eHealth Ontario

Privacy and Security Training Policy

Electronic Health Record

Version: 1.2

Document ID: 3877

Ontario
eHealth Ontario

Document Control

The electronic version of this document is recognized as the only valid version.

Approval History

APPROVER(S)	APPROVED DATE
ConnectingPrivacy Committee Members	September 24, 2015

Revision History

VERSION NO.	DATE YYYY-MM-DD	SUMMARY OF CHANGE	CHANGED BY
1.2	2015-11-25	Minor revisions – updated for ConnectingOntario	Samara Strub, Privacy Analyst, eHealth Ontario
1.1	2015-09-24	Revision to reflect requirement to deliver privacy and security training.	Promila Gonsalves, Sr. Privacy Business Analyst, eHealth Ontario
1.0	2014-11-17	Final version	Urooj Kirmani, Senior Privacy Analyst, eHealth Ontario
0.01	2014-11-04	Initial draft based on ConnectingPrivacy Committee Harmonized Privacy and Security Training Policy v1.0.	Promila Gonsalves, Privacy Analyst, eHealth Ontario

1 Contents

1 Purpose/ Objective

To define the policies, procedures and practices for providing privacy and security training in respect of the Electronic Health Record (EHR).

2 Scope

This policy and its associated procedures apply to the provision of privacy and security training in respect the EHR. The EHR is comprised of the ConnectingOntario Solution and the Diagnostic Imaging Common Services Repository. The ConnectingOntario Solution and the Diagnostic Imaging Common Services Repository are classified as clinical repository and/or ancillary systems designed to store and make available specified electronic PHI from the electronic health information systems of HICs[1].

This policy and its associated procedures do not apply to privacy and security training:

- In respect of any system other than the EHR;
- In respect of any information other than personal health information (PHI) in the EHR;
- To agents of HICs who do not collect, use or disclose PHI in the EHR;
- To Electronic Service Providers of HICs who do not view, handle or otherwise deal with PHI in the EHR; or
- To agents or Electronic Service Providers of eHealth Ontario who do not view, handle or otherwise deal with PHI in the EHR.

This policy and its associated procedures also do not apply to basic privacy and security training provided by HICs and eHealth Ontario to their agents and Electronic Service Providers.

3 Policy

3.1 Guiding Policies

3.1.1 The *Personal Health Information Protection Act, 2004* (PHIPA) requires a HIC that is not a natural person, such as a HIC that is a corporation or partnership, to designate a contact person to facilitate the HIC's compliance with PHIPA and to ensure that all agents of the HIC are appropriately informed of their duties under PHIPA.

3.1.2 PHIPA permits a HIC that is a natural person to designate a contact person to facilitate the HIC's compliance with PHIPA and to ensure that all agents of the HIC are appropriately informed of their duties under PHIPA. Where a HIC that is a natural person does not designate a contact person to perform these functions, the HIC is required to perform these functions on his or her own.

3.1.3 PHIPA requires eHealth Ontario to ensure that those acting on its behalf agree to comply with conditions and restrictions necessary to enable eHealth Ontario to comply with PHIPA.

3.1.4 HICs and eHealth Ontario shall have in place and maintain policies, procedures and practices in respect of privacy and security that are necessary to enable them to comply with their obligations under PHIPA, applicable agreements and this policy and its associated procedures.

[1] Variance in policy and procedure requirements between the ConnectingOntario Solution and the Diagnostic Imaging Common Services Repository is highlighted within the policy.

3.1.5 **Connecting Ontario**

HICs and eHealth Ontario shall have in place and maintain policies, procedures and practices in respect of privacy and security that comply with PHIPA and provide training to their agents and Electronic Service Providers on the policies, procedures and practices as required by PHIPA.

Diagnostic Imaging Common Services Repository

Throughout this policy for Diagnostic Imaging Common Services Repository, wherever training is noted, it is sufficient for HICs and eHealth Ontario to have in place and maintain policies, procedures and practices in respect of privacy and security that comply with PHIPA to appropriately inform their agents and Electronic Service Providers on the policies, procedures and practices as required by PHIPA.

3.1.6 HICs and eHealth Ontario shall take steps that are reasonable in the circumstances to ensure that their agents and Electronic Service Providers comply with PHIPA, applicable agreements and this policy and its associated procedures.

4 Procedure

4.1 Procedures Related to Creating Privacy and Security Training Materials by eHealth Ontario

4.1.1 eHealth Ontario shall develop and distribute privacy and security training materials to enable HICs and eHealth Ontario to train their agents and Electronic Service Providers who collect, use or disclose PHI in the EHR or who view, handle or otherwise deal with PHI in the EHR, as the case may be, on their privacy and security duties and obligations.

4.1.2 eHealth Ontario shall ensure that the privacy and security training materials are role-based to enable HICs and agents and Electronic Service Providers of HICs and eHealth Ontario to understand how to meet their duties and obligations in respect of the EHR in their day-to-day operations.

4.1.3 At a minimum, the privacy and security training materials shall include the information described in paragraph 4.4.1.

4.1.4 eHealth Ontario shall review and refresh the privacy and security training materials every two years or earlier in circumstances where amendments to PHIPA, applicable agreements or the policies, procedures and practices in respect of privacy and security that have been implemented in relation to the EHR will impact the duties and obligations of HICs, eHealth Ontario and/or their agents and Electronic Service Providers in relation to the EHR.

4.2 Procedures Related to Delivering Privacy and Security Training

4.2.1 HICs shall provide privacy and security training to their agents and Electronic Service Providers[2] to ensure that they are appropriately informed of their duties under PHIPA, applicable agreements and the policies, procedures and practices in respect of privacy and security implemented in relation to the EHR, prior to permitting their agents and Electronic Service Providers to collect, use or disclose PHI in the EHR or to view, handle or otherwise deal with PHI in the EHR, as the case may be and at a minimum every year thereafter.

4.2.2 eHealth Ontario shall provide privacy and security training to its agents and Electronic Service Providers to ensure that they are appropriately informed of their duties under PHIPA, applicable agreements and the policies, procedures and practices in respect of privacy and security implemented in relation to the EHR, prior to permitting its agents and Electronic Service Providers to view, handle or otherwise deal with PHI in the EHR and at a minimum every year thereafter.

4.2.3 HICs and eHealth Ontario shall not permit their agents and Electronic Service Providers to continue to collect, use or disclose PHI in the EHR or to continue to view, handle or otherwise deal with PHI in the EHR, as the case may be, unless the agent or Electronic Service Provider has completed the ongoing privacy and security training.

[2] All references in this policy and its associated procedures to agents or Electronic Service Providers of a HIC or HICs are references to agents or Electronic Service Providers other than eHealth Ontario or agents and Electronic Service Providers of eHealth Ontario.

4.2.4 When providing privacy and security training to agents and Electronic Service Providers to ensure that they are appropriately informed of their duties under PHIPA, applicable agreements and the policies, procedures and practices in respect of privacy and security implemented in relation to the EHR, HICs and eHealth Ontario shall ensure that their agents and Electronic Service Providers are provided the information described in paragraph 4.4.1, if relevant to their day-to-day duties.

4.2.5 HICs and eHealth Ontario shall have in place and maintain policies, procedures and practices to identify agents and Electronic Service Providers who do not complete initial and ongoing annual privacy and security training and to impose consequences on agents and Electronic Service Providers who do not complete the initial and ongoing annual privacy and security training.

4.2.6 HICs and eHealth Ontario shall maintain a log of all agents and Electronic Service Providers that have completed the initial and ongoing annual privacy and security training. The log shall include the:

- Name of the agent or Electronic Service Provider;
- Date that the agent or Electronic Service Provider completed the initial privacy and security training;
- Date that the agent or Electronic Service Provider completed the ongoing annual privacy and security training; and
- Anticipated date of the next privacy and security training.

4.3 Procedures Related to End User Agreements

4.3.1 eHealth Ontario shall ensure that the EHR requires HICs and agents and Electronic Service Providers of HICs and eHealth Ontario to acknowledge and agree to comply with the duties and obligations in the End User Agreement prior to collecting, using or disclosing PHI in the EHR or prior to viewing, handling or otherwise dealing with PHI in the EHR, as the case may be, and at a minimum, every year thereafter.

4.3.2 eHealth Ontario shall ensure that the EHR does not permit agents and Electronic Service Providers of HICs and eHealth Ontario to collect, use or disclose PHI in the EHR or to view, handle or otherwise deal with PHI in the EHR, as the case may be, unless the agent or Electronic Service Provider has acknowledged and agreed to comply with the duties and obligations in the annual End User Agreement.

4.3.3 eHealth Ontario shall develop and implement an End User Agreement that, at a minimum:

- Sets out the purposes for which HICs and agents and Electronic Service Providers of HICs are permitted to collect, use or disclose PHI in the EHR or to view, handle or otherwise deal with PHI in the EHR, as the case may be;
- Sets out the purposes for which agents and Electronic Service Providers of eHealth Ontario are permitted to view, handle or otherwise deal with PHI in the EHR;
- Requires HICs and agents and Electronic Service Providers of HICs and eHealth Ontario to acknowledge that they understand and agree to comply with the policies, procedures and practices in respect of privacy and security implemented in relation to the EHR;
- Requires HICs and agents and Electronic Service Providers of HICs and eHealth Ontario to agree to comply with PHIPA;
- Requires HICs and agents and Electronic Service Providers of HICs and eHealth Ontario to implement the administrative, technical and physical safeguards set out in the End User Agreement to protect PHI in the EHR;
- Requires HICs and agents and Electronic Service Providers of HICs and eHealth Ontario to provide notification in accordance with the *Electronic Health Record Privacy Breach Management Policy* and its associated procedures, as amended from time to time, or the *Electronic Health Record Information Security Incident Management Policy* and its associated procedures, as amended from time to time, as the case may be, if they believe that an actual or suspected Privacy Breach or an actual or suspected Security Breach has occurred or is about to occur in respect of the EHR; and
- Sets out the consequences of breach of the End User Agreement.

4.4 Privacy and Security Training Content

4.4.1 In providing privacy and security training in respect of the EHR, the following information shall be included where relevant to the day-to-day duties of the agent or Electronic Service Provider:

- The nature of PHI that is retained in the EHR;

- The status under PHIPA of eHealth Ontario and other organizations participating in the EHR and the duties and obligations arising from this status;
- The purposes for which HICs and their agents and Electronic Service Providers are permitted to collect, use and disclose PHI in the EHR or to view, handle or otherwise deal with PHI in the EHR, as the case may be, and the limitations placed thereon;
- The authority for the collection, use and disclosure of PHI in the EHR or the viewing, handling or dealing with PHI in the EHR, as the case may be, by HICs and their agents and Electronic Service Providers;
- The purposes for which PHI in the EHR is permitted to be viewed, handled or otherwise dealt with by eHealth Ontario and its agents and Electronic Service Providers and the limitations placed thereon;
- The authority for viewing, handling or dealing with PHI in the EHR by eHealth Ontario and its agents and Electronic Service Providers;
- An overview of the policies, procedures and practices in respect of privacy and security that have been implemented in relation to the EHR and the duties and obligations of HICs and agents and Electronic Service Providers of HICs and eHealth Ontario arising from these policies, procedures and practices;
- The consequences of breach of the policies, procedures and practices in respect of privacy and security that have been implemented in relation to the EHR;
- The administrative, technical and physical safeguards put in place to protect PHI in the EHR against theft, loss and unauthorized use or disclosure and to protect records of PHI in the EHR from unauthorized copying, modification or disposal;
- The duties and obligations of HICs and agents and Electronic Service Providers of HICs and eHealth Ontario in implementing the administrative, technical and physical safeguards;
- The End User Agreement that HICs and agents and Electronic Service Providers of HICs and eHealth Ontario must acknowledge and agree to comply with;
- The duties and obligations of HICs and agents and Electronic Service Providers of HICs and eHealth Ontario with respect to identifying, reporting, containing and participating in the investigation and remediation of Privacy Breaches and Security Breaches; and
- A statement informing agents and Electronic Service Providers of HICs and eHealth Ontario that they are subject to the professional obligations under their regulatory colleges, where applicable.

5 Enforcement

5.1.1 All instances of non-compliance will be reviewed by the applicable privacy and security committee. The applicable privacy and security committee will recommend appropriate action to the applicable oversight body.

5.1.2 The applicable oversight body has the authority to impose appropriate penalties, up to and including termination of the applicable agreements with the HIC or termination of the access privileges of agents and Electronic Service Providers, and to require the implementation of remedial actions.

6 Glossary and Terms

Electronic Health Record (EHR)
The ConnectingOntario Solution and the Diagnostic Imaging Common Services Repository which are clinical repository and/or ancillary systems designed to store and make available specified electronic PHI from the electronic health information systems of HICs to act as a single repository.

Electronic Service Provider
A person who provides goods or services for the purpose of enabling a HIC to use electronic means to collect, use, modify, disclose, retain or dispose of PHI, and includes a health information network provider.

End User Agreement

An agreement entered into between a HIC and the agents or Electronic Service Providers of a HIC and an agreement entered into between eHealth Ontario and the agents and Electronic Service Providers of eHealth Ontario in respect of the EHR.

Privacy Breach
Privacy Breach has the same meaning as in the *Electronic Health Record Privacy Breach Management Policy* and its associated procedures, as amended from time to time.

Security Breach
Security Breach has the same meaning as in the *Electronic Health Record Information Security Incident Management Policy* and its associated procedures, as amended from time to time.

Policy Governance Structure	ConnectingOntario Solution	Diagnostic Imaging Common Services Repository
Applicable Privacy and Security Committee	Privacy: Connecting Privacy Committee Security: Connecting Security Committee	Privacy: Diagnostic Imaging Common Services Privacy and Security Working Group Security: Connecting Security Committee
Applicable Oversight Body	Privacy: ConnectingOntarioCommittee Security: eHealth Ontario Strategy Committee	Privacy: Diagnostic Imaging Common Services Executive Committee Security: eHealth Ontario Strategy Committee

Table 1: Applicable Governance Bodies

Term or Acronym	Definition
HIC	Health Information Custodian
PHI	Personal Health Information, as defined in the *Personal Health Information Protection Act, 2004*
PHIPA	*Personal Health Information Protection Act, 2004*

7 References and Associated Documents

Personal Health Information Protection Act, 2004 (PHIPA)
Electronic Health Record Privacy Breach Management Policy and its associated procedures
Electronic Health Record Information Security Incident Management Policy and its associated procedures