eHealth Ontario
It's working for you.

TRAINING STRATEGY - PRIVACY AND SECURITY TRAINING FOR ONTARIO'S ELECTRONIC HEALTH RECORD

Last Edited: July 2017
Document Owner: eHealth Ontario Privacy Office

If you have any questions or require further clarification, please contact privacy@ehealthontario.on.ca.

Ontario
eHealth Ontario

Privacy and Security Training

Overview

The *Electronic Health Record Privacy and Security Training Policy* requires the completion of privacy and security role-based training to agents and Electronic Service Providers of Health Information Custodians participating in the Electronic Health Record. This document provides an outline of the training delivery options and the resources available to your organization.

Privacy and security training materials available in the ConnectingOntario Privacy Toolkit enable Health Information Custodians and eHealth Ontario to train their agents and Electronic Service Providers who collect, use or disclose PHI in the Electronic Health Record or who view, handle or otherwise deal with PHI in the Electronic Health Record, as the case may be, on their privacy and security duties and obligations.

These materials have been developed and approved by the C*onnectingPrivacy Committee* leveraging existing privacy and security training materials, in consultation with the Regional Privacy and Security Working Groups, Regional Clinical Working Groups, the Information and Privacy Commissioner of Ontario and the Ministry of Health and Long Term Care.

How to Navigate This Document

1. Organization's Training Profile
2. Delivery Timing and Tracking
3. E-Learning Courses Specifications
4. AODA Compliance
5. Roles- *for the various roles within organizations, please see the slide number reference below*

Role	Slides
Privacy Officer/ Security Officer	8, 9
Clinical End Users	10
Technical and Operational Support	11
Local Registration Authority and Sponsor	12

6. FAQs

Note: This documents only addresses the training requirements to comply with the *Electronic Health Record Privacy and Security Training Policy* and does not address other training requirements that may be applicable.

1. Organization's Training Profile

The following options are available to your organization or practice depending on the training methods currently in place:

Your organization or practice's training profile	Recommendation
1. No existing privacy or security training and no existing training delivery resources	Delivery: User to complete the E-Learning Course Tracking: User prints certificate of completion and provides copy to person responsible for tracking at your organization
2. No existing privacy or security training, has a Learning Management System	Delivery: Upload Articulate or Captivate SCORM-compliant E-Learning file Tracking: LMS tracks completion of training
3. Has existing privacy and security training and training delivery resources	Delivery: Leverage mandatory and foundational (where required) content into existing training via PowerPoint, PDF or editable Articulate Storyboard 1 file Tracking: existing privacy and security training tracking process

Once you have determined the appropriate delivery method your organization, leverage the materials in the Privacy Toolkit- references will be displayed here as (XX).

Checklists are available to support the planning and implementation activities for each training course. Checklists provide instruction on what content is required, foundational and supplementary.

2. Delivery Timing and Tracking

Refer to the table below to identify when the training must be delivered for a user's role and who is responsible for tracking.

Course	Delivery Timing	Tracking
Privacy Officer/ Security Officer	Prior to completion of Readiness Assessment, scheduled by Privacy/Security Onboarding Lead	Privacy/Security Onboarding Lead is responsible for tracking training for Privacy and Security Officers and will maintain a tracking log
Clinical End Users	Prior to accessing the system and annually thereafter	Sites are responsible for tracking training for their agents and ESPs
Technical and Operational Support	Prior to accessing the system and annually thereafter (as applicable)	Sites are responsible for tracking training for their agents and ESPs
Local Registration Authority and Sponsor	Prior to granting users access to the system and annually thereafter (as applicable)	Sites are responsible for tracking training for their agents and ESPs

Tracking: your organization may leverage the *Privacy Training Log* in the *Privacy Toolkit*, retain copies of the printed *Certificate of Completion* or via your Learning Management System. Confirmation of training completion prior to on-boarding must be reported to your Account Manager.

3. e-Learning Courses

Where available, e-Learning courses were developed using the following software:

Articulate Storyboard version 1

- Sharable Content Object Reference Model (SCORM) 1.2, 2004 compliant

Adobe Captivate 6

- Forward compatible

E-Learning Course Features

- Text
- Images (characters and Viewer screenshots)
- Transitions and pop-ups
- Voiceover
- Quiz
- Certificate of Completion

Please note eHealth Ontario is unable to provide technical support for the e-Learning files.

4. AODA Compliance

All training materials text size will be at least 13 and illustrations will be limited to characters only.

There will be a downloadable/printable PDF of the e-Learning Modules (where applicable) in the Privacy Toolkit with larger-font (approximately size 16) of the e-Learning Module for reference.

5. Roles - Privacy Officer

10.A./10.B.

Role description: corresponds to the individual identified in the EHR Contributor Agreement.

Delivery Methods:

1. Greater Toronto Area and Northern and Eastern Ontario Viewing and/or Contributing: Webinar and Teleconference hosted by Privacy Onboarding Lead (10.A)
2. South Western Ontario Viewing and/or Contributing: Webinar and Teleconference hosted by Privacy Onboarding Lead (10.B)

Duration: approximately 90 minutes

Content:

1. Overview of ConnectingOntario/ DHDR
2. ConnectingOntario Privacy Readiness Assessment
3. Privacy and Security Overview
4. Privacy and Security Obligations for HICs
5. Privacy Operations
6. Assurance
7. Breach Management
8. Contact Information
9. Appendix

5. Roles - Security Officer

10.A./10.B.

Role description: corresponds to the individual identified in the EHR Contributor Agreement.

Delivery Methods:

1. Viewing: EHR Security Overview Webinar for Viewing Organizations using ONE ID or ClinicalConnect accounts
2. Contributing: Webinar and Teleconference hosted by Security Onboarding Lead (10.A/10.B)

Duration: approximately 90 minutes

Content:

1. Overview of ConnectingOntario/DHDR
2. Privacy and Security Overview
3. Privacy and Security Obligations for HICs
4. Information Security Policies
5. Assurance
6. Incident Management
7. Contact Information
8. Appendix

5. Roles - Clinical End User

Checklist (11.A)

Role description: users providing or assisting in the provision of health care. Refer to *ConnectingOntario – Guidance to Support Identifying End Users*.

Delivery Methods:

1. E-Learning:
   - eHealth Ontario Website
   - Articulate file to be embedded in existing LMS (11.E)
   - Articulate file to be customized (11.F)
   - Captivate file to be customized (11.G)
2. Classroom/ Other:
   - Microsoft PowerPoint/ Adobe PDF (11.B)
     - Glossary (11.C)
     - Question Bank (11.D)

Duration: approximately 15 minutes

Content:

1. What is Ontario's Electronic Health Record?
2. Why do I need to complete this training?
   - Privacy Background (i.e. PHIPA, PHI)
3. What are my privacy and security requirements as a user of Ontario's Electronic Health Record?
   - Rules on Viewing Personal Health Information
   - Understanding Individual Consent
   - Consent Directives
   - Overriding Consent Directives
   - Understanding Access and Correction
   - How to Deal with Questions and/or Complaints
   - Understanding Privacy Breaches and Security Incidents
   - My Role in a Privacy Breach or Security Incident
   - Privacy and Security Do's and Don'ts
   - Privacy and Security Safeguards
4. Quiz

5. Roles - Technical and Operational Support

Checklist (12.A)

Role description (where applicable*): Administrators (Portal, System, etc);Testers (Quality Assurance, Performance, Clinical Validation); Site Help Desk

Delivery Methods:

1. E-Learning:
   - eHealth Ontario Website
   - Articulate file to be embedded in existing LMS (12.E)
   - Articulate file to be customized (12.F)
2. Classroom/ Other:
   - Microsoft PowerPoint/ Adobe PDF (12.B)
     - Glossary (12.C)
     - Question Bank (12.D)

Duration: approximately 15 minutes

Content:

1. What is Ontario's Electronic Health Record?
2. Why do I need to complete this training?
   - Privacy Background (i.e. PHIPA, PHI)
3. What are my privacy and security requirements as a user of Ontario's Electronic Health Record?
   - Role-based Expectations
     - Administrator
     - Tester
     - Clinical Validator
     - Help Desk
     - TELUS Service
     - eHealth Ontario
   - Understanding Privacy Breaches and Security Incidents
   - My Role in a Privacy Breach or Security Incident
   - Privacy and Security Do's and Don'ts
   - Privacy and Security Safeguards
4. Quiz

*Roles may not be applicable when the organization is viewing only.

5. Roles - Local Registration Agent and Sponsor

Checklist (13.A)

Role description: - Local Registration Agents; Sponsors

Delivery Methods:

1. E-Learning:
   - eHealth Ontario Website
   - Articulate file to be embedded in existing LMS (13.E)
   - Articulate file to be customized (13.F)
2. Classroom/ Other:
   - Microsoft PowerPoint/ Adobe PDF (13.B)
     - Glossary (13.C)
     - Question Bank (13.D)

Duration: approximately 15 minutes

Content:

1. What is Ontario's Electronic Health Record?
2. Why do I need to complete this training?
   - Privacy Background (i.e. PHIPA, PHI)
3. As a Local Registration Agent or Sponsor of Ontario's Electronic Health Record, what is expected of me?
   - Expectations for your Organization
   - Registering and Enrolling Users
   - AL2 Requirements
   - Entitlement Criteria
   - Revoking/Suspending Access
   - Maintaining a Record of Enrolled Users
   - Understanding Privacy Breaches and Security Incidents
   - My Role in a Privacy Breach or Security Incident
   - Privacy and Security Do's and Don'ts
   - Privacy and Security Safeguards
4. Quiz

6. FAQs

#1

I perform multiple roles at my organization, what training am I required to complete?

Where an individual has multiple roles, each training course must be completed for each role. For example, if individual is both a Tester and Privacy Officer, this individual must complete the Technical Support training and the Privacy Officer training.

The only exception is sole practitioners: only the Privacy and Security Clinical End User training module needs to be completed.

6. FAQs

#2

How often do I need to deliver training?

Training must be provided prior to accessing the system and annually thereafter, as applicable.

For example, a physician that is registered to the ConnectingOntario ClinicalViewer and their account has been active over a year, this user is required to complete training. A tester that has access to the system during on-boarding but no longer as access to the system, does not need to receive training.

6. FAQs

#3

The training references systems and repositories my organization does not participate in, won't my staff be confused?

The training developed for Ontario's Electronic Health Record is provincial training that includes privacy and security requirements for systems and repositories managed by eHealth Ontario:

- ConnectingOntario Clinical Data Repository
- Diagnostic Imaging Common Services
- Ontario Laboratory Information System
- Digital Health Drug Repository

If your organization does not currently participate in this initiative, you may amend the training in accordance with the checklist(s) or communicate the availability of the system/ repository to your staff.

6. FAQs

#4

There is a technical issue with the training or the certificate of completion is not displayed/cannot be printed- how can I complete training delivery?

If you experience issues with the file or your users are experiencing a technical issue with the e-Learning course, please choose an alternative method of delivering the training and please indicate successful review of the training using the log template from *4 Templates for Privacy Logs* in the EHR Privacy Toolkit.

Note: eHealth Ontario is unable to provide technical support for e-Learning.

6. FAQs

#5

My organization just completed our annual privacy and security training, do users need to be re-trained before go-live?

Users must be trained on the required messages as identified in the Checklists prior to accessing the system.

Tip: much of the content may have already been covered in the annual training therefore your organization only needs to deliver the messages that are new.

Ensure you track the delivery of the new messages.