eHealth Ontario

# Assurance Policy

## Electronic Health Record

Version: 2.0

Document ID: 3874

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 | December 8, 2016 |

## Revision History

| VERSION NO. | DATE YYYY-MM-DD | SUMMARY OF CHANGE | CHANGED BY |
|---|---|---|---|
| 2.0 | 2016-12-01 | Revisions as per CPC Policy Evaluation | Rand Muhtam, Privacy Analyst, eHealth Ontario |
| 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 Assurance Policy v1.2. | Promila Gonsalves, Privacy Analyst, eHealth Ontario |

# Contents

# 1 Purpose/ Objective

This document defines the policies, procedures and practices that health information custodians (HICs) and eHealth Ontario shall have in place to provide assurance that HICs and eHealth Ontario comply with their obligations under the *Personal Health Information Protection Act, 2004* (PHIPA), applicable agreements, and the policies, procedures and practices implemented in respect of the Electronic Health Record (EHR).

# 2 Scope

This policy and its associated procedures apply to the conduct of eHealth Ontario, HICs who create and contribute or who collect, use or disclose personal health information (PHI) in the EHR, and agents and Electronic Service Providers of the HICs or eHealth Ontario. 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].

# 3 Policy

## 3.1 Guiding Policies

3.1.1 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.

3.1.2 HICs and eHealth Ontario shall ensure alignment between the applicable agreements and the policies, procedures and practices implemented in respect of the EHR.

3.1.3 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.

3.1.4 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 the policies, procedures and practices implemented in respect of the EHR.

3.1.5 HICs shall identify and mitigate privacy and security risks and areas of non-compliance[2] in respect of the EHR, including through privacy and security readiness self-assessments (as applicable), privacy and security operational self-attestations, auditing and monitoring activities and assurance of agents and Electronic Service Providers.

3.1.6 eHealth Ontario shall identify and mitigate privacy and security risks and areas of non-compliance in respect of the EHR, including through privacy impact assessments , privacy and security readiness self-assessments (as applicable), privacy and security operational self-attestations, auditing and monitoring activities and assurance of agents, Electronic Service Providers and third parties.

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

[2] For purposes of this policy and its associated procedures "areas of non-compliance" include non-compliance with PHIPA, applicable agreements and the policies, procedures and practices implemented in respect of the EHR.

3.1.7 HICs and eHealth Ontario shall report any privacy or security risks and areas of non-compliance that could be expected to impact the privacy of individuals or the security of their PHI in the EHR to the applicable privacy and security committee.

3.1.8 HICs and eHealth Ontario shall comply with the decisions and directions of the applicable oversight body and shall cooperate in any audits conducted by the applicable privacy and security committee pursuant to this policy and its associated procedures.

# 4 Procedure

## 4.1 Procedures for Privacy Impact Assessments

4.1.1 eHealth Ontario shall monitor and identify and provide a written report to the applicable privacy and security committee as soon as possible, after the identification of one or more of the following circumstances in respect of the EHR:

- New PHI feed/source;
- New types or roles of HICs or agents of HICs who are collecting, using or disclosing PHI;
- New types or roles of eHealth Ontario or Electronic Service Providers who are viewing, handling or dealing with PHI;
- New collections, uses or disclosures of PHI by HICs and their agents;
- New viewing, handling or dealing with PHI by eHealth Ontario or Electronic Service Providers;
- Changes to existing front-end or back-end architecture or functionality that could be expected to impact the privacy of individuals or the security of their PHI;
- Changes to operational support model or operational systems, processes or parties that could be expected to impact the privacy of individuals or the security of their PHI;
- Changes to applicable agreements that could be expected to impact the privacy of individuals or the security of their PHI;
- Legislative changes to PHIPA that could be expected to impact the privacy of individuals or the security of their PHI; or
- A vulnerability that has or may result in a privacy breach within the meaning of the *Electronic Health Record Privacy Breach Management Policy* and its associated procedures, as amended from time to time.

4.1.2 The written report under paragraph 4.1.1 shall:

- Describe the circumstance(s) and the impact of the circumstance(s) on the privacy of individuals or the security of their PHI; and
- Make a recommendation as to whether eHealth Ontario should conduct or revise a privacy impact assessment (PIA).

4.1.3 The applicable privacy and security committee shall, at its next meeting following receipt of the report under paragraph 4.1.2, review and provide the report, along with its written recommendation on whether eHealth Ontario should conduct or revise a PIA to the applicable oversight body for consideration at its next meeting.

4.1.4 The applicable oversight body shall, at its next meeting following receipt of the report and recommendation under paragraph 4.1.3:

- Review the report and recommendation received;
- Make a written decision as to whether eHealth Ontario must conduct or revise a PIA;
- Where it is decided that a PIA must be conducted or revised, provide written directions to eHealth Ontario, including in respect of the timeframe within which the PIA must be conducted or revised; and
- Provide a copy of its decision and directions to eHealth Ontario and the applicable privacy and security committee.

4.1.5 eHealth Ontario shall comply with the decision and directions of the applicable oversight body and provide written updates on the status of the PIA at each meeting of the applicable privacy and security committee.

4.1.6 The applicable privacy and security committee shall monitor compliance of eHealth Ontario with the decision and directions of the applicable oversight body and may require further documented evidence to demonstrate compliance. eHealth Ontario shall comply with any request from the applicable privacy and security committee for documented evidence to demonstrate compliance.

4.1.7 eHealth Ontario shall perform Threat Risk Assessments (TRAs) in the circumstances and in accordance with the *Electronic Health Record Threat Risk Management Policy* and its associated procedures, as amended from time to time.

4.1.8 The applicable privacy and security committee shall establish criteria that must be used by eHealth Ontario in determining whether each privacy and security risk and area of non-compliance identified in a PIA is a "high," "medium" or "low" risk. The applicable oversight body shall be consulted by the applicable privacy and security committee in the establishment of the criteria.

4.1.9 eHealth Ontario shall:

- Assign a risk rating to each privacy and security risk and area of non-compliance identified in a PIA in accordance with paragraph 4.1.8;
- Develop a remediation plan;[3]
- Ensure the remediation plan includes measures to mitigate privacy and security risks and areas of non-compliance assigned a "high" risk rating; and
- Ensure the remediation plan includes measures to mitigate privacy and security risks and areas of non-compliance assigned a "medium" or "low" risk rating or provides a rationale for not mitigating one or more of these privacy and security risks and areas of non-compliance.

4.1.10 eHealth Ontario shall complete PIAs during the conceptual design phase and must review and update the PIAs, if necessary, during the detailed design and implementation phase.

4.1.11 eHealth Ontario shall, as soon as possible, but in any event no later than 30 days after completing or updating a PIA, provide the applicable privacy and security committee with:

- A copy of the PIA;
- The risk rating assigned to each privacy and security risk and area of non-compliance identified;
- The remediation plan; and
- A rationale for not mitigating one or more privacy and security risks and areas of non-compliance assigned a "medium" or "low" risk rating.

4.1.12 The applicable privacy and security committee shall, as soon as possible, but in any event no later than at its next meeting following receipt of the information under paragraph 4.1.11:

- Review the information received;
- Ensure all privacy and security risks and areas of non-compliance have been identified;
- Ensure the risk rating assigned to each privacy and security risk and area of non-compliance identified accords with paragraph 4.1.8;
- Ensure the remediation plan adequately mitigates privacy and security risks and areas of non-compliance assigned a "high" risk rating;
- Ensure the remediation plan adequately mitigates privacy and security risks and areas of non-compliance assigned a "medium" or "low" risk rating or provides a rationale for not mitigating one or more of these privacy and security risks and areas of non-compliance; and

---

[3] For purposes of this policy and its associated procedures, a remediation plan shall, at a minimum, include the measures to mitigate the privacy and security risks and areas of non-compliance identified and the timelines and persons responsible for implementing the measures.

- Make a written recommendation to approve the PIA and remediation plan or provide written directions to eHealth Ontario to amend and re-submit the PIA and remediation plan and to provide the timeframe within which they must be amended and re-submitted;
- Provide a copy of its directions to eHealth Ontario; and
- Provide the information received under paragraph 4.1.11, along with its written recommendations, to the applicable oversight body.

4.1.13 The applicable oversight body eHealth Ontario shall amend and re-submit the PIA and remediation plan to the applicable privacy and security committee for recommendation for approval in accordance with the timeframe set out in the written directions under paragraph 4.1.13 when directed to do so.

4.1.14 The applicable oversight body shall, as soon as possible, but in any event no later than at its next meeting following receipt of the information and recommendations under paragraph 4.1.12:

- Review the information and the recommendations received;
- Ensure all privacy and security risks and areas of non-compliance have been identified;
- Ensure the risk rating assigned to each privacy and security risk and area of non-compliance identified accords with paragraph 4.1.8;
- Ensure the remediation plan adequately mitigates privacy and security risks and areas of non-compliance assigned a "high" risk rating;
- Ensure the remediation plan adequately mitigates privacy and security risks and areas of non-compliance assigned a "medium" or "low" risk rating or provides a rationale for not mitigating one or more of these privacy and security risks and areas of non-compliance;
- Make a written decision to accept any privacy and security risks and areas of non-compliance assigned a "medium" or "low" risk rating that are proposed not to be mitigated or provide written directions to eHealth Ontario to amend the remediation plan to address these privacy and security risks and areas of non-compliance; and
- Make a written decision to approve the PIA and remediation plan or provide written directions to eHealth Ontario to amend and re-submit the PIA and remediation plan and to provide the timeframe within which they must be amended and re-submitted; and
- Provide a copy of its decision and directions to eHealth Ontario and the applicable privacy and security committee.

4.1.15 eHealth Ontario shall amend and re-submit the PIA and remediation plan to the applicable oversight body for approval in accordance with the timeframe set out in the written directions under paragraph 4.1.13 when directed to do so.

4.1.16 eHealth Ontario shall, upon the approval of the PIA and remediation plan by the applicable oversight body:

- Provide a copy of the PIA, as well as a copy of the remediation plan, to each HIC who creates and contributes or who collects, uses or discloses PHI in the EHR;
- Implement the remediation plan;
- Provide written updates on the status of implementation of the remediation plan at each meeting of the applicable privacy and security committee; and
- Provide a written attestation to the applicable privacy and security committee that the remediation plan has been fully implemented, as soon as possible, but in any event no later than 30 days after implementation.

4.1.17 The applicable privacy and security committee shall monitor compliance of eHealth Ontario with the implementation of the approved remediation plan approved by the applicable oversight body and may require further documented evidence to demonstrate compliance. eHealth Ontario shall comply with any request from the applicable privacy and security committee for documented evidence to demonstrate compliance.

**ConnectingOntario Solution only**

## 4.2 Procedures for Privacy and Security Readiness Self-Assessment

4.2.1 The applicable privacy and security committee shall establish:

- The requirements in the privacy and security readiness self-assessment that must be used to evaluate the privacy and security readiness and to identify the privacy and security risks and areas of non-compliance posed by eHealth Ontario and HICs who create and contribute or who collect, use or disclose PHI in the EHR; and
- Whether a failure to satisfy each requirement is a "high," "medium" or "low" risk.

4.2.2 The applicable privacy and security committee shall create, maintain and administer the privacy and security readiness self-assessment in respect of eHealth Ontario.

4.2.3 eHealth Ontario shall create, maintain and administer the privacy and security readiness self-assessments in respect of each HIC who creates and contributes or who collects, uses or discloses PHI in the EHR.

4.2.4 As soon as possible, but in any event prior to eHealth Ontario viewing, handling or dealing with PHI or prior to a HIC contributing or collecting, using or disclosing PHI in the EHR, eHealth Ontario or the HIC, as the case may be, shall:

- Complete the privacy and security readiness self-assessment;
- Assign a risk rating to each privacy risk and area of non-compliance identified in the privacy and security readiness self-assessment in accordance with paragraph 4.2.1;
- Develop a remediation plan;
- Ensure the remediation plan includes measures to mitigate privacy risks and areas of non-compliance assigned a "high" risk rating;
- Ensure the remediation plan includes measures to mitigate privacy risks and areas of non-compliance assigned a "medium" or "low" risk rating or provides a rationale for not mitigating one or more of these privacy risks and areas of non-compliance; and
- Ensure an Officer signs-off on the privacy and security readiness self-assessment and remediation plan.

4.2.5 As soon as possible, but in any event prior to eHealth Ontario viewing, handling or dealing with PHI or prior to a HIC contributing or collecting, using or disclosing PHI in the EHR, eHealth Ontario or the HIC, as the case may be, shall provide the applicable privacy and security committee with a copy of the completed privacy and security readiness self-assessment.

## 4.3 Procedures for Privacy and Security Operational Self-Attestation

4.3.1 The applicable privacy and security committee, in consultation with the applicable oversight body, shall establish:

- The requirements in the privacy and security operational self-attestation that must be used to evaluate the ongoing operational privacy and security posture and to identify the privacy and security risks and areas of non-compliance posed by eHealth Ontario and HICs who create and contribute or who collect, use or disclose PHI in the EHR;
- Whether a failure to satisfy each requirement is a "high," "medium" or "low" risk; and
- The timeframe each year in which the privacy and security operational self-attestation must be administered and completed.

4.3.2 The applicable privacy and security committee shall create, maintain and administer the privacy and security operational self-attestations in respect of eHealth Ontario.

4.3.3 eHealth Ontario shall create, maintain and administer privacy and security operational self-attestations in respect of each HIC who creates and contributes or who collects, uses or discloses PHI in the EHR.

4.3.4 Within the timeframe each year stipulated by the applicable privacy and security committee under paragraph 4.3.1, eHealth Ontario and HICs creating and contributing or collecting, using or disclosing PHI in the EHR shall:

- Complete the privacy and security operational self-attestation;

- Assign a risk rating to each privacy and security risk and area of non-compliance identified in the privacy and security operational self-attestation in accordance with paragraph 4.3.1;
- Develop a remediation plan;
- Ensure the remediation plan includes measures to mitigate privacy and security risks and areas of non-compliance assigned a "high" risk rating;
- Ensure the remediation plan includes measures to mitigate privacy and security risks and areas of non-compliance assigned a "medium" or "low" risk rating or provides a rationale for not mitigating one or more of these privacy and security risks and areas of non-compliance; and
- Ensure an Officer signs-off on the privacy and security operational self-attestation and remediation plan.

4.3.5 As soon as possible, but in any event no later than 30 days after the timeframe stipulated under paragraph 4.3.1, eHealth Ontario and HICs creating and contributing or collecting, using or disclosing PHI in the EHR shall provide the applicable privacy and security committee with:

- A copy of the completed privacy and security operational self-attestation;
- The risk rating assigned to each privacy and security risk and area of non-compliance identified; and
- The remediation plan.

4.3.6 The applicable privacy and security committee shall, as soon as possible, but in any event no later than at its next scheduled committee meeting after receipt of the information under paragraph 4.3.5:

- Review the information received;
- Solicit comments from eHealth Ontario in respect of information provided by a HIC under paragraph 4.3.5;
- Ensure all privacy and security risks and areas of non-compliance have been identified;
- Ensure the risk rating assigned to each privacy and security risk and area of non-compliance identified accords with paragraph 4.3.1;
- Ensure the remediation plan satisfies the requirements under paragraph 4.3.4;
- Make a written decision to approve the privacy and security operational self-attestation and remediation plan or provide written directions to eHealth Ontario or the HIC, as the case may be, to amend and re-submit the privacy and security operational self-attestation and remediation plan and to provide the timeframe within which they must be amended and re-submitted;
- Provide a copy of its decision and directions to eHealth Ontario or the HIC, as the case may be; and
- Provide the information received under paragraph 4.3.5, the comments received from eHealth Ontario, where applicable, and its written recommendations to the applicable oversight body.

4.3.7 eHealth Ontario or the HIC, as the case may be, shall amend and re-submit the privacy and security operational self-attestation and remediation plan to the [PRIVACY AND SECURITY COMMITTEE] for approval in accordance with the timeframe set out in the written directions under paragraph 4.3.7 when directed to do so.

4.3.8 The [APPROPRIATE PROGRAM OFFICE STEERING COMMITTEE] shall, as soon as possible, but in any event no later than at its next meeting after receipt of the information and recommendations under paragraph 4.3.6:

- Review the information and the recommendations received;
- Ensure all privacy and security risks and areas of non-compliance have been identified;
- Ensure the risk rating assigned to each privacy and security risk and area of non-compliance identified accords with paragraph 4.3.1;
- Ensure the remediation plan satisfies the requirements under paragraph 4.3.4;
- Make a written decision to accept any privacy and security risks and areas of non-compliance assigned a "medium" or "low" risk rating that are proposed not to be mitigated or provide written directions to eHealth Ontario or the HIC, as the case may be, to amend the remediation plan to address these privacy and security risks and areas of non-compliance; and

- Provide a copy of its decision and directions to eHealth Ontario or the HIC, as the case may be and the applicable privacy and security committee.
- Provide a copy of its decision and directions to eHealth Ontario or the HIC, as the case may be, and to the applicable privacy and security committee.

4.3.9 eHealth Ontario or the HIC, as the case may be, shall, upon the approval of the privacy and security operational self-attestation and remediation plan by the applicable oversight body:

- Implement the remediation plan;
- Provide written updates on the status of implementation of the remediation plan at each meeting of the applicable privacy and security committee; and
- Provide a written attestation to the applicable privacy and security committee that the remediation plan has been fully implemented as soon as possible, but in any event no later than 30 days after implementation.

4.3.10 The applicable privacy and security committee shall monitor compliance of eHealth Ontario or the HIC, as the case may be, with the implementation of the approved remediation plan and may require further documented evidence to demonstrate compliance. eHealth Ontario or the HIC, as the case may be, shall comply with any request from the applicable privacy and security committee for documented evidence to demonstrate compliance.

## 4.4 Assurance of Agents, Electronic Service Providers and Third Parties

4.4.1 eHealth Ontario shall ensure, including having in place a policy, that any agents, Electronic Service Providers and third parties it retains to assist in providing services in respect of the EHR comply with the restrictions and conditions that are necessary to enable eHealth Ontario to comply with PHIPA, applicable agreements and the policies, procedures and practices implemented in respect of the EHR.

4.4.2 HICs shall take steps that are reasonable in the circumstances to ensure that their agents and Electronic Service Providers comply with PHIPA, applicable agreements and the policies, procedures and practices implemented in respect of the EHR.

## 4.5 Auditing and Monitoring

4.5.1 eHealth Ontario and HICs creating and contributing or collecting, using or disclosing PHI in the EHR shall conduct auditing and monitoring of activities in respect of the EHR in accordance with PHIPA, applicable agreements and the policies, procedures and practices implemented in respect of the EHR, including the *Electronic Health Record Logging and Auditing Policy*, *Electronic Health Record Privacy Breach Management Policy* and the *Electronic Health Record Information Security Logging and Monitoring Policy* and their associated procedures, as amended from time to time.

4.5.2 eHealth Ontario and HICs creating and contributing or collecting, using or disclosing PHI in the EHR shall, at the first reasonable opportunity, report to the applicable privacy and security committee any privacy or security risks or areas of non-compliance that could be expected to impact the privacy of individuals or the security of their PHI in the EHR that are not identified in PIAs, privacy and security readiness self-assessments and privacy and security operational self-attestations.

4.5.3 Applicable privacy and security committee shall determine whether any privacy or security risks or areas of non-compliance that could be expected to impact the privacy of individuals or the security of their PHI in the EHR identified in PIAs, privacy and security readiness self-assessments and privacy and security operational self-attestations may require an audit by the applicable privacy and security committee.

4.5.4 The applicable privacy and security committee shall, as soon as possible, but in any event no later than at its next meeting following receipt of the report under paragraph 4.5.2 or having identified privacy or security risks or areas of non-compliance under paragraph 4.5.3:

- Solicit comments from eHealth Ontario or the HIC suspected of posing the privacy or security risks or suspected of non-compliance, as the case may be;
- Assess whether there are privacy or security risks or areas of non-compliance that could be expected to impact the privacy of individuals or the security of their PHI in the EHR;
- Assess whether eHealth Ontario or the HIC suspected of posing the privacy or security risks or suspected of non-compliance, as the case may be, has or will be implementing measures to mitigate the privacy or security risks or areas of non-compliance;
- Assess whether an audit should be conducted;

- Provide the applicable oversight body with the report received under paragraph 4.5.2, if applicable, and the comments received from eHealth Ontario or the HIC suspected of posing the privacy or security risks or suspected of non-compliance, as the case may be; and
- Provide the applicable oversight body with its written recommendations.

4.5.5 In providing recommendations to the applicable oversight body under paragraph 4.5.4, the applicable privacy and security committee shall:

- Where it is recommended that an audit be conducted, include recommendations in respect of the nature and scope of the audit, the process to be followed in conducting the audit and the timeframe within which the audit must be conducted; or
- Where it is recommended that an audit not be conducted, include recommendations, if any, in respect of proposed measures to mitigate the privacy or security risks or areas of non-compliance.

4.5.6 The applicable oversight body shall, as soon as possible, but in any event no later than at its next meeting following receipt of the information and recommendations under paragraph 4.5.4:

- Review the information and recommendations received;
- Make a written decision as to whether the applicable privacy and security committee must conduct an audit of eHealth Ontario or the HIC suspected of posing the privacy or security risks or suspected of non-compliance, as the case may be;
- Where the applicable oversight body has decided that an audit must be conducted, provide written directions to the applicable privacy and security committee, including in respect of the nature and scope of the audit, the process to be followed in conducting the audit and the timeframe within which the audit must be conducted;
- Where the applicable oversight body has decided that an audit should not be conducted, provide written directions, if any, to the applicable privacy and security committee in respect of proposed measures to mitigate the privacy or security risks or areas of non-compliance; and
- Provide a copy of its decision and directions to the applicable privacy and security committee and to eHealth Ontario or the HIC suspected of posing the privacy or security risks or suspected of non-compliance, as the case may be.

4.5.7 The applicable privacy and security committee shall conduct an audit in accordance with the decision and directions of the applicable oversight body.

4.5.8 eHealth Ontario or the HIC suspected of posing the privacy or security risks or suspected of non-compliance, as the case may be, shall comply with the decision and directions of the applicable oversight body and shall remediate the privacy or security risks or areas of non-compliance or shall cooperate in any audit by the applicable privacy and security committee, as the case may be.

4.5.9 The applicable privacy and security committee shall, as soon as possible, but in any event no later than at its next meeting after completing the audit, report to the applicable oversight body:

- The findings of the audit; and
- Its recommendations for remediating the privacy or security risks or areas of non-compliance identified, along with the timeframe for implementing the recommendations.

4.5.10 The applicable oversight body shall, as soon as possible, but in any event no later than at its next meeting after receipt of the information and recommendations under paragraph 4.5.9:

- Review the information and the recommendations received;
- Ensure all privacy and security risks and areas of non-compliance have been identified;
- Ensure the recommendations adequately mitigate the privacy and security risks and areas of non-compliance identified;
- Make a written decision to approve the recommendations and provide directions in respect of the timeframe for implementing the decision or provide written directions to the applicable privacy and security committee to amend and re-submit the recommendations and to provide the timeframe within which they must be amended and re-submitted; and
- Provide a copy of its decision and directions to the applicable privacy and security committee.

4.5.11 The applicable privacy and security committee shall amend and re-submit the recommendations to the applicable oversight body for approval in accordance with the timeframe set out in the written directions under paragraph 4.5.10 when directed to do so.

4.5.12 The applicable privacy and security committee shall, upon the approval of the recommendations by the applicable oversight body, provide a copy of the findings of the audit and the decision and directions of the applicable oversight body to eHealth Ontario or the HIC that posed the privacy or security risks or who is in non-compliance.

4.5.13 eHealth Ontario or the HIC that posed the privacy or security risks or who is in non-compliance, as the case may be, shall, upon receipt of the information under paragraph 4.5.12:

- Implement the decision and directions within the timeframe approved by the applicable oversight body;
- Provide written updates on the status of implementation of the decision and directions at each meeting of the applicable privacy and security committee; and
- Provide a written attestation to the applicable privacy and security committee that the decision and directions have been fully implemented, as soon as possible, but in any event no later than 30 days after implementation.

4.5.14 The applicable privacy and security committee shall monitor compliance of eHealth Ontario or the HIC, as the case may be, with the implementation of the decision and directions of the applicable oversight body and may require further documented evidence to demonstrate compliance. eHealth Ontario or the HIC, as the case may be, shall comply with any request from the applicable privacy and security committee for documented evidence to demonstrate compliance.

## 4.6 Non-Compliance

4.6.1 Non-compliance with PHIPA, applicable agreements, and the policies, procedures and practices implemented in respect of the EHR will be identified, including through the following activities documented in this policy:

- PIAs;
- Privacy and security readiness self-assessments;
- Privacy and security operational self-attestations;
- Assurance of agents, Electronic Service Providers and third parties;
- Auditing and monitoring activities under paragraph 4.5.1; and
- Audits conducted by the applicable privacy and security committee.

# 5 Enforcement

5.1.1 All instances of non-compliance will be reviewed by the applicable privacy and security committee which may 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 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

**Applicable Agreements**
The agreements entered into by HICs, eHealth Ontario, agents and Electronic Service Providers of a HIC, or agents and Electronic Service Providers of eHealth Ontario in respect of the EHR.

**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.

**Applicable Oversight Body**
The committee mandated to approve strategies, escalate and/or resolve privacy and security risks and areas of non-compliance, make decisions on key strategic objectives and deliverables and consider and, as applicable, approve the recommendations of the Applicable privacy and security committee for the EHR.

**Applicable Privacy and Security Committee**
A committee to support the privacy and information security governance structure of the EHR and that is comprised of HICs or agents of HICs creating and contributing or collecting, using or disclosing PHI in the EHR.

**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.

**Officer**
An Officer includes the chairperson of the board of directors, the president, a vice-president, the secretary, the treasurer, the comptroller, the general counsel, the general manager, a managing director, of a corporation, or any other individual who performs functions for a corporation similar to those normally performed by an individual occupying any of those offices.

| Policy Governance Structure | ConnectingOntario Solution | Diagnostic Imaging Common Services Repository |
|---|---|---|
| **Applicable Privacy and Security Committee** | Privacy: Connecting Privacy Committee<br><br>Security: Connecting Security Committee | Privacy: Diagnostic Imaging Common Services Privacy and Security Working Group<br><br>Security: Connecting Security Committee |
| **Applicable Oversight Body** | Privacy: ConnectingOntario Committee<br><br>Security: eHealth Ontario Strategy Committee | Privacy: Diagnostic Imaging Common Services Executive Committee<br><br>Security: eHealth Ontario Strategy Committee |

**Table 1: Applicable Governance Bodies**

| Acronym | Term |
|---|---|
| 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* |
| PIA | Privacy Impact Assessment |
| TRA | Threat and Risk Assessment |

# 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 Logging and Auditing Policy* and its associated procedures
- *Electronic Health Record Security Logging and Monitoring Policy* and its associated procedures
- *Electronic Health Record Threat Risk Management Policy* and its associated procedures