eHealth Ontario

Logging and Auditing Policy

Electronic Health Record

Version: 1.1

Document ID: 3876

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	June 24, 2014

Revision History

VERSION NO.	DATE YYYY-MM-DD	SUMMARY OF CHANGE	CHANGED BY
1.1	2015-11-25	Minor revisions – updated for ConnectingOntario	Samara Strub, Privacy 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 Logging and Auditing Policy v1.1.	Promila Gonsalves, Privacy Analyst, eHealth Ontario

1 Contents

1 Purpose/ Objective

To define the policies, procedures and practices that apply in logging, auditing and monitoring all instances where:

- All or part of the personal health information (PHI) in the Electronic Health Record(EHR) is viewed, handled or otherwise dealt with[1];
- All or part of the PHI in the EHR is transferred to a health information custodian (HIC);
- All or part of the PHI in EHR is disclosed to and collected by a HIC as a result of an override of a Consent Directive; and
- A Consent Directive is made, modified or withdrawn in the EHR.

To facilitate the identification and investigation of actual or suspected Privacy Breaches or Security Breaches.

2 Scope

This policy and its associated procedures apply to logging, auditing and monitoring in the EHR for the purpose of facilitating the identification and investigation of actual or suspected Privacy Breaches or Security Breaches related to PHI in 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[2].

This policy and its associated procedures do not apply to logging, auditing and monitoring in any other system other than the EHR.

3 Policy

3.1 Guiding Policies

3.1.1 The *Personal Health Information Protection Act, 2004* (PHIPA) requires HICs to retain, transfer and dispose of PHI in a secure manner and to take steps that are reasonable in the circumstances to ensure that PHI in their custody or control is protected against theft, loss and unauthorized use or disclosure.

3.1.2 PHIPA requires eHealth Ontario to implement safeguards to protect the security and confidentiality of PHI in the EHR, including the protection of PHI against unauthorized use and disclosure.

3.1.3 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.

3.1.4 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 inform their agents and Electronic Service Providers on the policies, procedures and practices as required by PHIPA.

3.1.5 eHealth Ontario shall have a program in place and provide tools to enable HICs to satisfy their auditing and monitoring requirements in accordance with PHIPA, applicable agreements and this policy and its associated procedures.

---

[1] For greater clarity, viewing, handling or dealing with includes collection, use or disclosure where applicable.

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

3.1.6 eHealth Ontario shall have a program and tools in place to enable eHealth Ontario to satisfy its logging, auditing and monitoring requirements in accordance with PHIPA, applicable agreements and this policy and its associated procedures.

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

3.1.8 This policy and its associated procedures will support HICs and eHealth Ontario in meeting their legislative obligations through logging, auditing and monitoring in the EHR.

4 Procedure

4.1 Procedures Related to Logging by eHealth Ontario

4.1.1 eHealth Ontario shall ensure that the EHR logs all instances where:

- All or part of the PHI in the EHR is viewed, handled or otherwise dealt with;
- All or part of the PHI in the EHR is transferred to a HIC;
- All or part of the PHI in the EHR is disclosed to and collected by a HIC as a result of an override of a Consent Directive; and
- A Consent Directive is made, withdrawn or modified in the EHR.

4.1.2 eHealth Ontario shall ensure that the log of all instances where all or part of the PHI in the EHR is viewed, handled or otherwise dealt with identifies:

- The individual to whom the PHI relates;
- The type of PHI that is viewed, handled or otherwise dealt with;
- All persons who have viewed, handled or otherwise dealt with the PHI;
- Any person on whose behalf the PHI was viewed, handled or otherwise dealt with, if applicable; and
- The date, time and location of the viewing, handling or dealing with.

4.1.3 eHealth Ontario shall ensure that the log of all instances where all or part of the PHI in the EHR is transferred to a HIC identifies:

- The individual to whom the PHI relates;
- The type of PHI that was transferred;
- The HIC requesting the PHI to be transferred;
- The date and time the PHI was transferred; and
- The location to which the PHI was transferred.

4.1.4 eHealth Ontario shall ensure that the log of all instances where all or part of the PHI in the EHR is disclosed to and collected by a HIC as a result of an override of a Consent Directive identifies:

- The HIC that disclosed the PHI;
- The HIC that collected the PHI;
- Any agent that collected the PHI on behalf of the HIC;
- The individual to whom the PHI relates;
- The type of PHI that was disclosed;
- The date and time the PHI was disclosed; and
- The purpose of the disclosure.

4.1.5 eHealth Ontario shall ensure that the log of all instances where a Consent Directive is made, withdrawn or modified in the EHR identifies:

- The individual or the substitute decision-maker (SDM) for the individual who made, withdrew or modified the Consent Directive;
- The Consent Directive implemented in response to the instructions that the individual or the SDM for the individual provided regarding the Consent Directive;
- The HIC, agent or other person to whom the directive is made, withdrawn or modified; and
- The date and time the Consent Directive was made, withdrawn or modified.

4.1.6 eHealth Ontario shall provide the Information and Privacy Commissioner of Ontario with the logs set out in paragraph 4.1.1 and containing the content set out in paragraphs 4.1.2 to 4.1.5 upon request of the Information and Privacy Commissioner of Ontario for the purposes of Part VI of PHIPA.

4.1.7 Prior to providing the logs described in paragraph 4.1.6 to the Information and Privacy Commissioner of Ontario, eHealth Ontario shall notify the HIC(s) that are named in the logs, or whose agent or Electronic Service Provider is named in the logs, that eHealth Ontario has provided the logs to the Information and Privacy Commissioner of Ontario.

4.1.8 eHealth Ontario shall, upon the request of a HIC who requires the logs to audit and monitor compliance with PHIPA, applicable agreements and this policy and its associated procedures, provide the HIC with the logs set out in paragraph 4.1.1 and containing the content set out in in paragraphs 4.1.2. to 4.1.5.

4.1.9 eHealth Ontario shall ensure that logs are securely retained, transferred and disposed of in a manner than enables compliance with PHIPA, the *Electronic Health Record Retention Policy* (to be drafted) and the *Electronic Health Record Information Security Policy* and its associated procedures, as amended from time to time.

4.2 Procedures Related to Auditing and Monitoring by eHealth Ontario

4.2.1 eHealth Ontario shall conduct the auditing and monitoring described in paragraphs 4.2.2 to 4.2.5 to ensure compliance with PHIPA, applicable agreements and the policies, procedures and practices implemented in respect of the EHR in accordance with the auditing and monitoring criteria established by the applicable privacy and security committee.

4.2.2 eHealth Ontario shall audit and monitor instances where all or part of the PHI in the EHR is viewed, handled or otherwise dealt with by agents or Electronic Service Providers of eHealth Ontario.

4.2.3 eHealth Ontario shall audit and monitor other instances where all or part of the PHI in the EHR is viewed, handled or otherwise dealt with.

4.2.4 eHealth Ontario shall audit and monitor instances where all or part of the PHI in the EHR is transferred to a HIC.

4.2.5 eHealth Ontario shall audit, monitor and alert the HIC that collected the PHI in the EHR in all instances where all or part of the PHI in the EHR is disclosed to and collected by the HIC as a result of an override of a Consent Directive, in accordance with the *Electronic Health Record Consent Management Policy* and its associated procedures, as amended from time to time.

4.2.6 eHealth Ontario shall submit to the Information and Privacy Commissioner of Ontario, at least annually, a written report respecting every instance where all or part of the PHI in the EHR is disclosed to and collected by a HIC as a result of an override of a Consent Directive.

4.2.7 eHealth Ontario shall audit and monitor all instances where a Consent Directive is made, withdrawn or modified in the EHR.

4.2.8 Where eHealth Ontario identifies any actual or suspected Privacy Breaches, eHealth Ontario shall follow the *Electronic Health Record Privacy Breach Management Policy* and its associated procedures, as amended from time to time. Where eHealth Ontario identifies any actual or suspected Security Breaches, eHealth Ontario shall follow *Electronic Health Record Information Security Incident Management Policy* and its associated procedures, as amended from time to time.

4.3 Procedures Related to Auditing and Monitoring Tools by eHealth Ontario

4.3.1 eHealth Ontario will make available to HICs, auditing and monitoring tools and reports to enable HICs to satisfy their auditing and monitoring responsibilities under PHIPA, applicable agreements and this policy and its associated procedures.

4.3.2 The auditing and monitoring tools and reports that will be made available by eHealth Ontario will be in a secure, immutable and widely used format.

4.3.3 eHealth Ontario will automate auditing and monitoring in the EHR as technology becomes available to better support proactive auditing and monitoring in the EHR.

4.4 Procedures Related to Auditing and Monitoring by HICs

4.4.1 HICs shall conduct the auditing and monitoring activities described in paragraphs 4.4.2 to 4.4.4 to ensure compliance with PHIPA, applicable agreements and the policies, procedures and practices implemented in respect of the EHR in accordance with the auditing and monitoring criteria established by the applicable privacy and security committee.

4.4.2 All HICs shall audit and monitor instances where all or part of the PHI in the EHR is viewed, handled or otherwise dealt with by the HIC and agents or Electronic Service Providers of the HIC, other than eHealth Ontario and agents or Electronic Service Providers of eHealth Ontario.

4.4.3 All HICs shall audit and monitor all instances where the HIC and agents or Electronic Service Providers of the HIC, other than eHealth Ontario and agents or Electronic Service Providers of eHealth Ontario, implemented the instructions of an individual or his or her SDM to make, withdraw or modify a Consent Directive in the EHR.

4.4.4 HICs that created and contributed the PHI to the EHR shall, in addition to the auditing and monitoring in paragraphs 4.4.2 and 4.4.3, audit and monitor:

- All other instances where all or part of the PHI that the HIC created and contributed to the EHR is viewed, handled or otherwise dealt with; and
- All instances where a Consent Directive is made, withdrawn or modified in relation to PHI created and contributed to the EHR by the HIC.

4.4.5 Where a HIC identifies any actual or suspected Privacy Breaches, the HIC shall follow the *Electronic Health Record Privacy Breach Management Policy* and its associated procedures, as amended from time to time. Where a HIC identifies any actual or suspected Security Breaches, the HIC shall follow the *Electronic Health Record Information Security Breach Management Policy* and its associated procedures, as amended from time to time.

4.4.6 Upon receiving notice from eHealth Ontario that the HIC has collected all or part of the PHI in the EHR as a result of an override of a Consent Directive, the HIC shall comply with the HIC's obligations under PHIPA and the *Electronic Health Record Consent Management Policy* and its associated procedures, as amended from time to time.

4.5 Procedures For Establishing Auditing and Monitoring Criteria

4.5.1 The applicable privacy and security committee shall, prior to any PHI in the EHR being viewed, handled or otherwise dealt with, establish auditing and monitoring criteria that will be used by eHealth Ontario and HICs, as the case may be. The applicable oversight body shall be consulted by the applicable privacy and security committee on the auditing and monitoring criteria.

4.5.2 The criteria established under paragraph 4.5.1, shall enable HICs and eHealth Ontario to comply with their obligations under PHIPA, applicable agreements and the policies, procedures and practices implemented in respect of the EHR and shall be consistent with industry standards and best practices and shall be based on an assessment of the threats and risks posed to PHI in the EHR.

5 Enforcement[3]

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 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 to act as a single repository.

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

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.

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: ConnectingOntario Committee Security: eHealth Ontario Strategy Committee	Privacy: Diagnostic Imaging Common Services Executive Committee Security: eHealth Ontario Strategy

[3] References to the applicable privacy and security committee and the applicable oversight body can be found in *Table 1: Applicable Governance Bodies*.

		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*
SDM	Substitute Decision-Maker, as defined in the *Personal Health Information Protection Act, 2004*

7 References and Associated Documents

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