • 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, and Privacy Breach Updated compliance will be enforced in accordance with the <i>Progressive Discipline Policy</i> 	N/A		
------------	--	-----	--	--

Policy Repeal

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

Appendix A - Content Required in Privacy and Security Training

The Initial Privacy Training addresses:

- A description of the OH's role pursuant to Part V.1 of the PHIPA and the duties and responsibilities that arise as a result;
 - A description of the OH's role as a Prescribed Entity and Prescribed Person under PHIPA and the duties and responsibilities that arise as a result;
- A description of the nature and purposes for which PHI is provided to OH by HICs and other organizations as permitted under PHIPA or FIPPA;
- The purposes for which Employees and other OH Agents may view, handle, or otherwise deal with PHI received for the purpose of developing or maintaining the electronic health record (**EHR**);
 - Limitations placed on the Collection, viewing, handling, Using, Disclosing or otherwise dealing with PHI by Employees and other OH Agents;
 - Notice that all instances in which PHI in the EHR is viewed, handled or otherwise dealt with by any person will be logged, audited and monitored;
 - Limitations, conditions or restrictions placed on the PHI or PI, including a prohibition on Collecting, viewing, handling, Using, Disclosing or otherwise dealing with PHI or PI if other information such as de-identified and/or aggregate information, will serve the permitted purpose and on Collecting, viewing, handling, Using, Disclosing, or otherwise dealing with more of the PHI or PI that is necessary;
 - A description of the procedure that must be followed in the event that an employee or other OH Agent is requested to apply a consent directive to PHI in the EHR is developed or maintained by the OH;
 - A description of the procedure that must be followed in the event that an employee or other OH Agent is requested to provide PHI to the Minister of Health (**Minister**), or another person as directed by the Minister;
 - An overview of the privacy policies, procedures and practices that have been implemented by OH and the obligations arising from these policies, procedures and practices;
 - The consequences of breach of the privacy policies, procedures and practices implemented;
 - An explanation of the privacy program, including the key activities of the program and the employee(s) and other OH Agents that have been delegated day-to-day authority to manage the privacy program;

- The administrative, technical and physical safeguards implemented by OH to ensure that any PHI received or managed by OH is not Collected, without authority and is protected against theft, loss and unauthorized Use or Disclosure and that records of PHI received are protected against unauthorized copying, modification or disposal;
- The duties and responsibilities of employees and other OH Agents in implementing the administrative, technical and physical safeguards put in place by OH;

The purposes for which PHI received by OH for the purpose of developing or maintaining the EHR, which has been de-identified or aggregated, may be viewed, handled or otherwise dealt with by employees or other OH Agents;

The purposes of using de-identified or aggregate information, derived from PHI collected by OH as a PP or PE may be used or disclosed;

A prohibition on using de-identified or aggregate information, either alone or with other information, to identify an individual, unless the re-identified information is done in accordance with the De-Identification Guidelines or permitted by PHIPA or another Act;

- Notice that compliance with the prohibition on using de-identified or aggregated information to identify an individual will be audited and monitored;
- A discussion of the nature and purpose of the Privacy Notices, Confidentiality Agreements and End User Agreements that employees and other OH Agents must execute and the key provisions of these notices and agreements; and

An explanation of the Policy and Procedures for Privacy Breach Management and the duties and responsibilities imposed on employees and other persons acting on behalf of OH in identifying, reporting, containing and participating in the investigation and remediation of privacy breaches, including the duty to provide notice at the first reasonable opportunity of a privacy breach or suspected privacy breach.

An explanation of the mandatory nature of privacy training, including prohibition on all OH Agents and employees to handle PHI without having completed initial privacy training and of ongoing privacy training on an annual basis thereafter.

Content of Ongoing Privacy Training

Ongoing training:

Includes role-based training in order to ensure that Employees and other OH Agents understand how to apply the privacy policies, procedures and practices in their day-to-day employment, contractual or other responsibilities, as these may have evolved since their last training;

- Addresses any new privacy policies, procedures and practices and significant amendments to existing privacy policies, procedures and practices; and
- Takes into account any:

- Recommendations with respect to privacy training made in privacy impact assessments, privacy audits and the investigation of privacy breaches and privacy complaints;
- Orders, decisions, guidelines, fact sheets and best practices issued by the IPC under PHIPA and its regulations; and
- Amendments to PHIPA and its regulations relevant to OH.

Initial Security Training addresses:

- An overview of the security policies, procedures and practices that have been implemented by OH and the obligations arising from these policies, procedures and practices;
- The consequences of breach of the security policies, procedures and practices implemented;
- An explanation of the security program, including the key activities of the program and the employee(s) and other person(s) acting on behalf of OH that have been delegated day-to-day authority to manage the security program;
- The administrative, technical and physical safeguards implemented by OH to ensure that PHI accessible by means of the EHR is not collected without authority and is protected against theft, loss and unauthorized use or disclosure and that records of PHI accessible by means of the EHR are protected against unauthorized copying, modification or disposal;
- The duties and responsibilities of employees and other OH Agents in implementing the administrative, technical and physical safeguards put in place by OH; and
- An explanation of the Policy and Procedures for Information Security Breach Management and the duties and responsibilities imposed on employees and other persons acting on behalf of OH in identifying, reporting, containing and participating in the investigation and remediation of information security breaches.

Content of Ongoing Security Training

Ongoing training:

- Includes role-based training in order to ensure that Employees and other OH Agents understand how to apply the security policies, procedures and practices in their day-to-day employment, contractual or other responsibilities;
- Addresses any new security policies, procedures and practices and significant amendments to existing security policies, procedures and practices; and
- Takes into account any:
 - Recommendations with respect to security training made in security audits, privacy impact assessments and the investigation of information security breaches;

- Orders, decisions, guidelines, fact sheets and best practices issued by the IPC under PHIPA and its regulations; and
- Amendments to PHIPA and its regulations relevant to the Minister and OH.