# Table of Contents

1. Access and Correction Policy v2.0  
2. Assurance Policy v2.0  
3. Consent Management Policy v1.3  
4. Inquiries and Complaints Policy v1.1  
5. Logging and Auditing Policy v1.1  
6. Privacy and Security Training Policy v1.2  
7. Privacy Breach Management Policy v2.0  
8. Retention Policy v2.0
Document Control

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

Approval History

<table>
<thead>
<tr>
<th>APPROVER(S)</th>
<th>APPROVED DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>ConnectingPrivacy Committee Members</td>
<td>March 17, 2016</td>
</tr>
</tbody>
</table>

Revision History

<table>
<thead>
<tr>
<th>VERSION NO.</th>
<th>DATE YYYY-MM-DD</th>
<th>SUMMARY OF CHANGE</th>
<th>CHANGED BY</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.0</td>
<td>2016-12-01</td>
<td>Revisions as per CPC Policy Evaluation</td>
<td>Rand Muhtam, Privacy Analyst, eHealth Ontario</td>
</tr>
<tr>
<td>0.01</td>
<td>2014-11-04</td>
<td>Initial draft based on ConnectingPrivacy Committee Harmonized Access and Correction Policy v1.3.</td>
<td>Promila Gonsalves, Privacy Analyst, eHealth Ontario</td>
</tr>
<tr>
<td>1.0</td>
<td>2014-11-17</td>
<td>Final version</td>
<td>Urooj Kirmani, Senior Privacy Analyst, eHealth Ontario</td>
</tr>
<tr>
<td>1.1</td>
<td>2015-11-25</td>
<td>Minor revisions – updated for ConnectingOntario</td>
<td>Samara Strub, Privacy Analyst, eHealth Ontario</td>
</tr>
</tbody>
</table>
## Contents

1. **Purpose/Objective** ................................................................. 1
2. **Scope** .................................................................................. 1
3. **Policy** .................................................................................. 1
   3.1 Guiding Policies..................................................................... 1
4. **Procedure** .......................................................................... 2
   4.1 Procedures for Responding to a Request for Access.................... 2
   4.2 Procedures for Charging Fees for Access.......................... 5
   4.3 Procedures for Responding to a Request for Correction........... 5
   4.4 Complaints Related to Requests for Access, Requests for Correction and Fees ......................................................... 7
5. **Enforcement** ....................................................................... 7
6. **Glossary and Terms** ............................................................ 7
7. **References and Associated Documents** ................................. 8
1 Purpose/ Objective

This document defines the policies, procedures and practices that apply in receiving and responding to Requests for Access and Requests for Correction in respect of records of personal health information (PHI) in the Electronic Health Record (EHR) made by the individual¹ to whom the PHI relates.

2 Scope

This policy and its associated procedures apply to Requests for Access and Requests for Correction in respect of records of PHI in the EHR.

This policy and its associated procedures do not apply to Requests for Access and Requests for Correction in respect of records of PHI that have not been contributed to 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 HICs².

3 Policy

3.1 Guiding Policies

3.1.1 The Personal Health Information Protection Act, 2004 (PHIPA) permits an individual to make a Request for Access and a Request for Correction to the individual’s own records of PHI in the custody or control of a health information custodian (HIC), and requires HICs to grant the request subject to limited and specific exceptions.

3.1.2 Under PHIPA, HICs must respond to a Request for Access and to a Request for Correction within 30 days of receiving the request or, within 30 days of receiving the request, may extend the deadline for a further period of time not exceeding 30 days in accordance with Part V of PHIPA and upon written notification to the individual.

3.1.3 PHIPA permits HICs to charge a fee for making a record of PHI available or for providing a copy of the record of PHI to the individual if the individual is first given an estimate of the fee and if the amount of the fee does not exceed the amount of reasonable cost recovery.

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.

3.1.5 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.

3.1.6 eHealth Ontario shall have a program in place to enable eHealth Ontario and HICs to satisfy their obligations in receiving and responding to Requests for Access and Requests for Correction in respect of records of PHI in the EHR 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.

¹ Note that “individual” also includes the individual’s substitute decision-maker (SDM) 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.
3.1.8 This policy and its associated procedures support an individual in exercising the individual's legislative right to make a Request for Access and a Request for Correction in respect of his or her records of PHI in the EHR and assist HICs in meeting their obligations under PHIPA in receiving and responding to such Requests for Access and Requests for Correction.

3.1.9 Without limiting the generality of paragraph 3.1.1, individuals will have the right to make a Request for Access to the following records of PHI in the EHR:

- Clinical records of the individual;
- Records of all instances where all or part of the PHI of the individual is viewed, handled or otherwise dealt with by HICs or their agents and Electronic Service Providers;
- Records of all instances where a consent directive is made, withdrawn or modified by the individual; and
- Records of all instances where a consent directive made by the individual is overridden and the purpose for which the consent directive is overridden.

3.1.10 Hospitals subject to the Freedom of Information and Protection of Privacy Act (FIPPA) are required to provide annually to the Information and Privacy Commissioner of Ontario, the reports identified in section 34 of FIPPA. Each hospital responsible for responding to a Request for Access or a Request for Correction in respect of records of PHI in the EHR shall include the number of requests and refusals in its report to the Information and Privacy Commissioner of Ontario, even if eHealth Ontario provided the records of PHI to the individual making the request on behalf of the hospital.

4 Procedure

4.1 Procedures for Responding to a Request for Access

4.1.1 Procedures from Individual for Records Created and Contributed Solely by the HIC

Where a HIC receives a Request for Access directly from an individual related to records of PHI that were created and contributed to the EHR solely by that HIC, the HIC shall follow Part V of PHIPA and its internal policies, procedures and practices to respond directly to the individual in respect of the Request for Access. This does not prevent a health information custodian or an agent of a health information custodian from, in response to an oral request for access, granting the individual access to a record of personal health information to which the individual is entitled during the provision of health care to the individual.

4.1.2 Procedures from Individual for Records Collected by the HIC

Where a HIC receives a Request for Access directly from an individual related to records of PHI that were collected by that HIC for the purpose of providing or assisting in the provision of healthcare, the HIC shall follow Part V of PHIPA and its internal policies, procedures and practices to respond directly to the individual in respect of the Request for Access. This does not prevent a health information custodian or an agent of a health information custodian from, in response to an oral request for access, granting the individual access to a record of personal health information to which the individual is entitled during the provision of health care to the individual.

4.1.3 Procedures to Records Created and Contributed by Another HIC

Where a HIC receives a Request for Access directly from an individual related to records of PHI that were created and contributed to the EHR by one or more other HICs and that the HIC that received the Request for Access has not collected, the HIC that received the Request for Access shall as soon as possible:

- Notify the individual that the Request for Access involves PHI not within the custody or control of the HIC that received the Request for Access; and
- Provide the individual with information on how to contact eHealth Ontario to make the Request for Access.

4.1.4 Procedures to Records from Another HIC

Where eHealth Ontario receives a Request for Access directly from an individual related to records of PHI that were created and contributed to the EHR, eHealth Ontario shall:

- Verify and validate the identity of the person making the Request for Access as the individual to whom the records of PHI in the EHR and that are subject to the Request for Access relate, or as the individual’s SDM;
- Notify the individual that the Request for Access will be sent to the HIC or HICs that created and contributed the records of PHI to the EHR;
- Obtain from the individual sufficient information to enable the HIC or HICs that created and contributed the records of PHI to the EHR to identify the individual in the EHR, to locate the individual's records in the EHR and to respond to the Request for Access; and
• Obtain from the individual, an address for the delivery of the response to the Request for Access or other contact information as is appropriate in the circumstances.

4.1.5 Upon a request from eHealth Ontario, HICs shall assist eHealth Ontario in verifying and validating the identity of the person making the Request for Access as the individual to whom the records of PHI in the EHR and that are subject to the Request for Access relate, or as the individual’s SDM.

4.1.6 As soon as possible, but in any event no later than 7 days after receiving a Request for Access directly from an individual related to records of PHI that were created and contributed to the EHR, eHealth Ontario shall identify the HIC or HICs that created and contributed the records of PHI to the EHR that are the subject of the Request for Access, and forward the Request for Access, to the HIC or HICs identified.

Request Received by eHealth Ontario Relates to Records Created and Contributed Solely by One HIC

4.1.7 When the Request for Access relates to records of PHI that were created and contributed to the EHR solely by one HIC, eHealth Ontario shall:

• Notify the HIC that it solely created and contributed the records of PHI to the EHR that are the subject of the Request for Access;
• Provide the HIC with the information received under paragraph 4.1.4; and
• Notify the HIC that the HIC is required to respond directly to the individual in respect of the Request for Access in accordance with Part V of PHIPA and its internal policies, procedures and practices within 30 days of the eHealth Ontario receiving the Request for Access from the individual.

4.1.8 Upon receiving a Request for Access from eHealth Ontario related to records of PHI that were created and contributed to the EHR solely by the HIC, the HIC shall follow Part V of PHIPA and its internal policies, procedures and practices to respond directly to the individual in respect of the Request for Access.

4.1.9 The HIC shall log as soon as possible that it has responded to the Request for Access.

Request Received by eHealth Ontario Relates to Records Created and Contributed by More Than One HIC

4.1.10 When the Request for Access relates to records of PHI that were created and contributed to the EHR by more than one HIC, eHealth Ontario shall:

• Notify each HIC that the records of PHI subject to the Request for Access were created and contributed by more than one HIC;
• Provide each HIC with the information received under paragraph 4.1.4;
• Advise each HIC that the HIC must, as soon as possible, but in any event no later than 21 days after receiving the Request for Access from eHealth Ontario, take the following actions:
  - Notify eHealth Ontario whether the HIC will grant the Request for Access in whole or in part and provide eHealth Ontario with explicit instructions to respond to the Request for Access;
  - Where the HIC will grant the Request for Access in whole or in part, provide eHealth Ontario with an estimate of the fee, if any, for providing access to the records of PHI;
  - Where the HIC will refuse the Request for Access in whole or in part, provide eHealth Ontario with a written notice addressed to the individual that has been prepared in accordance with Part V of PHIPA; and
  - Where the HIC is extending the time for responding to the Request for Access for a further period of time not exceeding 30 days, provide eHealth Ontario with a written notice addressed to the individual that has been prepared in accordance with Part V of PHIPA.

4.1.11 As soon as possible, but in any event no later than 21 days after receiving the Request for Access from eHealth Ontario, the HIC shall take the following actions:

• Notify the eHealth Ontario whether the HIC will grant the Request for Access in whole or in part and provide eHealth Ontario with explicit instructions to respond to the Request for Access;
• Where the HIC will grant the Request for Access in whole or in part, provide eHealth Ontario with an estimate of the fee, if any, for providing access to the records of PHI;
• Where the HIC will refuse the Request for Access in whole or in part, provide eHealth Ontario with a written notice addressed to the individual that has been prepared in accordance with Part V of PHIPA; and
• Where the HIC is extending the time for responding to the Request for Access for a further period of time not exceeding 30 days, provide eHealth Ontario with a written notice addressed to the individual that has been prepared in accordance with Part V of PHIPA.
Upon receiving request for access, eHealth Ontario shall, in accordance with Part V of PHIPA:

- Provide the individual with an estimate of the fee, if any, to provide access to the records of PHI for which the Request for Access is granted in whole or in part;
- Collect the fee, if any, on behalf of the HICs to provide access to the records of PHI for which the Request for Access is granted in whole or in part;
- Provide the individual with copies of the records of PHI for which the Request for Access is granted in whole or in part;
- Provide the individual with any written notices refusing the Request for Access in whole or in part;
- Provide the individual with any written notices extending the time for responding to a Request for Access; and
- Provide the individual with any written notices required under paragraph 4.1.12.

Within 30 days from when the individual made the Request for Access, eHealth Ontario shall, in accordance with Part V of PHIPA:

Where written notice extending the time for responding to a Request for Access has been provided to the individual, the HIC requesting the extension shall follow Part V of PHIPA and its internal policies, procedures and practices to respond directly to the individual in respect of the Request for Access.

The eHealth Ontario shall log as soon as possible that it has responded to the Request for Access on behalf of the HICs that created and contributed the records of PHI to the EHR unless the HIC did not respond to eHealth Ontario in respect of the Request for Access in accordance with the timelines in paragraph 4.1.11 or extended the time for responding to the Request for Access. A HIC that did not respond to eHealth Ontario in respect of the Request for Access in accordance with the timelines in paragraph 4.1.11 or that extended the time for responding to the Request for Access shall log as soon as possible that it has responded to the Request for Access.

Request Relates to Logs

Where a HIC receives a Request for Access directly from an individual related to the following records, the HIC shall follow Part V of PHIPA and its internal policies, procedures and practices to respond directly to the individual in respect of the Request for Access:

- Records of all instances where all or part of the PHI of the individual is viewed, handled or otherwise dealt with by HICs or their agents and Electronic Service Providers;
- Records of all instances where a consent directive is made, withdrawn or modified by the individual; and
- Records of all instances where a consent directive made by the individual is overridden and the purpose for which the consent directive is overridden.

Where the HIC that receives a Request for Access related to records referred to in paragraph 4.1.16 is unable to generate and provide copies of the records in response to the Request for Access, the HIC that received the Request for Access shall as soon as possible:

- Notify the individual that the HIC is unable to process the Request for Access; and
- Provide the individual with information on how to contact eHealth Ontario to make the Request for Access.

Where eHealth Ontario receives a Request for Access directly from an individual related to records referred to in paragraph 4.1.16, eHealth Ontario shall respond directly to the individual in respect of the Request for Access in accordance with Part V of PHIPA and its internal policies, procedures and practices.

Upon receiving the Request for Access related to records referred to in paragraph 4.1.16, eHealth Ontario shall:

- Verify and validate the identity of the person making the Request for Access as the individual to whom the records of PHI in the EHR and that are subject to the Request for Access relate, or as the individual’s SDM;
- Obtain from the individual sufficient information to enable eHealth Ontario to identify the individual in the EHR, to locate the individual’s records in the EHR and to respond to the Request for Access;
- Obtain from the individual an address for the delivery of the response to the Request for Access or other contact information as is appropriate in the circumstances; and
- Respond directly to the individual in respect of the Request for Access in accordance with Part V of PHIPA and its internal policies, procedures and practices; and
4.2 Procedures for Charging Fees for Access

4.2.1 HICs may charge a fee for providing access to records of PHI in respect of the EHR provided that:

- The HIC first gives an estimate of that fee;
- The fee does not exceed the amount of reasonable cost recovery; and
- The fee is consistent with applicable orders of the Information and Privacy Commissioner of Ontario.

4.2.2 HICs may exercise their discretion in determining to waive payment of all or any part of the fee in accordance with Part V of PHIPA and their own internal policies, procedures and practices.

4.2.3 Where the Request for Access relates to records of PHI that were created and contributed to the EHR by more than one HIC, eHealth Ontario is responsible for collecting the estimate of the fee that will be charged by the HICs that created and contributed the records, providing an estimate of the fee to the individual, if any, and for collecting the fee.

4.2.4 Where the Request for Access relates to records of PHI that were created and contributed to the EHR solely by one HIC, that HIC is responsible for providing an estimate of the fee, if any, that will be charged by that HIC and for collecting the fee.

4.2.5 eHealth Ontario will not charge a fee for its services associated with co-ordinating responses to Requests for Access or responding to Requests for Access related to records of PHI in the EHR.

4.3 Procedures for Responding to a Request for Correction

Request Directly from Individual for Records Created and Contributed Solely by the HIC

4.3.1 Where a HIC receives a Request for Correction directly from an individual related to records of PHI that were created and contributed to the EHR solely by that HIC, the HIC shall follow Part V of PHIPA and its internal policies, procedures and practices to respond directly to the individual in respect of the Request for Correction.

4.3.2 Where the HIC will grant the Request for Correction or is required to append a statement of disagreement under section 55(11) of PHIPA and the Request for Correction or statement of disagreement relates to a record of PHI in the EHR that cannot be made directly by the HIC, the HIC shall instruct eHealth Ontario as soon as possible to make the correction or append the statement of disagreement in accordance with Part V of PHIPA.

4.3.3 As soon as possible, but in any event no later than 7 days after receiving the instruction from the HIC, eHealth Ontario shall make the requested correction or append the statement of disagreement in accordance with Part V of PHIPA.

4.3.4 Upon making the requested correction or appending the statement of disagreement, eHealth Ontario shall as soon as possible, notify the HIC that eHealth Ontario has made the requested correction or appended the statement of disagreement and how the requested correction was made to enable the HIC to fulfill its obligations under section 55 of PHIPA.

4.3.5 Upon granting the Request for Correction the HIC shall, in accordance with section 55(10) of PHIPA:

- Give notice to the individual in respect of how the requested correction was made as soon as possible; and
- At the request of the individual, give written notice of the requested correction, to the extent reasonably possible, to the persons to whom the HIC disclosed the PHI, as soon as possible, except if the correction cannot reasonably be expected to have an effect on the ongoing provision of health care or other benefits to the individual.

4.3.6 The HIC shall log as soon as possible that it has responded to the Request for Correction.

4.3.7 eHealth Ontario shall ensure that the EHR maintains and displays a history of all corrections of records of PHI in the EHR, regardless of whether the correction is made by the HIC or eHealth Ontario.

4.3.8 HICs and eHealth Ontario shall ensure that all corrections of records of PHI in the EHR are made in accordance with section 55(10) of PHIPA.
Request Relates to Records Created and Contributed Solely by Another HIC or More Than One HIC

4.3.9 Where a HIC receives a Request for Correction directly from an individual related to records of PHI that were created and contributed to the EHR solely by another HIC or by more than one HIC, the HIC that received the Request for Correction shall as soon as possible:

- Notify the individual that the Request for Correction involves PHI not within the custody or control of the HIC that received the Request for Correction; and
- Provide the individual with information on how to contact eHealth Ontario to make the Request for Correction.

4.3.10 Where eHealth Ontario receives a Request for Correction directly from an individual related to records of PHI in the EHR created and contributed by one or more HICs, eHealth Ontario shall:

- Verify and validate the identity of the person making the Request for Correction as the individual to whom the records of PHI in the EHR and that are subject to the Request for Correction relate, or as the individual’s SDM;
- Notify the individual that the Request for Correction will be sent to the HIC or HICs that created and contributed the records of PHI to the EHR;
- Obtain from the individual sufficient information to enable the HIC or HICs that created and contributed the records of PHI to the EHR to identify the individual in the EHR, to locate the individual’s records in the EHR and to respond to the Request for Correction; and
- Obtain from the individual an address for the delivery of the response to the Request for Correction or other contact information as is appropriate in the circumstances.

4.3.11 Upon a request from eHealth Ontario, HICs shall assist eHealth Ontario in verifying and validating the identity of the person making the Request for Correction as the individual to whom the records of PHI in the EHR and that are subject to the Request for Correction relates, or as the individual’s SDM.

4.3.12 As soon as possible, but in any event no later than 7 days after receiving a Request for Correction, eHealth Ontario shall identify the HIC or HICs that created and contributed the records of PHI to the EHR that are the subject of the Request for Correction, and forward the Request for Correction to each of the HICs that have been identified.

4.3.13 In forwarding the Request for Correction, eHealth Ontario shall:

- Provide each HIC with the information received under paragraph 4.3.10; and
- Notify each HIC that the HIC is required to respond directly to the individual in respect of the Request for Correction in accordance with Part V of PHIPA and its internal policies, procedures and practices.

4.3.14 Upon receiving a Request for Correction from eHealth Ontario related to records of PHI that were created and contributed to the EHR by the HIC, the HIC shall follow Part V of PHIPA and its internal policies, procedures and practices to respond directly to the individual in respect of the Request for Correction.

4.3.15 Where the HIC will grant the Request for Correction or is required to append a statement of disagreement under section 54(11) of PHIPA and the Request for Correction or statement of disagreement relates to a record of PHI in the EHR that cannot be made directly by the HIC, the HIC shall instruct eHealth Ontario as soon as possible to make the correction or append the statement of disagreement in accordance with Part V of PHIPA.

4.3.16 As soon as possible, but in any event no later than 7 days after receiving the instruction from the HIC, eHealth Ontario shall make the requested correction or append the statement of disagreement, in accordance with Part V of PHIPA and notify the HIC that eHealth Ontario has made the requested correction or appended the statement of disagreement and how the requested correction was made to enable the HIC to fulfill its obligations under section 55 of PHIPA.

4.3.17 Upon granting the Request for Correction the HIC shall, in accordance with section 55(10) of PHIPA:

- Give notice to the individual in respect of how the requested correction was made as soon as possible; and
- At the request of the individual, given written notice of the requested correction, to the extent reasonably possible, to the persons to whom the HIC disclosed the PHI as soon as possible, except if the correction cannot reasonably be expected to have an effect on the ongoing provision of health care or other benefits to the individual.

4.3.18 The HIC shall log as soon as possible that it has responded to the Request for Correction.

4.3.19 eHealth Ontario shall ensure that the EHR maintains and displays a history of all corrections of records of PHI in the EHR regardless of whether the correction is made by the HIC or eHealth Ontario.

4.3.20 HICs and eHealth Ontario shall ensure that all corrections of records of PHI in the EHR are made in accordance with section 55(10) of PHIPA.
4.4 Complaints Related to Requests for Access, Requests for Correction and Fees

4.4.1 All complaints related to Requests for Access, Requests for Correction and fees for responding to Requests for Access shall be dealt with in accordance with the Electronic Health Record Inquiries and Complaints Policy and its associated procedures, as amended from time to time.

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 applicable oversight body.

5.1.2 The applicable oversight body has the authority 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.

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

Request for Access
A request made by an individual to exercise the right under Part V of PHIPA to access the individual’s records of PHI in the custody or control of a HIC. Without limiting the generality of the foregoing, an individual may make a Request for Access to the following records in respect of the EHR:

- Clinical records of the individual;
- Records of all instances where all or part of the PHI of the individual is viewed, handled or otherwise dealt with by HICs or their agents and Electronic Service Providers;
- Records of all instances where a consent directive is made, withdrawn or modified by the individual; and
- Records of all instances where a consent directive made by the individual is overridden and the purpose for which the consent directive is overridden.

Request for Correction
A request made by an individual to exercise the right under Part V of PHIPA to request a correction of the individual’s records of PHI that the individual believes are inaccurate or incomplete for the purposes for which the PHI has been collected or used or is being used.

<table>
<thead>
<tr>
<th>Policy Governance Structure</th>
<th>ConnectingOntario Solution</th>
<th>Diagnostic Imaging Common Services Repository</th>
</tr>
</thead>
</table>

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

<table>
<thead>
<tr>
<th>Applicable Oversight Body</th>
<th>Privacy: ConnectingOntario Committee</th>
<th>Security: eHealth Ontario Strategy Committee</th>
<th>Privacy: Diagnostic Imaging Common Services Executive Committee</th>
<th>Security: eHealth Ontario Strategy Committee</th>
</tr>
</thead>
</table>

### Term or Acronym | Definition
--- | ---
HIC | Health Information Custodian

| Term or Acronym | Definition |
--- | ---
PHI | Personal Health Information, as defined in the *Personal Health Information Protection Act, 2004*

| Term or Acronym | Definition |
--- | ---
PHIPA | *Personal Health Information Protection Act, 2004*

| Term or Acronym | Definition |
--- | ---
SDM | Substitute Decision-Maker

### 7 References and Associated Documents

*Personal Health Information Protection Act, 2004 (PHIPA)*
Information and Privacy Commissioner of Ontario (IPC), Order HO-009
*Electronic Health Record Inquiries and Complaints Policy* and its associated procedures
Assurance Policy
Electronic Health Record

Version: 2.0
Document ID: 3874
Copyright Notice
Copyright © 2017, eHealth Ontario

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 eHealth Ontario. The information contained in this document is proprietary to eHealth Ontario and may not be used or disclosed except as expressly authorized in writing by eHealth Ontario.

Trademarks
Other product names mentioned in this document may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.
Document Control

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

Approval History

<table>
<thead>
<tr>
<th>APPROVER(S)</th>
<th>APPROVED DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connecting Privacy Committee Members</td>
<td>December 8, 2016</td>
</tr>
</tbody>
</table>

Revision History

<table>
<thead>
<tr>
<th>VERSION NO.</th>
<th>DATE YYYY-MM-DD</th>
<th>SUMMARY OF CHANGE</th>
<th>CHANGED BY</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.0</td>
<td>2016-12-01</td>
<td>Revisions as per CPC Policy Evaluation</td>
<td>Rand Muhtam, Privacy Analyst, eHealth Ontario</td>
</tr>
<tr>
<td>1.1</td>
<td>2015-11-25</td>
<td>Minor revisions – updated for ConnectingOntario</td>
<td>Samara Strub, Privacy Analyst, eHealth Ontario</td>
</tr>
<tr>
<td>1.0</td>
<td>2014-11-17</td>
<td>Final version</td>
<td>Urooj Kirmani, Senior Privacy Analyst, eHealth Ontario</td>
</tr>
<tr>
<td>0.01</td>
<td>2014-11-04</td>
<td>Initial draft based on ConnectingPrivacy Committee Harmonized Assurance Policy v1.2</td>
<td>Promila Gonsalves, Privacy Analyst, eHealth Ontario</td>
</tr>
</tbody>
</table>
Contents

1  Purpose/Objective ................................................................. 1
2  Scope .............................................................................. 1
3  Policy ............................................................................. 1
  3.1 Guiding Policies ....................................................................................................................... 1
4  Procedure ........................................................................ 2
  4.1 Procedures for Privacy Impact Assessments ................................................................. 2
  4.2 Procedures for Privacy and Security Readiness Self-Assessment ..................................... 5
  4.3 Procedures for Privacy and Security Operational Self-Attestation ....................................... 5
  4.4 Assurance of Agents, Electronic Service Providers and Third Parties ............................. 7
  4.5 Auditing and Monitoring ....................................................................................................... 7
  4.6 Non-Compliance .................................................................................................................. 9
5  Enforcement ..................................................................... 9
6  Glossary and Terms ............................................................ 10
7  References and Associated Documents .................................................. 11
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.

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 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;
- 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.
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;
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.

<table>
<thead>
<tr>
<th>Policy Governance Structure</th>
<th>ConnectingOntario Solution</th>
<th>Diagnostic Imaging Common Services Repository</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applicable Privacy and Security Committee</td>
<td>Privacy: Connecting Privacy Committee</td>
<td>Privacy: Diagnostic Imaging Common Services Privacy and Security Working Group</td>
</tr>
<tr>
<td></td>
<td>Security: Connecting Security Committee</td>
<td>Security: Connecting Security Committee</td>
</tr>
<tr>
<td>Applicable Oversight Body</td>
<td>Privacy: ConnectingOntario Committee</td>
<td>Privacy: Diagnostic Imaging Common Services Executive Committee</td>
</tr>
<tr>
<td></td>
<td>Security: eHealth Ontario Strategy Committee</td>
<td>Security: eHealth Ontario Strategy Committee</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Term</th>
</tr>
</thead>
<tbody>
<tr>
<td>HIC</td>
<td>Health Information Custodian</td>
</tr>
<tr>
<td>PHI</td>
<td>Personal Health Information, as defined in the <em>Personal Health Information Protection Act, 2004</em></td>
</tr>
</tbody>
</table>
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
Document Control

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

Approval History

<table>
<thead>
<tr>
<th>APPROVER(S)</th>
<th>APPROVED DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>ConnectingPrivacy Committee Members</td>
<td>2014-04-30</td>
</tr>
</tbody>
</table>

Revision History

<table>
<thead>
<tr>
<th>VERSION NO.</th>
<th>DATE</th>
<th>SUMMARY OF CHANGE</th>
<th>CHANGED BY</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3</td>
<td>2016-03-01</td>
<td>Updated to reflect purpose of access and consent directive override functionality in DI CS</td>
<td>Promila Gonsalves, Senior Privacy Analyst, eHealth Ontario</td>
</tr>
<tr>
<td>1.2</td>
<td>2015-11-25</td>
<td>Minor revisions – updated for ConnectingOntario</td>
<td>Samara Strub, Privacy Analyst, eHealth Ontario</td>
</tr>
<tr>
<td>1.1</td>
<td>2015-10-30</td>
<td>Updated consent directive levels and consent override reasons for Diagnostic Imaging Common Services</td>
<td>Promila Gonsalves, Senior Privacy Analyst, eHealth Ontario</td>
</tr>
<tr>
<td>1.0</td>
<td>2014-11-17</td>
<td>Final version</td>
<td>Urooj Kirmani, Senior Privacy Analyst, eHealth Ontario</td>
</tr>
<tr>
<td>0.01</td>
<td>2014-11-04</td>
<td>Initial draft based on ConnectingPrivacy Committee Harmonized Consent Management Policy v1.3.</td>
<td>Promila Gonsalves, Privacy Analyst, eHealth Ontario</td>
</tr>
</tbody>
</table>
## Contents

1 Purpose/Objective ................................................................. 1

2 Scope .................................................................................. 1

3 Policy ................................................................................. 1

   3.1 Guiding Policies .................................................................. 1

4 Procedure ............................................................................. 3

   4.1 Procedures for Obtaining Consent ...................................... 3
   4.2 Procedures for Receiving and Implementing Consent Directives ................................................................. 3
   4.3 Procedures for Testing and Confirming Consent Directives Implemented ................................................... 7
   4.4 Procedures for Notifying Individuals of Consent Directive Implementation ..................................................... 7
   4.5 Procedures for Logging, Auditing and Monitoring Consent Directives that are Made, Modified or Withdrawn 7
   4.6 Procedures for Overriding a Consent Directive ................................................................................................. 7

5 Enforcement ......................................................................... 9

6 Glossary and Terms .............................................................. 10

7 References and Associated Documents ............................... 11
1 Purpose/ Objective

To define the policies, procedures and practices that apply in obtaining the consent of the individual in respect of the collection, use or disclosure of the individual's personal health information (PHI) in the Electronic Health Record (EHR) for the purpose of providing or assisting in the provision of health care to the individual.

To define the policies, procedures and practices that apply in implementing Consent Directives of the individual to give, withhold or withdraw consent to the collection, use or disclosure of the individual’s PHI in the EHR for the purpose of providing or assisting in the provision of health care to the individual.

To define the policies, procedures and practices that applies in overriding Consent Directives.

2 Scope

This policy and its associated procedures apply to obtaining consent, implementing Consent Directives and overriding Consent Directives in respect of the individual’s PHI in the EHR for the purpose of providing or assisting in the provision of health care to the individual and not to obtaining consent, implementing Consent Directives or overriding Consent Directives in respect of any other PHI or for any other purpose. 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.

3 Policy

3.1 Guiding Policies

3.1.1 This policy and its associated procedures will enable health information custodians (HICs) and eHealth Ontario to meet their obligations under the Personal Health Information Protection Act, 2004 (PHIPA) with respect to obtaining consent, receiving and implementing requests from individuals to make, modify or withdraw Consent Directives and overriding Consent Directives in the EHR.

3.1.2 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.

3.1.3 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.

3.1.4 eHealth Ontario shall have a program in place to enable HICs and eHealth Ontario to satisfy their responsibilities to receive and implement requests from individuals to make, modify or withdraw Consent Directives and their responsibilities in respect of overriding Consent Directives in the EHR in accordance with PHIPA, applicable agreements and this policy and its associated procedures.

1 Note that “individual” means the individual to whom the PHI relates and also includes the individual's substitute decision-maker 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.
3.1.5 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.

**Collection, Use or Disclosure of PHI in the EHR**

3.1.6 Subject to paragraph 3.1.13, a HIC is permitted to collect PHI:

- For the purpose of providing or assisting in the provision of health care to the individual; or

<table>
<thead>
<tr>
<th>Connecting Ontario Solution Only</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Eliminating or reducing a significant risk of serious bodily harm to a person or group of persons, where the HIC believes on reasonable grounds that the collection is necessary for this purpose.</td>
</tr>
</tbody>
</table>

3.1.7 PHIPA permits a HIC to assume an individual's implied consent to collect, use or disclose the individual's PHI for the purpose of providing or assisting in the provision of health care to the individual, unless the individual has expressly withheld or withdrawn such consent.

3.1.8 A HIC that collects PHI from the EHR for the purpose of providing or assisting in the provision of health care to the individual, may use or disclose the PHI for any purpose permitted by PHIPA.

3.1.9 A HIC that collects PHI from the ConnectingOntario Solution for the purpose of eliminating or reducing a significant risk of serious bodily harm to a person or group of persons, shall not use or disclose that PHI except for the purpose for which the PHI was collected.

**Giving, Withholding or Withdrawing Consent Through Consent Directives**

3.1.10 PHIPA gives the individual the right to give, withhold or withdraw consent to the collection, use or disclosure of the individual's PHI for the purpose of providing or assisting in the provision of health care to the individual. The individual may exercise this right by making, modifying or withdrawing a Consent Directive.

3.1.11 The individual may make, modify or withdraw the following Consent Directives in respect of the individual's PHI in the EHR:

<table>
<thead>
<tr>
<th>Diagnostic Imaging Common Services Repository3:</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Domain Consent Directives</td>
</tr>
<tr>
<td>- Record-Level Consent Directives</td>
</tr>
<tr>
<td>- HIC-Agents Consent Directives</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ConnectingOntario Solution:</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Global Consent Directives4</td>
</tr>
<tr>
<td>- Domain Consent Directives</td>
</tr>
<tr>
<td>- HIC-Records Consent Directives</td>
</tr>
<tr>
<td>- HIC-Agents Consent Directives</td>
</tr>
<tr>
<td>- Agent Consent Directives</td>
</tr>
</tbody>
</table>

3.1.12 This policy and its associated procedures will support the individual in exercising the right to give, withhold or withdraw consent to the collection, use or disclosure of the individual's PHI in the EHR for the purpose of providing or assisting in the provision of health care to the individual.

---

3 Additional consent management functionality will be added as technology becomes available.

4 The Global Consent Directive and Domain Consent Directive are the same at this time because the EHR is the only domain that is subject to the *Electronic Health Record Consent Management Policy* and its associated procedures, as amended from time to time.
Overriding Consent Directives

3.1.13 A HIC or an agent of a HIC shall only override a Consent Directive to collect PHI where the HIC or the agent of the HIC:

- Obtains the express consent of the individual to whom the PHI relates;

**Connecting Ontario Solution Only**

- Believes on reasonable grounds that the collection is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm to the individual to whom the PHI relates and it is not reasonably possible to obtain the consent of the individual in a timely manner; or

- Believes on reasonable grounds that the collection is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm to a person other than the individual to whom the PHI relates or to a group of persons.

3.1.14 A HIC or an agent of a HIC that overrides a Consent Directive to collect PHI in the EHR, shall only use or disclose that PHI for the purpose for which the PHI was collected.

3.1.15 All instances where all or part of the PHI in the EHR is collected as a result of an override of a Consent Directive shall be audited and monitored and notice of the collection shall be provided to the HIC or the HIC whose agents collected the PHI that is the subject of the Consent Directive, and to the individual to whom the PHI relates.

4 Procedure

4.1 Procedures for Obtaining Consent

4.1.1 HICs shall obtain consent from the individual in respect of the collection, use and disclosure of the individual’s PHI in the EHR in accordance with PHIPA and their internal policies, procedures and practices.

4.1.2 HICs shall post, make readily available or provide individuals the notice described in paragraph 4.1.3.

4.1.3 eHealth Ontario shall make available to HICs a notice that:

- Contains a general description of the PHI in the EHR;
- Describes the administrative, technical and physical safeguards and practices that are maintained with respect to PHI in the EHR;
- Describes the persons and organizations that are permitted to collect, use and disclose PHI in the EHR;
- Describes the purposes for which these persons and organizations may collect, use and disclose PHI in the EHR;
- Indicates that individuals have the right to give, withhold or withdraw consent to the collection, use or disclosure of their PHI in the EHR for the purpose of providing or assisting in the provision of their health care by making, modifying or withdrawing Consent Directives;
- Provides contact information for the person(s) to whom individuals may direct requests to make, modify or withdraw Consent Directives in the EHR;
- Provides contact information for the person(s) to whom individuals may direct requests for access and correction or direct inquiries or complaints in respect of PHI in the EHR; and
- Describes how individuals may make a complaint to the Information and Privacy Commissioner of Ontario in respect of the EHR.

4.2 Procedures for Receiving and Implementing Consent Directives

Receipt of Consent Directives
4.2.1 Where a HIC or eHealth Ontario receives a request to make, modify or withdraw a Consent Directive in the EHR, the HIC or eHealth Ontario shall follow its internal policies, procedures and practices to respond to the request while meeting the requirements under paragraph 4.2.2.

4.2.2 Upon receiving a request from the individual to make, modify or withdraw a Consent Directive in the EHR, the eHealth Ontario or the HIC shall:

- Log receipt of the request;
- Verify and validate that the person making the request is the individual to whom the PHI that is the subject of the request relates or the individual’s SDM;
- Obtain from the individual sufficient information to identify the individual in the EHR, to locate the individual’s PHI in the EHR and to implement the request;
- If the request does not contain sufficient detail, offer assistance to the individual making the request;
- Inform the individual about the impact of making, modifying, or withdrawing a Consent Directive;
- Inform the individual about the circumstances in which a Consent Directive may be overridden to collect PHI;
- Inform the individual that he or she will receive a notice in all instances where all or part of the individual’s PHI in the EHR is collected as a result of an override of a Consent Directive;
- Inform the individual that he or she may make, modify or withdraw a Consent Directive at any time;
- Obtain from the individual an address for delivery of the notice required under paragraph 4.4.1; and
- Where applicable, notify the individual that the request will be forwarded to eHealth Ontario to assist with the implementation of the request.

4.2.3 Paragraphs 4.2.1 and 4.2.2 do not apply where a HIC receives a request to make, modify or withdraw a HIC-Records Consent Directive in respect of PHI that was created and contributed to the EHR by another HIC.

4.2.4 Upon a request from eHealth Ontario, HICs shall assist eHealth Ontario in verifying and validating the identity of the person making the request as the individual to whom the PHI that is the subject of the request relates or as the individual’s SDM.

**Implementation of Global, Domain, Record-Level and HIC-Agents Consent Directives (as applicable)**

4.2.5 Where a HIC or eHealth Ontario receives a request from the individual to make, modify or withdraw a Global Consent Directive, Domain Consent Directive, Record-Level Consent Directive and/or HIC-Agents Consent Directive (as applicable according to paragraph 3.1.11) in the EHR, the HIC or eHealth Ontario shall, as soon as possible, but in any event no later than 7 days after verifying and validating the identity of the individual making the request:

- Implement the request; and
- Take reasonable steps to test and confirm that the request has been implemented.

4.2.6 Immediately after implementing and taking reasonable steps to test and confirm that the request has been implemented, the HIC or eHealth Ontario that received the request shall provide to the individual the notice required under paragraph 4.4.1.

**Implementation of HIC-Records Consent Directives**

4.2.7 Where a HIC receives a request from the individual to make, modify or withdraw a HIC-Records Consent Directive in respect of PHI that the HIC created and contributed to the EHR, the HIC shall:

5 Record-Level Consent Directives can only be implemented by eHealth Ontario.

6 For the Diagnostic Imaging Common Services, the HIC-Record Consent Directive is not currently in place. HICs will be notified when this functionality is active.
• Implement and take reasonable steps to test and confirm that the request has been implemented as soon as possible, but in any event no later than 7 days after verifying and validating the identity of the individual making the request; and

• Immediately after implementing and taking reasonable steps to test and confirm that the request has been implemented, provide to the individual the notice required under paragraph 4.4.1.

4.2.8 Where the HIC is not able to implement the request under paragraph 4.2.7 directly in the EHR, the HIC shall forward the request to eHealth Ontario as soon as possible, but in any event no later than 7 days after verifying and validating the identity of the individual making the request.

4.2.9 When forwarding a request to eHealth Ontario under paragraph 4.2.8, the HIC shall include:

• The identity of the individual to whom the PHI which is the subject of the request relates;

• The request from the individual to make, modify or withdraw a HIC-Records Consent Directive; and

• Sufficient information to identify the individual in the EHR, to locate the individual’s PHI in the EHR, to identify the HIC who is the subject of the request and to implement the request.

4.2.10 Upon receiving a forwarded request under paragraph 4.2.8, eHealth Ontario shall implement and take reasonable steps to test and confirm that the request has been implemented as soon as possible, but in any event no later than 7 days after receipt of the information under paragraph 4.2.9.

4.2.11 eHealth Ontario shall, as soon as possible after implementing and taking reasonable steps to test and confirm that the request has been implemented in accordance with paragraph 4.2.10, notify the HIC that the request has been implemented, tested and confirmed and that the HIC must provide to the individual the notice required under paragraph 4.4.1.

4.2.12 Immediately after receiving the notification under paragraph 4.2.11, the HIC shall provide to the individual the notice required under paragraph 4.4.1.

4.2.13 Where a HIC receives a request to make, modify or withdraw a HIC-Records Consent Directive in respect of PHI that was created and contributed to the EHR by another HIC, the HIC that receives the request shall, as soon as possible, but in any event no later than 7 days after receipt of the request:

• Notify the person that the HIC is unable to implement the request because it is in respect of PHI that was created and contributed to the EHR by another HIC; and

• Provide the person with information on how to contact eHealth Ontario to implement the Consent Directive.

4.2.14 Where eHealth Ontario receives a request from the individual to make, modify or withdraw a HIC-Records Consent Directive in respect of PHI in the EHR, eHealth Ontario shall:

• Implement and take reasonable steps to test and confirm that the request has been implemented as soon as possible, but in any event no later than 7 days after verifying and validating the identity of the individual making the request;

• Upon the request of the individual, notify the HIC that created and contributed the PHI that is the subject of the HIC-Records Consent Directive that a HIC-Records Consent Directive has been made, modified, or withdrawn; and

• Immediately after implementing and taking reasonable steps to test and confirm that the request has been implemented, provide to the individual the notice required under paragraph 4.4.1.

Implementation of Agent Consent Directives (as applicable)7

4.2.15 Where a HIC receives a request from the individual to make, modify or withdraw an Agent Consent Directive (as applicable according to paragraph 3.1.11) in the EHR, the HIC, as soon as possible, but in any event no later than 7 days after verifying and validating the identity of the individual making the request, shall:

---

7 For the Diagnostic Imaging Common Services, the Agent Consent Directive is not currently in place. HICs will be notified when this functionality is active.
• Implement and take reasonable steps to test and confirm that the request has been implemented; and
• Forward the request to eHealth Ontario.

4.2.16 When forwarding a request to eHealth Ontario under paragraph 4.2.15, the HIC shall include:
• The identity of the individual to whom the PHI which is the subject of the request relates;
• The request from the individual to make, modify or withdraw an Agent Consent Directive;
• The Agent Consent Directive implemented by the HIC; and
• Sufficient information to identify the individual in the EHR, to locate the individual’s PHI in the EHR, to identify the agent or agents who are the subject of the request and to implement the request.

4.2.17 Upon receiving a forwarded request under paragraph 4.2.15, eHealth Ontario shall, as soon as possible, but in any event no later than 7 days after receipt of the information under paragraph 4.2.16:
• Take reasonable steps to identify all HICs on whose behalf the agent or agents who are the subject of the request are collecting, using or disclosing PHI in the EHR;
• Implement and take reasonable steps to test and confirm that the request has been implemented, regardless of the HICs on whose behalf the agent or agents are collecting, using or disclosing PHI in the EHR; and
• Notify the HIC that the request has been implemented, tested and confirmed and that the HIC must provide to the individual the notice required under paragraph 4.4.1.

4.2.18 Immediately after receiving the notification under paragraph 4.2.17, the HIC shall provide to the individual, the notice required under paragraph 4.4.1.

4.2.19 Where eHealth Ontario receives a request from the individual to make, modify or withdraw an Agent Consent Directive in the EHR, eHealth Ontario shall, as soon as possible, but in any event no later than 7 days after verifying and validating the identity of the individual making the request:
• Take reasonable steps to identify all HICs on whose behalf the agent or agents who are the subject of the request are collecting, using or disclosing PHI in the EHR; and
• Implement and take reasonable steps to test and confirm that the request has been implemented, regardless of the HICs on whose behalf the agent or agents are collecting, using or disclosing PHI in the EHR.

4.2.20 Immediately after implementing and taking reasonable steps to test and confirm that the request has been implemented under paragraph 4.2.19, eHealth Ontario shall provide to the individual the notice required under paragraph 4.4.1.

4.2.21 In taking reasonable steps to identify all HICs on whose behalf the agent or agents who are the subject of the request are collecting, using and disclosing PHI in the EHR, and in taking reasonable steps to implement the request, regardless of the HICs on whose behalf the agent or agents are collecting, using or disclosing PHI in the EHR, eHealth Ontario shall:
• Search the Provider Registry to identify all potential accounts associated with the agent or agents who are the subject of the request;
• Contact the agent or agents that are the subject of the request to identify and confirm any other HICs on whose behalf the agent or agents are collecting, using or disclosing PHI in the EHR;
• Contact each HIC to verify whether the agent or agents are collecting, using or disclosing PHI on behalf of the HIC and to verify that the account in the Provider Registry is associated with the agent or agents who are the subject of the request; and
• Implement an Agent Consent Directive on each account associated with the agent or agents who are the subject of the request.

4.2.22 After implementing and taking reasonable steps to test and confirm that an Agent Consent Directive has been implemented under paragraphs 4.2.17 or 4.2.19, as the case may be, eHealth Ontario shall continuously audit and monitor the Agent Consent Directive to ensure that it continues to apply to all agents who are the subject of the Agent Consent Directive, regardless of the HICs on whose behalf the agent or agents are collecting, using or disclosing PHI in the EHR.

4.2.23 In continuously auditing and monitoring Agent Consent Directives under paragraph 4.2.22, eHealth Ontario shall:
• Maintain a list of all agents who are the subject of an Agent Consent Directive;
• Monitor changes to the accounts associated with the agents on the list of agents who are the subject of an Agent Consent Directive; and
• Evaluate changes to the accounts of the agents and update the Agent Consent Directive as required.

4.3 Procedures for Testing and Confirming Consent Directives Implemented

4.3.1 HICs and eHealth Ontario shall take reasonable steps to test and confirm that the requests to make, modify or withdraw Consent Directives that they have implemented in the EHR are properly implemented.

4.4 Procedures for Notifying Individuals of Consent Directive Implementation

4.4.1 Immediately after the HIC or eHealth Ontario that received a request from the individual to make, modify or withdraw a Consent Directive has implemented the request and has taken reasonable steps to test and confirm that the request has been implemented in the EHR, or has received notification that the request has been implemented, tested and confirmed in the EHR, as the case may be, the HIC or eHealth Ontario shall provide to the individual a notice:

• Describing the request received from the individual;
• Identifying and describing the Consent Directive that was made, modified or withdrawn in the EHR;
• Confirming that the Consent Directive was made, modified or withdrawn and the date that it was made, modified or withdrawn;
• Describing the impact of making, modifying or withdrawing the Consent Directive;
• Describing the circumstances in which the Consent Directive may be overridden to collect PHI;
• Indicating that the individual will receive a notice in all instances where all or part of the individual’s PHI in the EHR is collected as a result of an override of the Consent Directive;
• Providing contact information for the person to whom individuals may direct inquiries or complaints related to the Consent Directive;
• Indicating that the individual may make, modify or withdraw a Consent Directive at any time; and
• Where the eHealth Ontario is providing the notice, identify that eHealth Ontario is providing the notice on behalf of the HICs that collect, use or disclose PHI in the EHR.

4.4.2 The HIC or eHealth Ontario, as the case may be, shall keep a copy of the notice provided to the individual under paragraph 4.4.1 or a log of the notices provided.

4.5 Procedures for Logging, Auditing and Monitoring Consent Directives that are Made, Modified or Withdrawn

4.5.1 eHealth Ontario shall ensure that the EHR is capable of logging all instances where a Consent Directive is made, modified or withdrawn in the EHR and that the log contains the information required in PHIPA and the Electronic Health Record Logging and Auditing Policy and its associated procedures, as amended from time to time.

4.5.2 eHealth Ontario shall audit and monitor all instances where a Consent Directive is made, modified or withdrawn in the EHR in accordance with the Electronic Health Record Logging and Auditing Policy and its associated procedures, as amended from time to time.

4.5.3 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 request of an individual to make, modify or withdraw a Consent Directive in the EHR in accordance with the Electronic Health Record Logging and Auditing Policy and its associated procedures, as amended from time to time.

4.6 Procedures for Overriding a Consent Directive
4.6.1 eHealth Ontario shall ensure that the EHR is capable of notifying the HIC or the agent of the HIC if the PHI that is sought to be collected is the subject of a Consent Directive, as long as no PHI that is the subject of a Consent Directive is provided.

4.6.2 eHealth Ontario shall ensure that the EHR requires the HIC or the agent of the HIC that is seeking to collect PHI that is the subject of a Consent Directive, to identify for which of the three permitted purposes the Consent Directive is being overridden to collect PHI, in particular, whether the HIC or the agent of the HIC that is seeking to collect the PHI:

- Has obtained the express consent of the individual to whom the PHI relates;
- Believes on reasonable grounds that the collection is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm to the individual to whom the PHI relates and it is not reasonably possible to obtain the consent of the individual in a timely manner; or
- Believes on reasonable grounds that the collection is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm to a person other than the individual to whom the PHI relates or to a group of persons.

4.6.3 The HIC or the agent of the HIC that is seeking to collect PHI in the EHR that is the subject of a Consent Directive shall identify the purpose under paragraph 4.6.2 for which the Consent Directive is being overridden to collect PHI.

4.6.4 The HIC or the agent of the HIC that is seeking to collect PHI in the EHR that is the subject of a Consent Directive based on the express consent of the individual, shall obtain such consent in accordance with PHIPA; the HIC's internal policies, procedures and practices; and the requirements under paragraph 4.6.5.

4.6.5 In obtaining the express consent of the individual, the HIC or the agent of the HIC that is seeking to collect PHI in the EHR that is the subject of a Consent Directive, shall ensure that the individual knows:

- The purpose of the collection;
- He or she may give or withhold consent;
- The override of the Consent Directive will be in effect for no more than 4 hours for Diagnostic Imaging Common Services Repository and 24 hours for the ConnectingOntario Solution; and
- The PHI will only be used or disclosed for the purpose for which the PHI was collected.

4.6.6 eHealth Ontario shall ensure that the EHR is capable of logging all instances where all or part of the PHI in the EHR is disclosed to and collected by a HIC or an agent of a HIC as a result of an override of a Consent Directive.

4.6.7 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 or an agent of a HIC as a result of an override of a Consent Directive contains the information required under PHIPA and the Electronic Health Record Logging and Auditing Policy and its associated procedures, as amended from time to time.

4.6.8 eHealth Ontario shall continuously audit and monitor the log in paragraph 4.6.7 in accordance with the Electronic Health Record Logging and Auditing Policy and its associated procedures, as amended from time to time, and immediately provide written notice to the HIC or the HIC whose agent overrode a Consent Directive in the EHR to collect PHI. At a minimum, the notice shall set out:

- The HIC that disclosed the PHI that is the subject of the Consent Directive;
- The HIC that collected the PHI that is the subject of the Consent Directive;
- The agent of the HIC that collected the PHI that is the subject of the Consent Directive;
- The individual to whom the PHI that is the subject of the Consent Directive relates;
- The type of PHI subject to the Consent Directive that was collected;
- The date and time the PHI subject to the Consent Directive was collected; and
- The purpose for which the Consent Directive was overridden to collect PHI.

4.6.9 Upon receiving the notice under paragraph 4.6.8, the HIC that overrode or whose agent overrode a Consent Directive in the EHR to collect PHI shall, at the first reasonable opportunity, provide a notice to the individual to whom the PHI relates. The notice shall be in written form or as instructed by the
individual. At a minimum, the notice shall indicate that a Consent Directive was overridden to collect PHI and shall identify:

- The type of PHI subject to the Consent Directive that was collected;
- The HIC that collected the PHI that is the subject of the Consent Directive;
- The agent of the HIC that collected the PHI that is the subject of the Consent Directive;
- The date and time the PHI subject to the Consent Directive was collected;
- The HIC that disclosed the PHI that is the subject of the Consent Directive;
- The purpose for which the Consent Directive was overridden to collect PHI;
- The person to whom individuals may direct inquiries or complaints related to the override of a Consent Directive and contact information for this person; and
- How to make a complaint to the Information and Privacy Commissioner of Ontario.

4.6.10 A HIC that overrode or whose agent overrode a Consent Directive in the EHR to collect PHI shall keep a copy of the notice provided to the individual under section 4.6.9 or a log of the notices provided.

4.6.11 A HIC that overrode or whose agent overrode a Consent Directive in the EHR to collect PHI for the purpose of eliminating or reducing a significant risk of serious bodily harm to a person other than the individual to whom the PHI relates or to a group of persons, shall not provide identifying information about the person or group of persons at significant risk of serious bodily harm in the notice required under paragraph 4.6.9.

4.6.12 A HIC that overrode or whose agent overrode a Consent Directive in the EHR to collect PHI for the purpose of eliminating or reducing a significant risk of serious bodily harm to a person other than the individual to whom the PHI relates or to a group of persons, shall provide written notice to the Information and Privacy Commissioner of Ontario in a manner that does not provide identifying information about the individual to whom the PHI relates or the person or group of persons at significant risk of serious bodily harm.

4.6.13 The notice required under paragraph 4.6.12 shall be provided to the Information and Privacy Commissioner of Ontario as soon as possible, but in any event no later than 7 days after receipt of the notice under paragraph 4.6.8, and shall identify:

- The HIC that disclosed the PHI that is the subject of the Consent Directive;
- The HIC that collected the PHI that is the subject of the Consent Directive;
- The agent of the HIC that collected the PHI that is the subject of the Consent Directive;
- The type of PHI subject to the Consent Directive that was collected; and
- The date and time the PHI subject to the Consent Directive was collected.

5 Enforcement

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

---

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

Agent Consent Directive  
A Consent Directive made by the individual to give, withhold or withdraw consent to the collection, use and disclosure of all of the individual’s PHI in the EHR by one or more but not all agents of one or more but not all HICs.

Consent Directive  
A directive made by the individual to withhold or withdraw, in whole or in part, his or her consent to the collection, use or disclosure of the individual’s PHI in the EHR for the purpose of providing or assisting in the provision of health care to the individual, and includes a directive to modify or withdraw a directive that has already been made. The following demographic information cannot be made subject to a Consent Directive because it is required to uniquely identify the individual in the EHR for the purpose of managing privacy procedures related to the individual and to ensure the accuracy of the PHI in the EHR:

- First Name
- Last Name
- Gender
- Date of Birth
- Primary Address (street, postal code, city, province, country)
- Health Card Number (if available)
- HIC ID and MRN assigned by the HIC (if available)

Domain Consent Directive  
A Consent Directive made by the individual to withhold or withdraw consent to the collection, use and disclosure of all of the individual’s PHI in one or more but not all of the repositories in [NAME OF SYSTEM].

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.

Global Consent Directive  
A Consent Directive made by the individual to withhold or withdraw consent to the collection, use and disclosure of all of the individual’s PHI in the EHR.

HIC-Agents Consent Directive  
A Consent Directive made by the individual to give, withhold or withdraw consent to the collection, use and disclosure of all of the individual’s PHI in the EHR by all agents of one or more but not all HICs.

HIC-Records Consent Directive  
A Consent Directive made by the individual to give, withhold or withdraw consent to the collection, use and disclosure of all of the individual’s PHI created and contributed to the EHR by one or more but not all HICs.

9 The Global Consent Directive and Domain Consent Directive are the same at this time because the Electronic Health Record is the only domain that is subject to the Electronic Health Record Consent Management Policy and its associated procedures, as amended from time to time.
Table 1: Applicable Governance Bodies

<table>
<thead>
<tr>
<th>Term or Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>HIC</td>
<td>Health Information Custodian</td>
</tr>
<tr>
<td>PHI</td>
<td>Personal Health Information, as defined in the <em>Personal Health Information Protection Act, 2004</em></td>
</tr>
<tr>
<td>PHIPA</td>
<td><em>Personal Health Information Protection Act, 2004</em></td>
</tr>
<tr>
<td>SDM</td>
<td>Substitute Decision-Maker</td>
</tr>
</tbody>
</table>

7 References and Associated Documents

*Personal Health Information Protection Act, 2004 (PHIPA)*
*Electronic Health Record Logging and Auditing Policy* and its associated procedures
Copyright Notice
Copyright © 2017, eHealth Ontario

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 eHealth Ontario. The information contained in this document is proprietary to eHealth Ontario and may not be used or disclosed except as expressly authorized in writing by eHealth Ontario.

Trademarks
Other product names mentioned in this document may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.
### Document Control

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

### Approval History

<table>
<thead>
<tr>
<th>APPROVER(S)</th>
<th>APPROVED DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>ConnectingPrivacy Committee Members</td>
<td>2014-06-26</td>
</tr>
</tbody>
</table>

### Revision History

<table>
<thead>
<tr>
<th>VERSION NO.</th>
<th>DATE YYYY-MM-DD</th>
<th>SUMMARY OF CHANGE</th>
<th>CHANGED BY</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>2015-11-25</td>
<td>Minor revisions – updated for ConnectingOntario</td>
<td>Samara Strub, Privacy Analyst, eHealth Ontario</td>
</tr>
<tr>
<td>1.0</td>
<td>2014-11-17</td>
<td>Final version</td>
<td>Urooj Kirmani, Senior Privacy Analyst, eHealth Ontario</td>
</tr>
<tr>
<td>0.01</td>
<td>2014-11-04</td>
<td>Initial draft based on ConnectingPrivacy Committee Harmonized Inquiries and Complaints Policy v1.1.</td>
<td>Promila Gonsalves, Privacy Analyst, eHealth Ontario</td>
</tr>
</tbody>
</table>
Contents

1 Purpose/ Objective 1

2 Scope 1

3 Policy 1
   3.1 Guiding Policies ................................................................. 1

4 Procedure 2
   4.1 Procedures Related to Inquiries ........................................... 2
   4.2 Procedures Related to Complaints ........................................ 4

5 Enforcement 7

6 Glossary and Terms 7

7 References and Associated Documents 9
1 Purpose/ Objective

To define the policies, procedures and practices that apply in receiving, documenting, tracking, addressing and responding to Inquiries and Complaints in respect of the Electronic Health Record (EHR).

2 Scope

This policy and its associated procedures apply to Inquiries and Complaints in respect of 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.

This policy and its associated procedures do not apply to Inquiries or Complaints in respect of any system other than the EHR or in respect of any information other than personal health information (PHI) in the EHR.

3 Policy

3.1 Guiding Policies

3.1.1 The Personal Health Information Protection Act, 2004 (PHIPA) requires a health information custodian (HIC) that is not a natural person, such as a HIC that is a corporation or partnership, to designate a contact person to respond to Inquiries about the HIC’s information practices, to receive Complaints about the HIC’s alleged contravention of PHIPA and to ensure 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 respond to Inquiries about the HIC’s information practices, to receive Complaints about the HIC’s alleged contravention of PHIPA and to ensure 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 A person who has reasonable grounds to believe that a HIC, eHealth Ontario or one of their agents or Electronic Service Providers has contravened or is about to contravene PHIPA may also make a complaint to the Information and Privacy Commissioner of Ontario.

3.1.4 This policy and its associated procedures will support a person in exercising his or her right to make an Inquiry or Complaint in respect of the EHR, and will enable HICs and eHealth Ontario to meet their obligations under PHIPA in this regard.

3.1.5 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.
3.1.6 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.

3.1.7 eHealth Ontario shall have a program in place to enable HICs and eHealth Ontario to satisfy their obligations in receiving, documenting, tracking, addressing and responding to Inquiries and Complaints in respect of the EHR in accordance with PHIPA, applicable agreements and this policy and its associated procedures.

3.1.8 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.

4 Procedure

4.1 Procedures Related to Inquiries

Inquiry Relates to the Party Receiving the Inquiry

4.1.1 Where a HIC directly receives an Inquiry related solely to the HIC or to the agents or Electronic Service Providers of that HIC2, the HIC shall receive, document, track, address and respond directly to the person making the Inquiry as soon as possible, but in any event no later than 30 days following receipt of the Inquiry, in accordance with its internal policies, procedures and practices.

4.1.2 Where eHealth Ontario directly receives an Inquiry related solely to eHealth Ontario or to the agents or Electronic Service Providers of eHealth Ontario, eHealth Ontario shall receive, document, track, address and respond directly to the person making the Inquiry as soon as possible, but in any event no later than 30 days following receipt of the Inquiry, in accordance with its internal policies, procedures and practices.

HIC Receives Inquiry Relating to eHealth Ontario, another HIC or More Than One HIC

4.1.3 Where a HIC directly receives an Inquiry that it is able to address and respond to related to another HIC, more than one HIC, eHealth Ontario or to the agents or Electronic Service Providers of another HIC, more than one HIC or eHealth Ontario, the HIC receiving the Inquiry shall receive, document, track, address and respond directly to the person making the Inquiry as soon as possible, but in any event no later than 30 days following receipt of the Inquiry, in accordance with its internal policies, procedures and practices.

4.1.4 Where a HIC directly receives an Inquiry under paragraph 4.1.3 that it is unable to address and respond to, the HIC shall, as soon as possible, but in any event no later than 4 days following receipt of the Inquiry:

- Notify the person making the Inquiry that the HIC is unable to address and respond to the Inquiry; and
- Provide the person making the Inquiry with information on how to contact eHealth Ontario to make the Inquiry.

eHealth Ontario Receives Inquiry Relating to One or More HICs

4.1.5 Where eHealth Ontario directly receives an Inquiry that it is able to address and respond to related to one or more HICs or to the agents or Electronic Service Providers of one or more HICs, eHealth Ontario shall receive, document, track, address and respond directly to the person making the Inquiry as soon as possible, but in any event no later than 30 days following receipt of the Inquiry, in accordance with its internal policies, procedures and practices.

4.1.6 Where eHealth Ontario directly receives an Inquiry that it is unable to address and respond to under paragraph 4.1.5, eHealth Ontario shall:

- Log receipt of the Inquiry;

---

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.
• Advise the person making the Inquiry as soon as possible, but in any event no later than 4 days following receipt of the Inquiry, that:
  - eHealth Ontario received the Inquiry;
  - eHealth Ontario will forward the Inquiry to the HIC or HICs to whom the Inquiry relates, as the case may be;
  - The person making the Inquiry will receive a response to the Inquiry from the HIC in paragraph 4.1.7 or eHealth Ontario, as the case may be, as soon as possible, but in any event no later than 30 days following receipt of the Inquiry by eHealth Ontario;
  - The person making the Inquiry will be provided with a revised date for response if the Inquiry cannot be responded to within 30 days following receipt of the Inquiry by eHealth Ontario;
• Obtain sufficient information from the person making the Inquiry in order to facilitate the preparation of a response to the Inquiry; and
• Obtain from the person making the Inquiry the preferred method of contact and contact information for the response to the Inquiry.

4.1.7 Upon receiving an Inquiry related solely to one HIC, eHealth Ontario shall, as soon as possible, but in any event no later than 4 days following receipt of the Inquiry:
• Forward the Inquiry to the HIC to whom the Inquiry relates;
• Notify the HIC that the Inquiry received relates solely to that HIC;
• Provide the HIC with the date that the Inquiry was received by eHealth Ontario;
• Provide the HIC with information about the identity of the person making the Inquiry, the preferred method of contact of the person making the Inquiry, contact information for the response to the Inquiry and sufficient information to facilitate the preparation of a response to the Inquiry; and
• Notify the HIC that it must, as soon as possible, but in any event no later than 30 days following receipt of the Inquiry by eHealth Ontario, either respond directly to the person making the Inquiry in accordance with the HIC’s internal policies, procedures and practices or provide the person making the Inquiry with a revised date for response if the Inquiry cannot be responded to within that timeframe.

4.1.8 Upon receiving a forwarded Inquiry from eHealth Ontario related solely to that HIC, that HIC shall:
• Receive, document, track, address and respond directly to the person making the Inquiry as soon as possible, but in any event no later than 30 days following receipt of the Inquiry by eHealth Ontario, in accordance with its internal policies, procedures and practices;
• Provide the person making the Inquiry with a revised date for response as soon as possible, but in any event no later than 30 days following receipt of the Inquiry by eHealth Ontario, if the Inquiry cannot be responded to within 30 days following receipt of the Inquiry by eHealth Ontario; and
• Record that the Inquiry was responded to by maintaining a copy of the response or logging that the Inquiry was responded to.

4.1.9 Upon receiving an Inquiry related to more than one HIC, eHealth Ontario shall, as soon as possible, but in any event no later than 4 days following receipt of the Inquiry:
• Forward the Inquiry to each HIC to whom the Inquiry relates;
• Notify each HIC that the Inquiry received relates to more than one HIC;
• Provide each HIC with the date that the Inquiry was received by eHealth Ontario;
• Provide each HIC with information about the identity of the person making the Inquiry; and
• Advise each HIC that it must, as soon as possible, but in any event no later than 14 days following receipt of the Inquiry by eHealth Ontario, provide to eHealth Ontario the information necessary to enable eHealth Ontario to draft a proposed response to the Inquiry on behalf of each HIC.

4.1.10 Upon receiving a forwarded Inquiry from eHealth Ontario related to more than one HIC, each HIC to whom the Inquiry relates shall, as soon as possible, but in any event no later than 14 days following receipt of the
Inquiry by eHealth Ontario, provide eHealth Ontario with the information necessary to enable eHealth Ontario to draft a proposed response to the Inquiry on behalf of each HIC.

4.1.11 eHealth Ontario shall, as soon as possible, but in any event no later than 4 days following receipt of the information under paragraph 4.1.10, draft a proposed response to the person making the Inquiry and provide the proposed response to each HIC to whom the Inquiry relates for comments.

4.1.12 Upon receiving the proposed response under paragraph 4.1.11, each HIC shall provide comments to eHealth Ontario as soon as possible, but in any event no later than 4 days following receipt of the proposed response. If comments are not provided within 4 days after receipt of the proposed response, it will be assumed that there are no comments.

4.1.13 Upon receiving comments on the proposed response to the Inquiry related to more than one HIC, eHealth Ontario shall, as soon as possible, but in any event no later than 4 days following receipt of the comments under paragraph 4.1.12, respond to the person making the Inquiry.

4.1.14 Where one or more HICs do not provide the information necessary to enable eHealth Ontario to respond to the Inquiry in accordance with the timelines in paragraph 4.1.10, eHealth Ontario shall provide written notice to the person making the Inquiry that one or more HICs have failed to respond to the Inquiry and that the person may make an Inquiry or Complaint to one or more of the HICs that failed to respond and/or a complaint to the Information and Privacy Commissioner of Ontario.

4.1.15 Where the Inquiry is related to more than one HIC, eHealth Ontario shall provide the person making the Inquiry with a revised date for response if the Inquiry cannot be responded to within 30 days following receipt of the Inquiry by eHealth Ontario.

4.2 Procedures Related to Complaints

Complaint Relates to the Party Receiving the Complaint

4.2.1 Where a HIC directly receives a Complaint related solely to the HIC or to the agents or Electronic Service Providers of that HIC, the HIC shall receive, document, track, investigate, remediate and respond directly to the person making the Complaint as soon as possible, but in any event no later than 30 days following receipt of the Complaint, in accordance with its internal policies, procedures and practices.

4.2.2 Where eHealth Ontario directly receives a Complaint related solely to eHealth Ontario or to the agents or Electronic Service Providers of eHealth Ontario, eHealth Ontario shall receive, document, track, investigate, remediate and respond directly to the person making the Complaint as soon as possible, but in any event no later than 30 days following receipt of the Complaint, in accordance with its internal policies, procedures and practices.

HIC Receives Complaint Relating to eHealth Ontario, Another HIC or More Than One HIC

4.2.3 Where a HIC directly receives a Complaint related to another HIC, more than one HIC, eHealth Ontario or to the agents or Electronic Service Providers of another HIC, more than one HIC or eHealth Ontario, the HIC receiving the Complaint shall, as soon as possible, but in any event no later than 4 days following receipt of the Complaint:

- Notify the person making the Complaint that the HIC is unable to address and respond to the Complaint; and
- Provide the person making the Complaint with information on how to contact eHealth Ontario to make the Complaint.

eHealth Ontario Receives Complaint Relating to One or More HICs

4.2.4 Where eHealth Ontario directly receives a Complaint related to one or more HICs or to the agents or Electronic Service Providers of one or more HICs, eHealth Ontario shall:

- Log receipt of the Complaint;
- Advise the person making the Complaint as soon as possible, but in any event no later than 4 days following receipt of the Complaint, that:
  - eHealth Ontario received the Complaint;
  - eHealth Ontario will forward the Complaint to the HIC or HICs to whom the Complaint relates, as the case may be;
- The person making the Complaint will receive a response to the Complaint from the HIC in paragraph 4.2.7 or eHealth Ontario, as the case may be, as soon as possible, but in any event no later than 30 days following receipt of the Complaint by eHealth Ontario;

- The person making the Complaint will be provided with a revised date for response if the Complaint cannot be responded to within 30 days following receipt of the Complaint by eHealth Ontario;

  - Obtain sufficient information from the person making the Complaint in order to facilitate the preparation of a response to the Complaint; and
  - Obtain from the person making the Complaint the preferred method of contact and contact information for the response to the Complaint.

4.2.5 Where eHealth Ontario receives an anonymous Complaint, that Complaint shall be reported, contained, investigated and remediated in accordance with the Electronic Health Record Privacy Breach Management Policy or the Electronic Health Record Information Security Incident Management Policy and their associated procedures, as amended from time to time. eHealth Ontario shall take all reasonable steps to inform the person making an anonymous Complaint of the possible limitations related to the investigation of anonymous Complaints, which include:

  - Limitations on investigating a Complaint related to records of personal health information of an anonymous individual; and
  - Limitations on proactively and directly providing the person making the anonymous Complaint a response to the Complaint.

4.2.6 Upon receiving a Complaint related solely to one HIC, eHealth Ontario shall, as soon as possible, but in any event no later than 4 days following receipt of the Complaint:

  - Forward the Complaint to the HIC to whom the Complaint relates;
  - Notify the HIC that the Complaint received relates solely to that HIC;
  - Provide the HIC with the date that the Complaint was received by eHealth Ontario;
  - Provide the HIC with information about the identity of the person making the Complaint, the preferred method of contact of the person making the Complaint, contact information for the response to the Complaint and sufficient information to facilitate the preparation of a response to the Complaint; and
  - Notify the HIC that it must, as soon as possible, but in any event no later than 30 days following receipt of the Complaint by eHealth Ontario, either respond directly to the person making the Complaint in accordance with the HIC’s internal policies, procedures and practices or provide the person making the Complaint with a revised date for response if the Complaint cannot be responded to within that timeframe.

4.2.7 Upon receiving a forwarded Complaint from eHealth Ontario related solely to that HIC, that HIC shall:

  - Receive, document, track, investigate, remediate and respond directly to the person making the Complaint as soon as possible, but in any event no later than 30 days following receipt of the Complaint by eHealth Ontario, in accordance with the HIC’s internal policies, procedures, and practices;
  - Provide the person making the Complaint with a revised date for response as soon as possible, but in any event no later than 30 days following receipt of the Complaint by eHealth Ontario, if the Complaint cannot be responded to within 30 days following receipt of the Complaint by eHealth Ontario; and
  - Record that the Complaint was responded to by maintaining a copy of the response or logging that the Complaint was responded to.

4.2.8 Upon receiving a Complaint related to more than one HIC, eHealth Ontario shall, as soon as possible, but in any event no later than 4 days following receipt of the Complaint:

  - Forward the Complaint to each HIC to whom the Complaint relates;
  - Notify each HIC that the Complaint received relates to more than one HIC;
  - Provide each HIC with the date that the Complaint was received by eHealth Ontario;
• Provide each HIC with information about the identity of the person making the Complaint; and
• Advise each HIC that it must, as soon as possible, but in any event no later than 14 days following receipt of the Complaint by eHealth Ontario, provide to eHealth Ontario the information necessary to enable eHealth Ontario to determine whether to investigate the Complaint and, if the Complaint will not be investigated, to draft a proposed response to the Complaint on behalf of each HIC.

4.2.9 Upon receiving a forwarded Complaint from eHealth Ontario related to more than one HIC, eHealth Ontario to whom the Complaint relates shall, as soon as possible, but in any event no later than 14 days following receipt of the Complaint by eHealth Ontario, provide eHealth Ontario with the information necessary to enable eHealth Ontario to determine whether to investigate the Complaint and, if the Complaint will not be investigated, to draft a proposed response to the Complaint on behalf of each HIC.

4.2.10 eHealth Ontario shall, as soon as possible, but in any event no later than 4 days following receipt of the information under paragraph 4.2.9, determine whether to investigate the Complaint. A Complaint shall be investigated where the Complaint relates to an actual or suspected Privacy Breach or to an actual or suspected Security Breach that has occurred or is about to occur in respect of the EHR.

4.2.11 Where the Complaint relates to more than one HIC and eHealth Ontario has made a determination to investigate the Complaint under paragraph 4.2.10, eHealth Ontario shall notify each HIC to whom the Complaint relates that:
• eHealth Ontario has made a determination to investigate the Complaint;
• The Complaint relates to an actual or suspected Privacy Breach or an actual or suspected Security Breach that has occurred or is about to occur in respect of the EHR; and
• The Complaint will be reported, contained, investigated and remediated and notification will be provided in accordance with the Electronic Health Record Privacy Breach Management Policy and its associated procedures or will be reported, contained, investigated and remediated in accordance with the Electronic Health Record Information Security Incident Management Policy and its associated procedures, as amended from time to time.

4.2.12 Where the Complaint relates to an actual or suspected Privacy Breach, the actual or suspected Privacy Breach shall be reported, contained, investigated and remediated and notification shall be provided in accordance with the Electronic Health Record Privacy Breach Management Policy and its associated procedures, as amended from time to time.

4.2.13 Where the Complaint relates to an actual or suspected Security Breach, the actual or suspected Security Breach shall be reported, contained, investigated and remediated in accordance with the Electronic Health Record Information Security Incident Management Policy and its associated procedures, as amended from time to time.

4.2.14 Where the Complaint relates to an actual or suspected Security Breach or where the Complaint relates to an actual or suspected Privacy Breach and the Complaint is made by a person other than the individual to whom the personal health information relates, eHealth Ontario shall respond to the person making the Complaint as soon as possible, but in any event no later than 5 days after receipt of the written report approved by the applicable oversight body under the Electronic Health Record Privacy Breach Management Policy or Electronic Health Record Information Security Incident Management Policy and their associated procedures, as amended from time to time. At a minimum, the response shall:
• Acknowledge receipt of the Complaint;
• Indicate that an investigation was undertaken in response to the Complaint;
• Indicate whether or not a Privacy Breach or Security Breach occurred and, if so, provide a description of the Privacy Breach or Security Breach and the scope of and circumstances in which the Privacy Breach or Security Breach occurred;
• Provide a summary of the results of the investigation and the measures that have been or will be implemented to remediate the Privacy Breach or Security Breach and to prevent similar Privacy Breaches or Security Breaches in future;
• Provide the name and contact information for the person or persons to whom the person making the Complaint may address inquiries or concerns; and
• Advise the person making the Complaint that he or she may make a complaint to the Information and Privacy Commissioner of Ontario.
4.2.15 Where eHealth Ontario has made a determination not to investigate the Complaint under paragraph 4.2.10, eHealth Ontario shall, as soon as possible, but in any event no later than 4 days following receipt of the information under paragraph 4.2.9:

- Notify each HIC to whom the Complaint relates that eHealth Ontario has made a determination not to investigate the Complaint; and
- Provide each HIC with a proposed response to the person making the Complaint and advise each HIC that it must, as soon as possible, but in any event no later than 4 days following receipt of the proposed response, provide comments on the proposed response to eHealth Ontario to enable eHealth Ontario to respond to the Complaint on behalf of each HIC.

4.2.16 Upon receiving the proposed response under paragraph 4.2.15, each HIC shall provide comments to eHealth Ontario as soon as possible, but in any event no later than 4 days following receipt of the proposed response. If comments are not provided within 4 days after receipt of the proposed response, it will be assumed that there are no comments.

4.2.17 Upon receiving comments on the proposed response to the Complaint related to more than one HIC, eHealth Ontario shall, as soon as possible, but in any event no later than 4 days following receipt of the comments, respond to the person making the Complaint. At a minimum, the response shall:

- Provide a response to the Complaint;
- Provide the name and contact information for the person or persons to whom the person making the Complaint may address inquiries or concerns; and
- Advise the person making the Complaint that he or she may make a complaint to the Information and Privacy Commissioner of Ontario.

4.2.18 Where one or more HICs do not provide the information necessary to enable eHealth Ontario to respond to the Complaint in accordance with the timelines in paragraph 4.2.9, eHealth Ontario shall provide written notice to the person making the Complaint that one or more HICs have failed to respond to the Complaint and that the person may make a Complaint to one or more of the HICs that failed to respond and/or a complaint to the Information and Privacy Commissioner of Ontario.

4.2.19 eHealth Ontario shall provide the person making the Complaint with a revised date for response if the Complaint cannot be responded to within 30 days following receipt of the Complaint by eHealth Ontario.

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 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.

Complaint

3 References to the applicable privacy and security committee and the applicable oversight body can be found in Table 1: Applicable Governance Bodies.
A concern raised by any person in respect of the EHR including, but not limited to, concerns raised in respect of compliance with PHIPA, applicable agreements and the policies, procedures and practices implemented in respect of 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.

**Inquiry**
A question raised by any person in respect of the EHR including, but not limited to, questions raised in respect of:

- When, how and the purposes for which PHI in the EHR is collected, used or disclosed or viewed, handled or otherwise dealt with;
- The administrative, technical and physical safeguards and practices maintained in respect of PHI in the EHR;
- The policies, procedures and practices implemented in respect of the EHR; and
- Compliance with PHIPA, applicable agreements and the policies, procedures and practices implemented 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

<table>
<thead>
<tr>
<th>Term or Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>HIC</td>
<td>Health Information Custodian</td>
</tr>
<tr>
<td>PHI</td>
<td>Personal Health Information, as defined in the <em>Personal Health Information Protection Act, 2004</em></td>
</tr>
<tr>
<td>PHIPA</td>
<td><em>Personal Health Information Protection Act, 2004</em></td>
</tr>
</tbody>
</table>
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
Copyright Notice
Copyright © 2017, eHealth Ontario

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 eHealth Ontario. The information contained in this document is proprietary to eHealth Ontario and may not be used or disclosed except as expressly authorized in writing by eHealth Ontario.

Trademarks
Other product names mentioned in this document may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.
Document Control

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

Approval History

<table>
<thead>
<tr>
<th>APPROVER(S)</th>
<th>APPROVED DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>ConnectingPrivacy Committee Members</td>
<td>June 24, 2014</td>
</tr>
</tbody>
</table>

Revision History

<table>
<thead>
<tr>
<th>VERSION NO.</th>
<th>DATE YYYY-MM-DD</th>
<th>SUMMARY OF CHANGE</th>
<th>CHANGED BY</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>2015-11-25</td>
<td>Minor revisions – updated for ConnectingOntario</td>
<td>Samara Strub, Privacy Analyst, eHealth Ontario</td>
</tr>
<tr>
<td>1.0</td>
<td>2014-11-17</td>
<td>Final version</td>
<td>Urooj Kirmani, Senior Privacy Analyst, eHealth Ontario</td>
</tr>
<tr>
<td>0.01</td>
<td>2014-11-04</td>
<td>Initial draft based on ConnectingPrivacy Committee Harmonized Logging and Auditing Policy v1.1.</td>
<td>Promila Gonsalves, Privacy Analyst, eHealth Ontario</td>
</tr>
</tbody>
</table>
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;
- 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.

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 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 that 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

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.

<table>
<thead>
<tr>
<th>Policy Governance Structure</th>
<th>ConnectingOntario Solution</th>
<th>Diagnostic Imaging Common Services Repository</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applicable Oversight Body</td>
<td>Privacy: ConnectingOntario Committee&lt;br&gt;Security: eHealth Ontario Strategy Committee</td>
<td>Privacy: Diagnostic Imaging Common Services Executive Committee&lt;br&gt;Security: eHealth Ontario Strategy</td>
</tr>
</tbody>
</table>

References to the applicable privacy and security committee and the applicable oversight body can be found in Table 1: Applicable Governance Bodies.
<table>
<thead>
<tr>
<th>Term or Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>HIC</td>
<td>Health Information Custodian</td>
</tr>
<tr>
<td>PHI</td>
<td>Personal Health Information, as defined in the <em>Personal Health Information Protection Act, 2004</em></td>
</tr>
<tr>
<td>PHIPA</td>
<td><em>Personal Health Information Protection Act, 2004</em></td>
</tr>
<tr>
<td>SDM</td>
<td>Substitute Decision-Maker, as defined in the <em>Personal Health Information Protection Act, 2004</em></td>
</tr>
</tbody>
</table>

### 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
Privacy and Security Training Policy

Electronic Health Record

Version: 1.2

Document ID: 3877
Copyright Notice
Copyright © 2017, eHealth Ontario

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 eHealth Ontario. The information contained in this document is proprietary to eHealth Ontario and may not be used or disclosed except as expressly authorized in writing by eHealth Ontario.

Trademarks
Other product names mentioned in this document may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.
**Document Control**

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

**Approval History**

<table>
<thead>
<tr>
<th>APPROVER(S)</th>
<th>APPROVED DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>ConnectingPrivacy Committee Members</td>
<td>September 24, 2015</td>
</tr>
</tbody>
</table>

**Revision History**

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

1 Purpose/ Objective ................................................................. 1
2 Scope .................................................................................. 1
3 Policy .................................................................................. 1
   3.1 Guiding Policies .................................................................. 1
4 Procedure .............................................................................. 2
   4.1 Procedures Related to Creating Privacy and Security Training Materials by eHealth Ontario .......... 2
   4.2 Procedures Related to Delivering Privacy and Security Training .................................................... 2
   4.3 Procedures Related to End User Agreements .............................................................................. 3
   4.4 Privacy and Security Training Content ................................................................................. 3
5 Enforcement .......................................................................... 4
6 Glossary ................................................................................ 4
7 References and Associated Documents ................................ 5
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.

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 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.

<table>
<thead>
<tr>
<th>Policy Governance Structure</th>
<th>ConnectingOntario Solution</th>
<th>Diagnostic Imaging Common Services Repository</th>
</tr>
</thead>
</table>
| **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

<table>
<thead>
<tr>
<th>Term or Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>HIC</td>
<td>Health Information Custodian</td>
</tr>
<tr>
<td>PHI</td>
<td>Personal Health Information, as defined in the <em>Personal Health Information Protection Act, 2004</em></td>
</tr>
<tr>
<td>PHIPA</td>
<td><em>Personal Health Information Protection Act, 2004</em></td>
</tr>
</tbody>
</table>

**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
**Document Control**

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

**Approval History**

<table>
<thead>
<tr>
<th>APPROVER(S)</th>
<th>APPROVED DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>ConnectingPrivacy Committee Members</td>
<td>July 6, 2016</td>
</tr>
</tbody>
</table>

**Revision History**

<table>
<thead>
<tr>
<th>VERSION NO.</th>
<th>DATE</th>
<th>SUMMARY OF CHANGE</th>
<th>CHANGED BY</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.0</td>
<td>2016-12-01</td>
<td>Revisions as per CPC Policy Evaluation</td>
<td>Rand Muhtam, Privacy Analyst, eHealth Ontario</td>
</tr>
<tr>
<td>1.1</td>
<td>2015-11-25</td>
<td>Minor revisions – updated for ConnectingOntario</td>
<td>Samara Strub, Privacy Analyst, eHealth Ontario</td>
</tr>
<tr>
<td>1.0</td>
<td>2014-11-17</td>
<td>Final version</td>
<td>Urooj Kirmani, Senior Privacy Analyst, eHealth Ontario</td>
</tr>
<tr>
<td>0.01</td>
<td>2014-11-04</td>
<td>Initial draft based on ConnectingPrivacy Committee Harmonized Privacy Breach Management Policy v1.4.</td>
<td>Promila Gonsalves, Privacy Analyst, eHealth Ontario</td>
</tr>
</tbody>
</table>
1 Purpose/Objective

To define the policies, procedures and practices that apply in identifying, reporting, containing, notifying, investigating, and remediating Privacy Breaches in respect of the Electronic Health Record (EHR).

2 Scope

This policy and its associated procedures apply to Privacy Breaches in respect of the EHR and not in respect of any system other than the EHR or in respect of any information other than personal health information (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.

3 Policy

3.1 Guiding Policies

3.1.1 The Personal Health Information Protection Act, 2004 (PHIPA) requires health information custodians (HICs) 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 and to ensure that records of PHI are protected against unauthorized copying, modification or disposal.

3.1.2 PHIPA requires HICs to ensure that records of PHI in their custody or control are retained, transferred and disposed of in a secure manner.

3.1.3 PHIPA requires agents of a HIC to notify the HIC at the first reasonable opportunity if PHI handled by the agent on behalf of the HIC is stolen, lost or accessed by unauthorized persons.

3.1.4 PHIPA requires eHealth Ontario to notify HICs at the first reasonable opportunity if eHealth Ontario or its agents or Electronic Service Providers have viewed, handled or otherwise dealt with PHI in contravention of PHIPA or if PHI is stolen, lost or accessed by unauthorized persons.

3.1.5 PHIPA requires HICs to notify individuals at the first reasonable opportunity if their PHI is stolen, lost or accessed by unauthorized persons.

3.1.6 This policy and its associated procedures will enable HICs and eHealth Ontario to meet their obligations under PHIPA with respect to identifying, reporting, containing, notifying, investigating and remediating Privacy Breaches in respect of the EHR.

3.1.7 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.

3.1.8 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.

1 Variance in policy and procedure requirements between the ConnectingOntario Solution and the Diagnostic Imaging Common Services Repository is highlighted within the policy.
eHealth Ontario shall have a program in place to enable eHealth Ontario and HICs to satisfy their responsibilities in respect of Privacy Breaches related to the EHR in accordance with PHIPA, applicable agreements and this policy and its associated procedures.

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.

### 4 Procedure

#### 4.1 Procedures for Identification of Privacy Breaches

4.1.1 HICs and eHealth Ontario shall develop and implement policies, procedures and practices to receive complaints related to actual or suspected Privacy Breaches in respect of the EHR that enable them to comply with PHIPA and the Electronic Health Record Inquiries and Complaints Policy and its associated procedures, as amended from time to time.

4.1.2 HICs and eHealth Ontario shall develop and implement policies, procedures and practices for auditing and monitoring the EHR for actual or suspected Privacy Breaches that comply with PHIPA and the Electronic Health Record Logging and Auditing Policy and its associated procedures, as amended from time to time.

4.1.3 HICs shall ensure that their agents and Electronic Service Providers notify them of actual or suspected Privacy Breaches, at the first reasonable opportunity, in accordance with PHIPA and the HICs’ internal policies, procedures and practices.

4.1.4 eHealth Ontario shall ensure that its agents and Electronic Service Providers notify eHealth Ontario of actual or suspected Privacy Breaches, at the first reasonable opportunity, in accordance with PHIPA and eHealth Ontario’s internal policies, procedures and practices.

4.1.5 A HIC shall report an actual or suspected Privacy Breach to eHealth Ontario as soon as possible, but in any event no later than the end of the next business day after the person at the HIC responsible for reporting actual or suspected Privacy Breaches to eHealth Ontario has become aware of an actual or suspected Privacy Breach caused or contributed to by:

- Another HIC or the agents or Electronic Service Providers of another HIC;
- More than one HIC or the agents or Electronic Service Providers of more than one HIC;
- eHealth Ontario or the agents or Electronic Service Providers of eHealth Ontario; or
- Any other unauthorized persons who are not agents or Electronic Service Providers of eHealth Ontario or any other HIC.

4.1.6 Upon receiving the report under paragraph 4.1.5 or upon identifying an actual or suspected Privacy Breach, eHealth Ontario shall, as soon as possible, but in any event no later than the end of the next business day after it was reported or identified, as the case may be, report the actual or suspected Privacy Breach to each HIC and each HIC whose agents or Electronic Service Providers caused or contributed to the actual or suspected Privacy Breach, where applicable.

4.1.7 The reports under paragraphs 4.1.5 and 4.1.6 shall include any information that is known and that may assist in the determination of whether a Privacy Breach has occurred.

#### 4.2 Procedures Where the Privacy Breach Was Solely Caused by a HIC that Solely Created and Contributed the PHI to the EHR

4.2.1 Where an actual or suspected Privacy Breach was solely caused by a HIC or the agents or Electronic Service Providers of a HIC\(^2\) and the HIC solely created and contributed the PHI to the EHR, the HIC shall, as soon as possible, determine whether a Privacy Breach has occurred.

---

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.
4.2.2 Where the HIC has determined that a Privacy Breach has occurred, the HIC shall:

- Report the Privacy Breach to eHealth Ontario in accordance with paragraph 4.2.3 as soon as possible, but in any event no later than the end of the next business day after making the determination that a Privacy Breach has occurred; and
- Follow its internal policies, procedures, and practices to notify the individual(s) to whom the PHI relates at the first reasonable opportunity in accordance with PHIPA and to contain, investigate and remediate the Privacy Breach.

4.2.3 In reporting the Privacy Breach to eHealth Ontario, the HIC shall provide as much information as is known at the time of reporting, including:

- An acknowledgement that the PHI in the EHR that was subject to the Privacy Breach was solely created and contributed by the HIC;
- An acknowledgement that the HIC or the agents or Electronic Service Providers of the HIC solely caused the Privacy Breach;
- The name of each agent and Electronic Service Provider of the HIC that solely caused the Privacy Breach, where the name is determined to be relevant by the HIC that solely caused the Privacy Breach (e.g., intentional unauthorized collection, use or disclosure of PHI by an agent);
- The date and time of the Privacy Breach;
- A description of the nature, scope and cause of the Privacy Breach;
- A description of the information in the EHR that was subject to the Privacy Breach, without disclosing any PHI;
- The measures implemented to contain the Privacy Breach;
- The measures that have been or will be implemented to remediate and prevent similar Privacy Breaches in future; and
- The timelines and persons responsible for implementing measures to remediate and prevent similar Privacy Breaches in future.

4.2.4 The HIC, as soon as possible after the investigation of the Privacy Breach, shall provide the eHealth Ontario and individual(s) to whom the PHI in the EHR relates with:

- A summary of the results of the investigation; and
- The measures, as is known at the time, that have been or will be implemented to remediate the Privacy Breach and to prevent similar Privacy Breaches in the future in accordance with its internal policies, procedure and practices.

4.3 Procedures Where the Privacy Breach Was Solely Caused by a HIC That Did Not Solely Create and Contribute the PHI to the EHR

Determination of Whether Privacy Breach Occurred

4.3.1 Where an actual or suspected Privacy Breach was solely caused by a HIC or the agents or Electronic Service Providers of a HIC and the HIC did not solely create and contribute the PHI to the EHR, the HIC or the HIC whose agents or Electronic Services Providers solely caused the Privacy Breach shall, as soon as possible, after the actual or suspected Privacy Breach was reported, determine whether a Privacy Breach has occurred.

Containment

4.3.2 Where the HIC or the HIC whose agents or Electronic Service Providers solely caused the Privacy Breach has determined that a Privacy Breach has occurred, that HIC shall follow its internal policies, procedures and practices to contain the Privacy Breach and, where required, request assistance from eHealth Ontario and/or other HICs under paragraph 4.3.3. in containing the Privacy Breach.

Reporting to eHealth Ontario and the HICs That Created and Contributed the PHI to the EHR

4.3.3 Where the HIC or the HIC whose agents or Electronic Service Providers solely caused the Privacy Breach has determined that a Privacy Breach has occurred or has reasonable suspicion that a Privacy Breach has occurred, the HIC shall report the Privacy Breach to eHealth Ontario as soon as possible, but in any event no
later than the end of the next business day after making the determination. In reporting the Privacy Breach, the HIC shall provide as much information as is known at time of reporting, including:

- An acknowledgement that the HIC or the agents or Electronic Service Providers of the HIC solely caused the Privacy Breach;
- The name of each agent and Electronic Service Provider of the HIC that solely caused the Privacy Breach, where the name is determined to be relevant by the HIC that solely caused the Privacy Breach (e.g., intentional unauthorized collection, use or disclosure of PHI by an agent);
- An acknowledgement that the PHI in the EHR that was subject to the Privacy Breach was not solely created and contributed by the HIC;
- The name of each HIC that created and contributed the PHI to the EHR;
- The date and time of the Privacy Breach;
- A description of the nature and scope of the Privacy Breach;
- A description of the PHI in the EHR that was subject to the Privacy Breach;
- The individual(s) to whom the PHI in the EHR relates;
- The measures implemented to contain the Privacy Breach;
- Any request for assistance from eHealth Ontario and/or other HICs in containing the Privacy Breach; and
- Sufficient information to assist with the notification of the individual(s) to whom the PHI relates in accordance with PHIPA.

4.3.4 As soon as possible, but in any event no later than the end of the next business day after receipt of the report in paragraph 4.3.3, eHealth Ontario shall report the Privacy Breach to each HIC that created and contributed the PHI to the EHR and shall advise each HIC:

- Whether the PHI in the EHR that was subject to the Privacy Breach was solely created and contributed by the HIC;
- Whether the PHI in the EHR that was subject to the Privacy Breach was created and contributed by more than one HIC and the name of each HIC;
- The name of the HIC or the HIC whose agents or Electronic Service Providers solely caused the Privacy Breach;
- The name of each agent and Electronic Service Provider of the HIC that solely caused the Privacy Breach, where the name is determined to be relevant by the HIC that solely caused the Privacy Breach (e.g., intentional unauthorized collection, use or disclosure of PHI by an agent);
- The date and time of the Privacy Breach;
- A description of the nature and scope of the Privacy Breach;
- A description of the PHI in the EHR that was subject to the Privacy Breach;
- The individual(s) to whom the PHI in the EHR relates;
- The measures implemented to contain the Privacy Breach;
- Any assistance that the HIC is being requested to provide in containing the Privacy Breach; and
- Sufficient information to assist with the notification of the individual(s) to whom the PHI relates in accordance with PHIPA.

4.3.5 eHealth Ontario and other HICs shall provide assistance in containing the Privacy Breach when requested to do so by the HIC or the HIC whose agents or Electronic Service Providers solely caused the Privacy Breach.

4.3.6 The HIC or the HIC whose agents or Electronic Service Providers solely caused the Privacy Breach shall also determine whether the Privacy Breach should be reported to any other person, including to the Information and Privacy Commissioner of Ontario, to law enforcement or to regulatory bodies in accordance with its internal policies, procedures and practices.

Notification of the Individual
4.3.7 Where the PHI in the EHR that was subject to the Privacy Breach was solely created and contributed by one other HIC, that HIC shall follow its internal policies, procedures, and practices to notify the individual(s) to whom the PHI relates at the first reasonable opportunity in accordance with PHIPA and paragraph 4.3.10.

4.3.8 Where the PHI in the EHR that was subject to the Privacy Breach was created and contributed by more than one HIC, those HICs shall, as soon as possible, but in any event no later than 7 days following receipt of the information in paragraph 4.3.4, identify the HIC that will be responsible for notifying the individual(s) to whom the PHI relates in accordance with PHIPA and paragraph 4.3.10.

4.3.9 In identifying the HIC that will be responsible for notifying individual(s), regard shall be had to:

- The HIC or the HIC whose agents or Electronic Service Providers solely caused the Privacy Breach;
- The HIC where the individual(s) most recently received health care; and
- The HIC where the individual(s) received the most health care.

4.3.10 In notifying individual(s), the HIC in paragraph 4.3.7 or 4.3.8, as the case may be, shall, at a minimum, provide the individual(s) with the following information:

- The name of the HIC or the HIC whose agents or Electronic Service Providers solely caused the Privacy Breach;
- The name of each agent and Electronic Service Provider of the HIC that solely caused the Privacy Breach, where the name is determined to be relevant by the HIC that solely caused the Privacy Breach (e.g., intentional unauthorized collection, use or disclosure of PHI by an agent);
- The name of each HIC that created and contributed the PHI to the EHR;
- The date and time of the Privacy Breach;
- A description of the nature and scope of the Privacy Breach;
- A description of the PHI in the EHR that was subject to the Privacy Breach;
- The measures implemented to contain the Privacy Breach;
- The name of the Breach Investigator;
- The HIC in paragraph 4.3.7 or 4.3.8, as the case may be, will provide the individual(s) with a summary of the results of the investigation and the measures, as is known at the time, that have been or will be implemented to remediate the Privacy Breach and to prevent similar Privacy Breaches in the future as soon as possible after the receipt of the approved written report from the eHealth Ontario under paragraph 4.3.29;
- The steps that the individual(s) can take to protect their privacy or minimize the impact of the Privacy Breach, if applicable;
- The name and contact information for the HIC in paragraph 4.3.7 or 4.3.8, as the case may be, to whom the individual(s) may address inquiries and concerns; and
- Information concerning how to make a complaint to the Information and Privacy Commissioner of Ontario.

4.3.11 eHealth Ontario and other HICs shall provide assistance in notifying the individual(s) to whom the PHI relates when requested to do so by the HIC in paragraph 4.3.7 or 4.3.8, as the case may be.

**Investigation**

4.3.12 eHealth Ontario, the HIC or HICs that created and contributed the PHI to the EHR that was subject to the Privacy Breach and the HIC or the HIC whose agents or Electronic Service Providers solely caused the Privacy Breach shall, as soon as possible, but in any event no later than 7 days after the determination that a Privacy Breach has occurred, identify a Breach Investigator.

4.3.13 In identifying the Breach Investigator under paragraph 4.3.12, regard shall be had to:

- Whether the HIC or the HIC whose agents or Electronic Services Providers solely caused the Privacy Breach has the capability to investigate the Privacy Breach; and
- Whether another HIC or eHealth Ontario would be more suitable to investigate the Privacy Breach.
4.3.14 The Breach Investigator shall, as soon as possible, but in any event no later than 7 days after the determination that a Privacy Breach has occurred, investigate the Privacy Breach in accordance with its internal policies, procedures and practices and paragraph 4.3.15.

4.3.15 In conducting the investigation, the Breach Investigator shall consult with the HIC or the HIC whose agents or Electronic Service Providers solely caused the Privacy Breach, where the HIC is not the Breach Investigator, and shall:

- Determine the nature, scope and cause of the Privacy Breach;
- Ensure the Privacy Breach has been effectively contained or determine whether further measures to contain the Privacy Breach must be implemented;
- Evaluate the adequacy of the administrative, technical and physical safeguards;
- Determine what measures must be implemented to remediate and prevent similar Privacy Breaches in future; and
- Determine the timelines and persons responsible for implementing measures to remediate and prevent similar Privacy Breaches in future.

4.3.16 Other HICs and eHealth Ontario, where they are not the Breach Investigator, shall provide assistance in investigating the Privacy Breach when requested to do so by the Breach Investigator.

4.3.17 Status reports on the investigation shall be provided by the Breach Investigator when requested by eHealth Ontario, the HIC or HICs that created and contributed the PHI to the EHR that was subject to the Privacy Breach or the HIC or the HIC whose agents or Electronic Service Providers solely caused the Privacy Breach, where they are not the Breach Investigator.

4.3.18 As soon as possible, but in any event no later than 7 days after completing the investigation, the Breach Investigator shall prepare a written report that, at a minimum, contains the following information:

- The HIC or the HIC whose agents or Electronic Service Providers solely caused the Privacy Breach;
- The name of each agent and Electronic Service Provider of the HIC that solely caused the Privacy Breach, where the name is determined to be relevant by the HIC that solely caused the Privacy Breach (e.g., intentional unauthorized collection, use or disclosure of PHI by an agent);
- The name of each HIC that created and contributed the PHI to the EHR;
- The date and time of the Privacy Breach;
- The nature, scope and cause of the Privacy Breach;
- A description of the information in the EHR that was subject to the Privacy Breach, without disclosing any PHI;
- The persons to whom the Privacy Breach was reported under paragraph 4.3.6;
- The measures implemented to contain the Privacy Breach;
- The nature, scope and process of the investigation of the Privacy Breach;
- The measures recommended to remediate and prevent similar Privacy Breaches in future; and
- The proposed timelines and persons responsible for implementing measures to remediate and prevent similar Privacy Breaches in future.

4.3.19 As soon as possible, but in any event no later than 4 days after the completion of the written report in paragraph 4.3.18, the Breach investigator shall provide the written report to the HIC or the HIC whose agents or Electronic Service Providers solely caused the Privacy Breach, where the HIC is not the Breach Investigator, for review and comment.

4.3.20 The HIC that received the written report under paragraph 4.3.19 shall, as soon as possible, but in any event no later than 7 days after receipt, review and provide comments to the Breach Investigator. If comments are not provided within 7 days after receipt, it will be assumed that there are no comments.
4.3.21 The Breach Investigator shall, as soon as possible, but in any event no later than 7 days after receipt of the comments under paragraph 4.3.20, make the required amendments and provide the written report to eHealth Ontario, where eHealth Ontario is not the Breach Investigator.

4.3.22 Where eHealth Ontario is not the Breach Investigator, eHealth Ontario shall, as soon as possible, but in any event no later than 7 days after receipt of the written report under paragraph 4.3.21, review and comment on the written report.

4.3.23 As soon as possible, but in any event no later than 7 days after receiving or preparing the written report in paragraph 4.3.21, as the case may be, eHealth Ontario shall forward the written report, along with its comments, if applicable, to the HIC or HICs that created and contributed the PHI to the EHR that was subject to the Privacy Breach for review and comment.

4.3.24 The HIC or HICs that received the written report under paragraph 4.3.23 shall, as soon as possible, but in any event no later than 7 days after receipt, review and provide comments to eHealth Ontario. If comments are not provided within 7 days after receipt, it will be assumed that there are no comments.

4.3.25 eHealth Ontario shall, as soon as possible, but in any event no later than 4 days after receipt of the comments under paragraph 4.3.24, advise the Breach Investigator, where eHealth Ontario is not the Breach Investigator, of any amendments to the written report that must be made or additional measures that must be taken to contain, investigate and/or remediate the Privacy Breach, if any.

4.3.26 The Breach Investigator shall, as soon as possible, but in any event no later than 7 days after receipt of the comments under paragraph 4.3.24 or 4.3.25, as the case may be, make the required amendments and implement the additional measures to contain, investigate and/or remediate the Privacy Breach in consultation with the HIC or the HIC whose agents or Electronic Service Providers solely caused the Privacy Breach, where the HIC is not the Breach Investigator, and prepare a revised written report.

4.3.27 Where eHealth Ontario is not the Breach Investigator, the Breach Investigator shall, as soon as possible, but in any event no later than 7 days after receipt of the comments under paragraph 4.3.25, provide the revised written report to eHealth Ontario.

4.3.28 As soon as possible, but in any event no later than 4 days after receiving or preparing the revised written report in paragraphs 4.3.26 or 4.3.27, as the case may be, eHealth Ontario shall forward the revised written report to the applicable privacy and security committee for review and approval and subsequently to the applicable oversight body for review and approval.

4.3.29 As soon as possible, but in any event no later than 4 days after the approval of the written report by the applicable oversight body, eHealth Ontario shall forward the approved written report to the HIC or the HIC whose agents or Electronic Service Providers solely caused the Privacy Breach, to each HIC that created and contributed the PHI to the EHR that was subject to the Privacy Breach and to each HIC responsible for implementing measures to remediate or prevent similar Privacy Breaches in future.

4.3.30 The HIC in paragraph 4.3.7 or 4.3.8, as the case may be, as soon as possible after the receipt of the report from the eHealth Ontario under paragraph 4.3.29, shall provide the individual(s) to whom the PHI in the EHR relates with:

- A summary of the results of the investigation; and
- The measures, as is known at the time, that have been or will be implemented to remediate the Privacy Breach and to prevent similar Privacy Breaches in the future in accordance with its internal policies, procedure and practices.

4.4 Procedures Where the Privacy Breach Was Caused or Contributed by More Than One HIC

Determination of Whether Privacy Breach Occurred

4.4.1 Where an actual or suspected Privacy Breach was caused or contributed by more than one HIC or the agents or Electronic Service Providers of more than one HIC, the HICs shall, as soon as possible, but in any event no later than the end of the next business day after the actual or suspected Privacy Breach was reported, identify the HIC responsible for determining whether a Privacy Breach has occurred and for leading containment of the Privacy Breach.

4.4.2 The HIC identified under paragraph 4.4.1 shall, as soon as possible, determine whether a Privacy Breach has occurred.
Containment

4.4.3 Where the HIC identified under paragraph 4.4.1 has determined that a Privacy Breach has occurred, that HIC shall follow its internal policies, procedures and practices to contain the Privacy Breach and, where required, request assistance from eHealth Ontario and/or other HICs under paragraph 4.4.4 in containing the Privacy Breach.

Reporting to eHealth Ontario and the HICs That Created and Contributed the PHI to the EHR

4.4.4 Where the HIC identified under paragraph 4.4.1 has determined that a Privacy Breach has occurred or has reasonable suspicion that a Privacy Breach has occurred, that HIC shall, in consultation with the other HICs and the other HICs whose agents or Electronic Service Providers caused or contributed to the Privacy Breach, report the Privacy Breach to eHealth Ontario as soon as possible, but in any event no later than the end of the next business day after making the determination. In reporting the Privacy Breach, the HIC identified under paragraph 4.4.1 shall provide as much information as is known at the time of reporting, including:

- The name of each HIC and each HIC whose agents or Electronic Service Providers caused or contributed to the Privacy Breach;
- The name of each agent and Electronic Service Provider of the HICs that caused or contributed to the Privacy Breach, where the name is determined to be relevant by the HIC identified under paragraph 4.4.1 (e.g., intentional unauthorized collection, use or disclosure of PHI by an agent);
- The name of each HIC that created and contributed the PHI to the EHR;
- The date and time of the Privacy Breach;
- A description of the nature and scope of the Privacy Breach;
- A description of the PHI in the EHR that was subject to the Privacy Breach;
- The individual(s) to whom the PHI in the EHR relates;
- The measures implemented to contain the Privacy Breach;
- Any request for assistance from eHealth Ontario and/or other HICs in containing the Privacy Breach; and
- Sufficient information to assist with the notification of the individual(s) to whom the PHI relates in accordance with PHIPA.

4.4.5 As soon as possible, but in any event no later than the end of the next business day after receipt of the report in paragraph 4.4.4, eHealth Ontario shall report the Privacy Breach to each HIC that created and contributed the PHI to the EHR and shall advise each HIC:

- Whether the PHI in the EHR that was subject to the Privacy Breach was solely created and contributed by the HIC;
- Whether the PHI in the EHR that was subject to the Privacy Breach was created and contributed by more than one HIC and the name of each HIC;
- The name of each HIC and each HIC whose agents or Electronic Service Providers caused or contributed to the Privacy Breach;
- The name of each agent and Electronic Service Provider of the HICs that caused or contributed to the Privacy Breach, where the name is determined to be relevant by the HIC identified under paragraph 4.4.1 (e.g., intentional unauthorized collection, use or disclosure of PHI by an agent);
- The date and time of the Privacy Breach;
- A description of the nature and scope of the Privacy Breach;
- A description of the PHI in the EHR that was subject to the Privacy Breach;
- The individual(s) to whom the PHI in the EHR relates;
- The measures implemented to contain the Privacy Breach;
- Any assistance that the HIC is being requested to provide in containing the Privacy Breach; and
• Sufficient information to assist with the notification of the individual(s) to whom the PHI relates in accordance with PHIPA.

4.4.6 eHealth Ontario and other HICs shall provide assistance in containing the Privacy Breach when requested to do so by the HIC identified under paragraph 4.4.1.

4.4.7 The HIC identified under paragraph 4.4.1 shall also determine, in consultation with the other HICs and the other HICs whose agents or Electronic Service Providers caused or contributed to the Privacy Breach, whether the Privacy Breach should be reported to any other person, including to the Information and Privacy Commissioner of Ontario, to law enforcement or to regulatory bodies in accordance with its internal policies, procedures and practices.

Notification of the Individual

4.4.8 Where the PHI in the EHR that was subject to the Privacy Breach was solely created and contributed by one other HIC, that HIC shall follow its internal policies, procedures and practices to notify the individual(s) to whom the PHI relates at the first reasonable opportunity in accordance with PHIPA and paragraph 4.4.11.

4.4.9 Where the PHI in the EHR that was subject to the Privacy Breach was created and contributed by more than one HIC, those HICs shall, as soon as possible, but in any event no later than 7 days following receipt of the information in paragraph 4.4.5, identify the HIC that will be responsible for notifying the individual(s) to whom the PHI relates in accordance with PHIPA and paragraph 4.4.11.

4.4.10 In identifying the HIC that will be responsible for notifying individual(s), regard shall be had to:

• The HICs or the HICs whose agents or Electronic Service Providers caused or contributed to the Privacy Breach;
• The HIC where the individual(s) most recently received health care; and
• The HIC where the individual(s) received the most health care.

4.4.11 In notifying individual(s), the HIC in paragraph 4.4.8 or 4.4.9, as the case may be, shall, at a minimum, provide the individual(s) with the following information:

• The name of each HIC and each HIC whose agents or Electronic Service Providers caused or contributed to the Privacy Breach;
• The name of each agent and Electronic Service Provider of the HICs that caused or contributed to the Privacy Breach, where the name is determined to be relevant by the HIC identified under paragraph 4.4.1 (e.g., intentional unauthorized collection, use or disclosure of PHI by an agent);
• The name of each HIC that created and contributed the PHI to the EHR;
• The date and time of the Privacy Breach;
• A description of the nature and scope of the Privacy Breach;
• A description of the PHI in the EHR that was subject to the Privacy Breach;
• The measures implemented to contain the Privacy Breach;
• The name of the Breach Investigator;
• The HIC in paragraph 4.4.8 or 4.4.9, as the case may be, will provide the individual(s) with a summary of the results of the investigation and the measures, as is known at the time, that have been or will be implemented to remediate the Privacy Breach and to prevent similar Privacy Breaches in the future as soon as possible after the receipt of the approved written report from the eHealth Ontario under paragraph 4.4.30;
• The steps that the individual(s) can take to protect their privacy or minimize the impact of the Privacy Breach, if applicable;
• The name and contact information for the HIC in paragraph 4.4.8 or 4.4.9, as the case may be, to whom the individual(s) may address inquiries and concerns; and
• Information concerning how to make a complaint to the Information and Privacy Commissioner of Ontario.

4.4.12 eHealth Ontario and other HICs shall provide assistance in notifying the individual(s) to whom the PHI relates when requested to do so by the HIC in paragraph 4.4.8 or 4.4.9, as the case may be.
Investigation

4.4.13 eHealth Ontario, the HIC or HICs that created and contributed the PHI to the EHR that was subject to the Privacy Breach and the HICs or the HICs whose agents or Electronic Service Providers caused or contributed to the Privacy Breach shall, as soon as possible, but in any event no later than 7 days after the determination that a Privacy Breach has occurred, identify a Breach Investigator.

4.4.14 In identifying the Breach Investigator under paragraph 4.4.13, regard shall be had to:
- Whether the HICs or the HICs whose agents or Electronic Service Providers caused or contributed to the Privacy Breach have the capability to investigate the Privacy Breach; and
- Whether another HIC or eHealth Ontario would be more suitable to investigate the Privacy Breach.

4.4.15 The Breach Investigator shall, as soon as possible, but in any event no later than 7 days after the determination that a Privacy Breach has occurred, investigate the Privacy Breach in accordance with its internal policies, procedures and practices and paragraph 4.4.16.

4.4.16 In conducting the investigation, the Breach Investigator shall consult with the HICs and the HICs whose agents or Electronic Service Providers caused or contributed to the Privacy Breach that are not the Breach Investigator, and shall:
- Determine the nature, scope and cause of the Privacy Breach;
- Ensure the Privacy Breach has been effectively contained or determine whether further measures to contain the Privacy Breach must be implemented;
- Evaluate the adequacy of the administrative, technical and physical safeguards;
- Determine what measures must be implemented to remediate and prevent similar Privacy Breaches in future; and
- Determine the timelines and persons responsible for implementing measures to remediate and prevent similar Privacy Breaches in future.

4.4.17 Other HICs and eHealth Ontario, where they are not the Breach Investigator, shall provide assistance in investigating the Privacy Breach when requested to do so by the Breach Investigator.

4.4.18 Status reports on the investigation shall be provided by the Breach Investigator when requested by eHealth Ontario, the HIC or HICs that created and contributed the PHI to the EHR that was subject to the Privacy Breach or the HICs or the HICs whose agents or Electronic Service Providers caused or contributed to the Privacy Breach, where they are not the Breach Investigator.

4.4.19 As soon as possible, but in any event no later than 7 days after completing the investigation, the Breach Investigator shall prepare a written report that, at a minimum, contains the following information:
- The name of each HIC and each HIC whose agents or Electronic Service Providers caused or contributed to the Privacy Breach;
- The name of each agent and Electronic Service Provider of the HICs that caused or contributed to the Privacy Breach, where the name is determined to be relevant by the HIC identified under paragraph 4.4.1 (e.g., intentional unauthorized collection, use or disclosure of PHI by an agent);
- The name of each HIC that created and contributed the PHI to the EHR;
- The date and time of the Privacy Breach;
- The nature, scope and cause of the Privacy Breach;
- A description of the information in the EHR that was subject to the Privacy Breach, without disclosing any PHI;
- The persons to whom the Privacy Breach was reported under paragraph 4.4.7;
- The measures implemented to contain the Privacy Breach;
- The nature, scope and process of the investigation of the Privacy Breach;
The measures recommended to remediate and prevent similar Privacy Breaches in future; and

The proposed timelines and persons responsible for implementing measures to remediate and prevent similar Privacy Breaches in future.

4.4.20 As soon as possible, but in any event no later than 4 days after the completion of the written report in paragraph 4.4.19, the Breach Investigator shall provide the written report to each HIC and each HIC whose agents or Electronic Service Providers caused or contributed to the Privacy Breach, that are not the Breach Investigator, for review and comment.

4.4.21 The HICs that received the written report under paragraph 4.4.20 shall, as soon as possible, but in any event no later than 7 days after receipt, review and provide comments to the Breach Investigator. If comments are not provided within 7 days after receipt, it will be assumed that there are no comments.

4.4.22 The Breach Investigator shall, as soon as possible, but in any event no later than 7 days after receipt of the comments under paragraph 4.4.21, make the required amendments and provide the written report to eHealth Ontario, where eHealth Ontario is not the Breach Investigator.

4.4.23 Where eHealth Ontario is not the Breach Investigator, eHealth Ontario shall, as soon as possible, but in any event no later than 7 days after receipt of the written report under paragraph 4.4.22, review and comment on the written report.

4.4.24 As soon as possible, but in any event no later than 7 days after receiving or preparing the written report in paragraph 4.4.22, as the case may be, eHealth Ontario shall forward the written report, along with its comments, if applicable, to the HIC or HICs that created and contributed the PHI to the EHR that was subject to the Privacy Breach for review and comment.

4.4.25 The HIC or HICs that received the written report under paragraph 4.4.24 shall, as soon as possible, but in any event no later than 7 days after receipt, review and provide comments to eHealth Ontario. If comments are not provided within 7 days after receipt, it will be assumed that there are no comments.

4.4.26 eHealth Ontario shall, as soon as possible, but in any event no later than 4 days after receipt of the comments under paragraph 4.4.25, advise the Breach Investigator, where eHealth Ontario is not the Breach Investigator, of any amendments to the written report that must be made or additional measures that must be taken to contain, investigate and/or remediate the Privacy Breach, if any.

4.4.27 The Breach Investigator shall, as soon as possible, but in any event no later than 7 days after receipt of the comments under paragraph 4.4.25 or 4.4.26, as the case may be, make the required amendments and implement the additional measures to contain, investigate and/or remediate the Privacy Breach in consultation with the HICs or the HICs whose agents or Electronic Service Providers caused or contributed to the Privacy Breach that are not the Breach Investigator, and prepare a revised written report.

4.4.28 Where eHealth Ontario is not the Breach Investigator, the Breach Investigator shall, as soon as possible, but in any event no later than 7 days after receipt of the comments under paragraph 4.4.26, provide the revised written report to eHealth Ontario.

4.4.29 As soon as possible, but in any event no later than 4 days after receiving or preparing the revised written report in paragraphs 4.4.27 or 4.4.28, as the case may be, eHealth Ontario shall forward the revised written report to the applicable privacy and security committee for review and approval and subsequently to the applicable oversight body for review and approval.

4.4.30 As soon as possible, but in any event no later than 4 days after the approval of the written report by the applicable oversight body, eHealth Ontario shall forward the approved written report to each HIC and each HIC whose agents or Electronic Service Providers caused or contributed to the Privacy Breach, to each HIC that created and contributed the PHI to the EHR that was subject to the Privacy Breach and to each HIC responsible for implementing measures to remediate or prevent similar Privacy Breaches in future.

4.4.31 The HIC in paragraph 4.4.8 or 4.4.9, as the case may be, as soon as possible after the receipt of the report from the eHealth Ontario under paragraph 4.4.30, shall provide the individual(s) to whom the PHI in the EHR relates with:

- A summary of the results of the investigation; and
- The measures, as is known at the time, that have been or will be implemented to remediate the Privacy Breach and to prevent similar Privacy Breaches in the future in accordance with its internal policies, procedure and practices.
4.5 Procedures Where the Privacy Breach Was Solely Caused by eHealth Ontario or by an Unauthorized Person Who Is Not an Agent of eHealth Ontario or A HIC

Determination of Whether Privacy Breach Occurred

4.5.1 Where an actual or suspected Privacy Breach was solely caused by eHealth Ontario, the agents or Electronic Service Providers of eHealth Ontario or an unauthorized person who is not an agent or Electronic Service Provider of eHealth Ontario or a HIC, eHealth Ontario shall, as soon as possible, determine whether a Privacy Breach has occurred.

Containment

4.5.2 Where eHealth Ontario has determined that a Privacy Breach has occurred, eHealth Ontario shall follow its internal policies, procedures and practices to contain the Privacy Breach and, where required, request assistance from HICs under paragraph 4.5.3 in containing the Privacy Breach.

Reporting to HICs That Created and Contributed the PHI to the EHR

4.5.3 Where eHealth Ontario has determined that a Privacy Breach has occurred, or has reasonable suspicion that a Privacy Breach has occurred, eHealth Ontario shall report the Privacy Breach to each HIC that created and contributed the PHI to the EHR as soon as possible, but in any event no later than the end of the next business day after making the determination. In reporting the Privacy Breach, eHealth Ontario shall provide as much information as is known at the time of reporting, including:

- Whether eHealth Ontario or agents or Electronic Service Providers of eHealth Ontario solely caused the Privacy Breach and the name of each agent and Electronic Service Provider of eHealth Ontario that caused the Privacy Breach, where the name is determined to be relevant by eHealth Ontario (e.g., intentional unauthorized viewing, handling or dealing with PHI);
- Whether an unauthorized person who is not an agent or Electronic Service Provider of eHealth Ontario or a HIC solely caused the Privacy Breach and the name or a description of the unauthorized person;
- Whether the PHI in the EHR that was subject to the Privacy Breach was solely created and contributed by the HIC;
- Whether the PHI in the EHR that was subject to the Privacy Breach was created and contributed by more than one HIC and the name of each HIC;
- The date and time of the Privacy Breach;
- A description of the nature and scope of the Privacy Breach;
- A description of the PHI in the EHR that was subject to the Privacy Breach;
- The individual(s) to whom the PHI in the EHR relates;
- The measures implemented to contain the Privacy Breach;
- Any assistance that the HIC is being requested to provide in containing the Privacy Breach; and
- Sufficient information to assist with the notification of the individual(s) to whom the PHI relates in accordance with PHIPA.

4.5.4 HICs shall provide assistance in containing the Privacy Breach when requested to do so by eHealth Ontario.

4.5.5 eHealth Ontario shall notify the Information and Privacy Commissioner of Ontario, in writing, of Privacy Breaches solely caused by eHealth Ontario or by agents or Electronic Service Providers of eHealth Ontario.

4.5.6 eHealth Ontario shall follow its internal policies, procedures, and practices to determine whether the Privacy Breach should be reported to any other person.

Notification of the Individual

4.5.7 Where the PHI in the EHR that was subject to the Privacy Breach was solely created and contributed by one HIC, that HIC shall follow its internal policies, procedures and practices to notify the individual(s) to whom the PHI relates at the first reasonable opportunity in accordance with PHIPA and paragraph 4.5.10.
4.5.8 Where the PHI in the EHR that was subject to the Privacy Breach was created and contributed by more than one HIC, those HICs shall, as soon as possible but in any event no later than 7 days following receipt of the information in paragraph 4.5.3, identify the HIC that will be responsible for notifying the individual(s) to whom the PHI relates in accordance with PHIPA and paragraph 4.5.10.

4.5.9 In identifying the HIC that will be responsible for notifying individual(s), regard shall be had to:
   - The HIC where the individual(s) most recently received health care; and
   - The HIC where the individual(s) received the most health care.

4.5.10 In notifying individual(s), the HIC in paragraph 4.5.7 or 4.5.8, as the case may be, shall, at a minimum, provide the individual(s) with the following information:
   - Whether eHealth Ontario or agents or Electronic Service Providers of eHealth Ontario solely caused the Privacy Breach and the name of each agent and Electronic Service Provider of eHealth Ontario that caused the Privacy Breach, where the name is determined to be relevant by eHealth Ontario (e.g., intentional unauthorized viewing, handling or dealing with PHI);
   - Whether an unauthorized person who is not an agent or Electronic Service Provider of eHealth Ontario or a HIC solely caused the Privacy Breach and the name or a description of the unauthorized person;
   - The name of each HIC that created and contributed the PHI to the EHR;
   - The date and time of the Privacy Breach;
   - A description of the nature and scope of the Privacy Breach;
   - A description of the PHI in the EHR that was subject to the Privacy Breach;
   - The measures implemented to contain the Privacy Breach;
   - The name of the Breach Investigator;
   - The HIC in paragraph 4.5.7 or 4.5.8, as the case may be, will provide the individual(s) with a summary of the results of the investigation and the measures, as is known at the time, that have been or will be implemented to remediate the Privacy Breach and to prevent similar Privacy Breaches in the future as soon as possible after the receipt of the approved written report from the eHealth Ontario under paragraph 4.5.28;
   - The steps that the individual(s) can take to protect their privacy or minimize the impact of the Privacy Breach, if applicable;
   - The name and contact information for the HIC in paragraph 4.5.7 or 4.5.8, as the case may be, to whom the individual(s) may address inquiries and concerns; and
   - Information concerning how to make a complaint to the Information and Privacy Commissioner of Ontario.

4.5.11 eHealth Ontario and other HICs shall provide assistance in notifying the individual(s) to whom the PHI relates when requested to do so by the HIC in paragraph 4.5.7 or 4.5.8, as the case may be.

Investigation

4.5.12 eHealth Ontario and the HIC or HICs that created and contributed the PHI to the EHR that was subject to the Privacy Breach shall, as soon as possible, but in any event no later than 7 days after the determination that a Privacy Breach has occurred, identify a Breach Investigator.

4.5.13 In identifying the Breach Investigator under paragraph 4.5.12, regard shall be had to:
   - Whether eHealth Ontario has the capability to investigate the Privacy Breach, and;
   - Whether a HIC would be more suitable to investigate the Privacy Breach.

4.5.14 The Breach Investigator shall, as soon as possible, but in any event no later than 7 days after the determination that a Privacy Breach has occurred, investigate the Privacy Breach in accordance with its internal policies, procedures and practices and paragraph 4.5.15.

4.5.15 In conducting the investigation, the Breach Investigator shall consult with eHealth Ontario, where eHealth Ontario is not the Breach Investigator, and shall:
   - Determine the nature, scope and cause of the Privacy Breach;
4.5.16 HICs or eHealth Ontario, where they are not the Breach Investigator, shall provide assistance in investigating the Privacy Breach when requested to do so by the Breach Investigator.

4.5.17 Status reports on the investigation shall be provided by the Breach Investigator when requested by eHealth Ontario or the HIC or HICs that created and contributed the PHI to the EHR that was the subject to the Privacy Breach, where they are not the Breach Investigator.

4.5.18 As soon as possible, but in any event no later than 7 days after completing the investigation, the Breach Investigator shall prepare a written report that, at a minimum, contains the following information:

- Whether eHealth Ontario or the agents or Electronic Service Providers of eHealth Ontario solely caused the Privacy Breach;
- The name of each agent and Electronic Service Provider of eHealth Ontario that caused the Privacy Breach, if applicable, and where the name is determined to be relevant by eHealth Ontario (e.g., intentional unauthorized viewing, handling, or dealing with PHI);
- Whether an unauthorized person who is not an agent or Electronic Service Provider of eHealth Ontario or a HIC solely caused the breach;
- The name or a description of the unauthorized person, if applicable;
- The name of each HIC that created and contributed the PHI to the EHR;
- The date and time of the Privacy Breach;
- The nature, scope and cause of the Privacy Breach;
- A description of the information in the EHR that was subject to the Privacy Breach, without disclosing any PHI;
- The persons to whom the Privacy Breach was reported under paragraphs 4.5.5 and 4.5.6;
- The measures implemented to contain the Privacy Breach;
- The nature, scope and process of the investigation of the Privacy Breach;
- The measures recommended to remediate and prevent similar Privacy Breaches in future; and
- The proposed timelines and persons responsible for implementing measures to remediate and prevent similar Privacy Breaches in future.

4.5.19 As soon as possible, but in any event no later than 4 days after the completion of the written report in paragraph 4.5.18, the Breach Investigator shall provide the written report to eHealth Ontario, where eHealth Ontario is not the Breach Investigator, for review and comment.

4.5.20 Where eHealth Ontario is not the Breach Investigator, eHealth Ontario shall, as soon as possible, but in any event no later than 7 days after receipt of the written report under paragraph 4.5.19, review and provide comments to the Breach Investigator. If comments are not provided within 7 days after receipt, it will be assumed that there are no comments.

4.5.21 Where eHealth Ontario is not the Breach Investigator, the Breach Investigator shall, as soon as possible, but in any event no later than 7 days after receipt of the comments under paragraph 4.5.20, make the required amendments and provide the written report to eHealth Ontario.

4.5.22 As soon as possible, but in any event no later than 7 days after receiving or preparing the written report in paragraphs 4.5.18 or 4.5.21, as the case may be, eHealth Ontario shall forward the written report to the HIC or HICs that created and contributed the PHI to the EHR that was subject to the Privacy Breach for review and comment.
4.5.23 The HIC or HICs that received the written report under paragraph 4.5.22 shall, as soon as possible, but in any event no later than 7 days after receipt, review and provide comments to eHealth Ontario. If comments are not provided within 7 days after receipt, it will be assumed that there are no comments.

4.5.24 eHealth Ontario shall, as soon as possible, but in any event no later than 4 days after receipt of the comments under paragraph 4.5.23, advise the Breach Investigator, where eHealth Ontario is not the Breach Investigator, of any amendments to the written report that must be made or additional measures that must be taken to contain, investigate and/or remediate the Privacy Breach, if any.

4.5.25 The Breach Investigator shall, as soon as possible, but in any event no later than 7 days after receipt of the comments under paragraph 4.5.23 or 4.5.24, as the case may be, make the required amendments and implement the additional measures to contain, investigate and/or remediate the Privacy Breach in consultation with eHealth Ontario, where eHealth Ontario is not the Breach Investigator, and prepare a revised written report.

4.5.26 Where eHealth Ontario is not the Breach Investigator, the Breach Investigator shall, as soon as possible, but in any event no later than 7 days after receipt of the comments under paragraph 4.5.24, provide a revised written report to eHealth Ontario.

4.5.27 As soon as possible, but in any event no later than 4 days after receiving or preparing the revised written report in paragraphs 4.5.25 or 4.5.26, as the case may be, eHealth Ontario shall forward the revised written report to the applicable privacy and security committee for review and approval and subsequently to the applicable oversight body for review and approval.

4.5.28 As soon as possible, but in any event no later than 4 days after the approval of the written report by the applicable oversight body, eHealth Ontario shall forward the approved written report to each HIC that created and contributed the PHI to the EHR that was subject to the Privacy Breach and to each HIC responsible for implementing measures to remediate or prevent similar Privacy Breaches in future.

4.5.29 The HIC in paragraph 4.5.7 or 4.5.8, as the case may be, as soon as possible after the receipt of the report from the eHealth Ontario under paragraph 4.5.28, shall provide the individual(s) to whom the PHI in the EHR relates with:

- A summary of the results of the investigation; and
- The measures, as is known at the time, that have been or will be implemented to remediate the Privacy Breach and to prevent similar Privacy Breaches in the future in accordance with its internal policies, procedure and practices.

4.6 Procedures Related to Remediation of Privacy Breaches

4.6.1 eHealth Ontario and HICs shall implement measures identified in the written report approved by the applicable oversight body to remediate and prevent similar Privacy Breaches in future.

4.6.2 Each HIC responsible for implementing measures to remediate or prevent similar Privacy Breaches in future shall, every 30 days, until all the measures for which the HIC is responsible have been implemented, provide a written report to eHealth Ontario setting out:

- The measures that the HIC is responsible for implementing and the timeline for implementation of each measure as identified in the written report approved by the applicable oversight body;
- The status of and the date or target date for implementation of each measure; and
- The manner in which each measure was or is expected to be implemented.

4.6.3 Each agent or Electronic Service Provider of the HIC or eHealth Ontario that caused the Privacy Breach by having collected, used or disclosed or having viewed, handled or otherwise dealt with PHI in an unauthorized manner, may be subject to additional auditing in accordance with the Electronic Health Record Logging and Auditing Policy and its associated procedures, as amended from time to time.

4.7 Procedures Related to Maintenance of Privacy Breach Logs

4.7.1 eHealth Ontario shall keep a log of all Privacy Breaches which shall include, for each Privacy Breach:

- If applicable, the name of each HIC or each HIC whose agents or Electronic Service Providers caused or contributed to the Privacy Breach and the name of each agent and Electronic Service Provider of the HIC that caused or contributed to the Privacy Breach, where the name has been determined to be relevant in accordance with this policy and its associated procedures;
• If applicable, that eHealth Ontario or the agents or Electronic Service Providers of eHealth Ontario solely caused the Privacy Breach and the name of each agent and Electronic Service Provider of eHealth Ontario that caused the Privacy Breach, where the name has been determined to be relevant in accordance with this policy and its associated procedures;

• If applicable, that an unauthorized person who is not an agent or Electronic Service Provider of eHealth Ontario or a HIC solely caused the Privacy Breach and the name or a description of the unauthorized person;

• The name of each HIC that created and contributed the PHI to the EHR;

• The date and time of the Privacy Breach;

• The nature, scope and cause of the Privacy Breach;

• A description of the information in the EHR that was subject to the Privacy Breach, without disclosing any PHI;

• The measures implemented to contain the Privacy Breach;

• The measures that have been or will be implemented to remediate and prevent similar Privacy Breaches in future;

• The timelines and persons responsible for implementing measures to remediate and prevent similar Privacy Breaches in future;

• The status of implementation of measures to remediate and prevent similar Privacy Breaches in future and the date or target date for implementation; and

• The manner in which each measure was or is expected to be implemented.

4.7.2 eHealth Ontario shall audit and monitor the log in paragraph 4.7.1 to:

• Identify patterns or trends in Privacy Breaches;

• Identify administrative, physical or technical safeguards that must be implemented to prevent or minimize the risk of Privacy Breaches; and

• Ensure that measures to remediate and prevent similar Privacy Breaches in future are implemented.

4.7.3 eHealth Ontario shall, every 30 days, forward a written report on the status of implementation of measures to remediate and prevent similar Privacy Breaches in future to each HIC and each HIC whose agents or Electronic Service Providers caused or contributed to the Privacy Breach, to each HIC that created and contributed the PHI to the EHR that was subject to the Privacy Breach and to each HIC responsible for implementing measures to remediate or prevent similar Privacy Breaches in future.

4.7.4 eHealth Ontario shall provide a written report on the status of implementation of measures to remediate and prevent similar Privacy Breaches in future at every meeting of the applicable privacy and security committee and applicable oversight body, or more frequently upon request of the applicable privacy and security committee and applicable oversight body.

4.7.5 At a minimum, the written report in paragraphs 4.7.3 and 4.7.4 shall set out:

• The measures that eHealth Ontario and/or HICs are responsible for implementing and the timeline for implementation of each measure as identified in the written report approved by the applicable oversight body;

• The status of and the date or target date for implementation of each measure; and

• The manner in which each measure was or is expected to be implemented.
5 Enforcement

5.1.1 All instances of non-compliance by agents or Electronic Service Providers of a HIC will be reviewed by that HIC and all instances of non-compliance by agents or Electronic Service Providers of eHealth Ontario will be reviewed by eHealth Ontario. The HIC or eHealth Ontario as the case may be, will impose appropriate penalties upon the agent or Electronic Service Provider and require the implementation of remedial action in accordance with its internal policies, procedures and practices.

5.1.2 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 applicable oversight body.

5.1.3 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.

Breach Investigator
A HIC or eHealth Ontario who is chosen to lead an investigation into the Privacy Breach by eHealth Ontario, the HIC or HICs that created and contributed the PHI to the EHR that was subject to the Privacy Breach and the HIC or HICs who caused or whose agents or Electronic Service Providers caused the Privacy Breach, as the case may be.

Applicable Agreements
The agreements entered into by the HIC, 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 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
A privacy breach includes circumstances where:
- A provision of PHIPA or its regulations has been contravened;
- The privacy provisions of the applicable agreements in respect of the EHR have been contravened;
- The privacy policies, procedures and practices implemented in respect of the EHR have been contravened;
- PHI in the EHR is lost or stolen or has been accessed by an unauthorized person; or
- Records of PHI in the EHR have been copied, modified or disposed of in an unauthorized manner.

3 References to the applicable privacy and security committee and the applicable oversight body can be found in Table 1: Applicable Governance Bodies.
<table>
<thead>
<tr>
<th>Policy Governance Structure</th>
<th>ConnectingOntario Solution</th>
<th>Diagnostic Imaging Common Services Repository</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applicable Oversight Body</td>
<td>Privacy: ConnectingOntario Committee Security: eHealth Ontario Strategy Committee</td>
<td>Privacy: Diagnostic Imaging Common Services Executive Committee Security: eHealth Ontario Strategy Committee</td>
</tr>
</tbody>
</table>

Table 1: Applicable Governance Bodies

<table>
<thead>
<tr>
<th>Term or Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>HIC</td>
<td>Health Information Custodian</td>
</tr>
<tr>
<td>PHI</td>
<td>Personal Health Information, as defined in the <em>Personal Health Information Protection Act, 2004</em></td>
</tr>
<tr>
<td>PHIPA</td>
<td><em>Personal Health Information Protection Act, 2004</em></td>
</tr>
<tr>
<td>SDM</td>
<td>Substitute Decision-Maker</td>
</tr>
</tbody>
</table>

7 References and Associated Documents

*Personal Health Information Protection Act, 2004 (PHIPA)*
Information and Privacy Commissioner of Ontario: What to do when Faced with a Privacy Breach: Guidelines for the Health Sector
*Electronic Health Record Inquires and Complaints Policy* and its associated procedures
*Electronic Health Record Logging and Auditing Policy* and its associated procedures
*Electronic Health Record Privacy and Security Training Policy* and its associated procedures
Copyright Notice
Copyright © 2017, eHealth Ontario

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 eHealth Ontario. The information contained in this document is proprietary to eHealth Ontario and may not be used or disclosed except as expressly authorized in writing by eHealth Ontario.

Trademarks
Other product names mentioned in this document may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.
Document Control
The electronic version of this document is recognized as the only valid version.

Approval History

<table>
<thead>
<tr>
<th>APPROVER(S)</th>
<th>APPROVED DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>ConnectingPrivacy Committee Members</td>
<td>December 8, 2016</td>
</tr>
</tbody>
</table>

Revision History

<table>
<thead>
<tr>
<th>VERSION NO.</th>
<th>DATE</th>
<th>SUMMARY OF CHANGE</th>
<th>CHANGED BY</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.0</td>
<td>2016-12-01</td>
<td>Revisions as per CPC Policy Evaluation</td>
<td>Rand Muhtam, Privacy Analyst, eHealth Ontario</td>
</tr>
<tr>
<td>1.1</td>
<td>2015-11-25</td>
<td>Minor revisions – updated for ConnectingOntario</td>
<td>Samara Strub, Privacy Analyst, eHealth Ontario</td>
</tr>
<tr>
<td>1.0</td>
<td>2015-06-10</td>
<td>Final version</td>
<td>Promila Gonsalves, Senior Privacy Business Analyst, eHealth Ontario</td>
</tr>
<tr>
<td>0.01</td>
<td>2015-03-05</td>
<td>Initial draft based on ConnectingPrivacy Committee Harmonized Retention Policy v1.0.</td>
<td>Promila Gonsalves, Senior Privacy Business Analyst, eHealth Ontario</td>
</tr>
</tbody>
</table>
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Purpose/ Objective</td>
<td>1</td>
</tr>
<tr>
<td>2 Scope</td>
<td>1</td>
</tr>
<tr>
<td>3 Policy</td>
<td>1</td>
</tr>
<tr>
<td>3.1 Guiding Policies and Principles</td>
<td></td>
</tr>
<tr>
<td>4 Procedure</td>
<td>2</td>
</tr>
<tr>
<td>4.1 Procedures Related to Retention of Records</td>
<td>2</td>
</tr>
<tr>
<td>4.2 Procedures Related to the Secure Disposal of Records</td>
<td>2</td>
</tr>
<tr>
<td>4.3 Retention Schedule</td>
<td>3</td>
</tr>
<tr>
<td>5 Enforcement</td>
<td>4</td>
</tr>
<tr>
<td>6 Glossary and Terms</td>
<td>4</td>
</tr>
<tr>
<td>7 References and Associated Documents</td>
<td>5</td>
</tr>
<tr>
<td>8 Appendix A</td>
<td>6</td>
</tr>
</tbody>
</table>
1 Purpose/Objective

To define the policies and procedures that apply in retaining records in respect of the Electronic Health Record (EHR).

2 Scope

This policy and its associated procedures apply to retention of the following records in respect of the EHR:

- Personal Health Information (PHI)
- Personal Information collected to support Provider Registry (PI)
- Audit logs and audit reports that contain PHI/PI;
- Information collected about an individual to respond to:
  - Requests for Access or Requests for Correction under the Personal Health Information Protection Act, 2004 (PHIPA);
  - Requests to make, modify, or withdraw a Consent Directive under PHIPA; and
  - Inquiries or Complaints under PHIPA.
- Information created about an individual as part of an investigation of Privacy Breaches and/or Security Incidents;
- System-level logs, tracking logs, reports and related documents for privacy and security tasks that do not contain PHI/PI;
- Corporate documents collected or created by eHealth Ontario, including:
  - Templates or resources developed by eHealth Ontario in respect of the EHR;
  - Assurance-related documents; and
  - eHealth Ontario business documents.

This policy and its associated procedures do not apply to copies of records of PHI/PI that have been made from the EHR and retained by the HIC, or by the agents or Electronic Service Providers of the HIC, other than eHealth Ontario and its agents or Electronic Service Providers.

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.

3 Policy

3.1 Guiding Policies and Principles

3.1.1 PHIPA requires a HIC to ensure that the records of PHI that it has in its custody or under its control are retained, transferred and disposed of in a secure manner and in accordance with any requirements under PHIPA.

3.1.2 PHIPA requires that a HIC retain records of PHI subject to a request for access under section 53 for as long as necessary to allow the individual to exhaust any recourse under PHIPA that he or she may have with respect to the request.

---

1 Variance in policy and procedure requirements between the ConnectingOntario Solution and the Diagnostic Imaging Common Services Repository is highlighted within the policy.
3.1.3 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, the Freedom of Information and Protection of Privacy Act, 1990 (FIPPA) or the Municipal Freedom of Information and Protection of Privacy Act, 1990 (mFIPPA) where applicable, 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 FIPPA/mFIPPA, where applicable, and inform their agents and Electronic Service Providers on the policies, procedures and practices as required by PHIPA and FIPPA/mFIPPA, where applicable.

3.1.5 eHealth Ontario shall have a program in place to enable eHealth Ontario and HICs to satisfy their obligations in retaining records of PHI/PI in accordance with PHIPA, FIPPA/mFIPPA where applicable, applicable agreements and this policy and its associated procedures.

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

3.1.7 HICs and eHealth Ontario shall maintain records in respect of the EHR in accordance with all applicable legal statutes, professional regulations, generally accepted industry practices, this policy and its associated procedures, and its internal policies, procedures, and practices.

4 Procedure

4.1 Procedures Related toRetention of Records

4.1.1 eHealth Ontario and HICs shall ensure the records identified in section 4.3 are retained for the time period specified in section 4.3. Records can be stored in various methods as long as they are retained in a secure manner and are retrievable in the time required.

4.1.2 eHealth Ontario and HICs shall ensure the information not identified in section 4.3 is retained as long as the information is required in respect of the EHR.

4.1.3 HICs and eHealth Ontario, and their agents and Electronic Service Providers, shall take steps that are reasonable in the circumstances to ensure records are protected against theft, loss and unauthorized use or disclosure and to ensure that the records are protected against unauthorized copying, modification or disposal at rest and during transit by adhering to Electronic Health Record Connecting Security Committee Harmonized Information Security Policy, Information and Asset Management Policy and its associated policies and procedures, as amended from time to time.

Additional Procedures Related to Retaining PHI/PI

4.1.4 eHealth Ontario shall ensure that the EHR is capable of retaining records of PHI/PI for as long as required as outlined in section 4.3.

4.1.5 At the end of the retention schedule in section 4.3, PHI/PI will no longer be made available by the EHR to HICs or eHealth Ontario, or their agents or Electronic Service Providers.

4.1.6 Despite paragraph 4.1.4, where the relationship between eHealth Ontario and the HIC that created and contributed the PHI/PI to the EHR is terminated, the applicable privacy and security committee will work with the HIC that created and contributed the PHI to the EHR to address the disposition of the PHI/PI created and contributed by the HIC to the EHR in a manner that complies with PHIPA, applicable agreements, this policy and its associated policies and procedures, as amended from time to time.

4.1.7 Where the PHI/PI in the EHR described in 4.1.6 has been collected by a HIC other than the one that created and contributed the PHI/PI, the PHI/PI will be retained in the EHR for the time period specified in section 4.3 and will be subject to further collection, use and disclosure by HICs and eHealth Ontario, and their agents and Electronic Service Providers.

4.1.8 Where the PHI/PI in the EHR described in 4.1.6 has not been collected by a HIC other than the one that created and contributed the PHI/PI, the PHI/PI will be retained in the EHR for the time period specified in section 4.3 however will be made unavailable and will not be collected, used or disclosed by HICs and eHealth Ontario, and their agents and Electronic Service Providers.

4.2 Procedures Related to the Secure Disposal of Records

4.2.1 HICs and eHealth Ontario, and their agents and Electronic Service Providers, shall ensure that records are disposed of in a secure manner that the reconstruction of the records is not reasonably foreseeable in the circumstance in accordance with the policies and procedures established in Electronic Health Record Connecting Security Committee Harmonized Information Security Policy and its associated policies and procedures, as amended from time to time.
### 4.3 Retention Schedule

eHealth Ontario, and HICs where applicable, shall retain records containing the information described in the chart below for the time set out in the chart below:

<table>
<thead>
<tr>
<th>Information Type</th>
<th>Retention Period</th>
</tr>
</thead>
</table>
| PHI in the EHR   | The longer of the following time periods:  
|                  | • as long as the HIC that created and contributed the PHI to the EHR retains the PHI in its local systems;  
|                  | • in accordance with the retention schedule of the HIC that created and contributed the PHI to the EHR; or  
|                  | • 30 years after the most recent instance of PHI being viewed, handled, or otherwise dealt with for the purpose of providing or assisting in the provision of health care; or 10 years after the patient has expired and in accordance with any applicable court order or court action or other legal requirement. |
| Audit logs and audit reports that contain PHI:  
| • Created and maintained for compliance purposes | The longer of 30 years or when PHI is removed from the EHR.  
| • Created and maintained for troubleshooting | Retain audit logs and audit reports that contain PHI created and maintained for troubleshooting and other operational purposes only as long as needed but no longer than 60 days unless expressly authorized by appropriate by eHealth Ontario CPO or authorized delegate to retain longer.  
| Archival copies of:  
| o The PHI in the EHR; and  
| o Audit logs and audit reports containing PHI. | Equals the retention period of the PHI in the EHR or the audit logs and audit reports respectively. |
| Backups of:  
| o The PHI in the EHR; and  
| o Audit logs and audit reports containing PHI. | Securely destroyed according to the schedule of the Electronic Service Provider, but retained no longer than 2 years. |
| Information collected to respond to individuals related to their:  
| o Request for Access or Request for Correction under PHIPA;  
| o Request to make, modify, or withdraw a Consent Directive under PHIPA; or  
| o Inquiries or Complaints under PHIPA. | 2 years after the Request for Access, Request for Correction, requests to make, modify, or withdraw a Consent Directive, or an Inquiry has been closed.  
| Information created about an individual as part of an investigation of Privacy Breaches and/or Security Incidents. | In the case of Complaints, 2 years after the Complaint has been closed by the HIC, eHealth Ontario or the Information and Privacy Commissioner of Ontario, whichever is longer. |
| Information collected for identity provider identification or registration that contains PI | 2 years after the Privacy Breach has been closed by the HIC, eHealth Ontario or the Information and Privacy Commissioner of Ontario, whichever is longer. |
| End User Credential Information where HIC is an Identity Provider | 7 years after last use |
| System-level logs, tracking logs, reports and related documents for privacy and security tasks that do not contain PHI | Permanent |
| Authentication Events where HIC is an Identity Provider | For a minimum of 2 years |
| | 60 days online, 24 months total in archive |

* Detail on the Information Types can be found in Appendix A.
<table>
<thead>
<tr>
<th>Information Type</th>
<th>Retention Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>Templates or resources developed by eHealth Ontario in respect of the EHR;</td>
<td>For a minimum of 2 years</td>
</tr>
<tr>
<td>Assurance-related documents</td>
<td>10 years</td>
</tr>
<tr>
<td>eHealth Ontario business documentation</td>
<td>For a minimum of 7 years</td>
</tr>
</tbody>
</table>

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 applicable oversight body.

5.1.2 The applicable oversight body has the authority 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.

**Complaint**
Complaint has the same meaning as in the Electronic Health Record Inquiries and Complaints Policy and its associated procedures, as amended from time to time.

**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.

**Inquiry**
Inquiry has the same meaning as in the Electronic Health Record Inquiries and Complaints Policy and its associated procedures, as amended from time to time.

**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.

**Request for Access**
Request for Access has the same meaning as in the Electronic Health Record Access and Correction Policy and its associated procedures, as amended from time to time.

**Request for Correction**
Request for Correction has the same meaning as in the Electronic Health Record Access and Correction Policy and its associated procedures, as amended from time to time.

---

3 References to the applicable privacy and security committee and the applicable oversight body can be found in Table 1: Applicable Governance Bodies.
Policy Governance Structure | ConnectingOntario Solution | Diagnostic Imaging Common Services Repository
--- | --- | ---
**Applicable Privacy and Security Committee** | Privacy: Connecting Privacy Committee | Privacy: Diagnostic Imaging Common Services Privacy and Security Working Group
Security: Connecting Security Committee | Security: Connecting Security Committee

**Applicable Oversight Body** | Privacy: ConnectingOntarioCommittee | Privacy: Diagnostic Imaging Common Services Executive Committee
Security: eHealth Ontario Strategy Committee | Security: eHealth Ontario Strategy Committee

Table 1: Applicable Governance Bodies

<table>
<thead>
<tr>
<th>Term or Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>FIPPA</td>
<td>Freedom of Information and Protection of Privacy Act, 1990</td>
</tr>
<tr>
<td>HIC</td>
<td>Health Information Custodian</td>
</tr>
<tr>
<td>mFIPPA</td>
<td>Municipal Freedom of Information and Protection of Privacy Act, 1990</td>
</tr>
<tr>
<td>PHI</td>
<td>Personal Health Information, as defined in the Personal Health Information Protection Act, 2004</td>
</tr>
<tr>
<td>PHIPA</td>
<td>Personal Health Information Protection Act, 2004</td>
</tr>
</tbody>
</table>

7 References and Associated Documents

*Personal Health Information Protection Act, 2004 (PHIPA)*
*Freedom of Information and Protection of Privacy Act, 1990 (FIPPA)*
*Municipal Freedom of Information and Protection of Privacy Act, 1990 (mFIPPA)*
*Electronic Health Record Connecting Security Committee Harmonized Information Security Policy and its associated procedures*
*Electronic Health Record Connecting Security Committee Harmonized Information and Asset Management Policy and its associated procedures*
*Electronic Health Record Inquiries and Complaints Policy and its associated procedures*
*Electronic Health Record Consent Management Policy and its associated procedures*
*Electronic Health Record Privacy Breach Management Policy and its associated procedures*
*Electronic Health Record Access and Correction Policy and its associated procedures*
## 8 Appendix A

<table>
<thead>
<tr>
<th>Information Type</th>
<th>Responsible</th>
</tr>
</thead>
<tbody>
<tr>
<td>PHI in the EHR</td>
<td>eHealth Ontario</td>
</tr>
<tr>
<td>Audit logs or audit reports that contain PHI</td>
<td>eHealth Ontario</td>
</tr>
<tr>
<td>Log of instances where all or part of the PHI in the EHR is viewed, handled or</td>
<td>eHealth Ontario</td>
</tr>
<tr>
<td>otherwise dealt with</td>
<td></td>
</tr>
<tr>
<td>Log of instances where all or part of the PHI in the EHR is transferred to a HIC</td>
<td>eHealth Ontario</td>
</tr>
<tr>
<td>Instances where all or part of the PHI in the EHR is disclosed to and collected</td>
<td>eHealth Ontario</td>
</tr>
<tr>
<td>by a HIC as a result of an override of a Consent Directive</td>
<td></td>
</tr>
<tr>
<td>Instances where a Consent Directive is made, withdrawn or modified in the EHR</td>
<td>eHealth Ontario</td>
</tr>
<tr>
<td>Notices related to Logging and Auditing</td>
<td>eHealth Ontario</td>
</tr>
<tr>
<td>Report to IPC of every instance where all or part of the PHI in the EHR is</td>
<td>eHealth Ontario</td>
</tr>
<tr>
<td>disclosed to and collected by a HIC as a result of an override of a Consent</td>
<td></td>
</tr>
<tr>
<td>Directive</td>
<td></td>
</tr>
<tr>
<td>Auditing and Monitoring Reports</td>
<td>HIC &amp; eHealth Ontario</td>
</tr>
<tr>
<td>Archival copies of:</td>
<td></td>
</tr>
<tr>
<td>PHI in the EHR; and</td>
<td>eHealth Ontario</td>
</tr>
<tr>
<td>Audit logs or audit reports that contain PHI</td>
<td></td>
</tr>
<tr>
<td>Backups of PHI in the EHR and audit logs or audit reports that contain PHI</td>
<td>eHealth Ontario</td>
</tr>
<tr>
<td>Information collected to respond to individuals related to their:</td>
<td></td>
</tr>
<tr>
<td>Requests for Access or Requests for Correction under the PHIPA;</td>
<td></td>
</tr>
<tr>
<td>Requests to make, modify, or withdraw a Consent Directive under PHIPA; and</td>
<td></td>
</tr>
<tr>
<td>Inquiries or Complaints under PHIPA.</td>
<td></td>
</tr>
<tr>
<td>Information created about an individual to respond to Request for Access, Request</td>
<td>eHealth Ontario or HIC who is accountable for</td>
</tr>
<tr>
<td>Correction, request to make, modify, or withdraw a Consent Directive, Inquiries</td>
<td>producing the record</td>
</tr>
<tr>
<td>or Complaints under PHIPA.</td>
<td></td>
</tr>
<tr>
<td>Copy of notices provided to individuals for Consent Directives</td>
<td></td>
</tr>
<tr>
<td>Notices related to Requests for Consent Directives</td>
<td></td>
</tr>
<tr>
<td>Requests for Access form (including identification and contact information)</td>
<td></td>
</tr>
<tr>
<td>Notices and Responses related to Requests for Access (including the fee estimate)</td>
<td></td>
</tr>
<tr>
<td>Request for Correction (including identification and contact information)</td>
<td></td>
</tr>
<tr>
<td>Notices and responses related to Requests for Correction (including the statement</td>
<td></td>
</tr>
<tr>
<td>of disagreement)</td>
<td></td>
</tr>
<tr>
<td>Documented Complaints and Inquiries (including contact information)</td>
<td></td>
</tr>
<tr>
<td>Notices and Copies of response to Complaints and Inquiries</td>
<td></td>
</tr>
<tr>
<td>Information created about an individual as part of an investigation of Privacy</td>
<td>eHealth Ontario</td>
</tr>
<tr>
<td>Breaches and/or Security Incidents</td>
<td>or HIC responsible for managing the incident</td>
</tr>
<tr>
<td>System-level logs of the EHR, tracking logs, reports and related documents for</td>
<td>eHealth Ontario</td>
</tr>
<tr>
<td>privacy and security tasks that do not contain PHI</td>
<td></td>
</tr>
<tr>
<td>System Troubleshooting Logs</td>
<td>eHealth Ontario</td>
</tr>
<tr>
<td>Log of all system-level access to EHR</td>
<td>eHealth Ontario</td>
</tr>
<tr>
<td>Log of information system events on the EHR</td>
<td>eHealth Ontario</td>
</tr>
<tr>
<td>Log of all access by the HIC, their agents or Electronic Service Providers to</td>
<td>HIC</td>
</tr>
<tr>
<td>EHR</td>
<td></td>
</tr>
<tr>
<td>Log all information system events on their identity provider services and data</td>
<td>HIC &amp; eHealth Ontario</td>
</tr>
<tr>
<td>contribution endpoints</td>
<td></td>
</tr>
<tr>
<td>Information Type</td>
<td>Responsible</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>Log of all information security exception requests</td>
<td>eHealth Ontario</td>
</tr>
<tr>
<td>Log of all activities of administrators and operators on their identity provider services and their data contribution endpoints</td>
<td>HIC</td>
</tr>
<tr>
<td>Log of all information system events found in the <em>Harmonized Security Logging and Monitoring Policy</em> Appendix A performed by the HIC, their agents or Electronic Service Providers</td>
<td>eHealth Ontario</td>
</tr>
<tr>
<td>Log of all activities of their information system administrators and information system operators</td>
<td>eHealth Ontario</td>
</tr>
<tr>
<td>List of all agents or Electronic Service Providers who have authorized access to identity provider technology and data contribution endpoints logs</td>
<td>HIC</td>
</tr>
<tr>
<td>List of all agents or Electronic Service Providers who have authorized access to logs</td>
<td>eHealth Ontario</td>
</tr>
<tr>
<td>Log of the destruction of the PHI in the EHR</td>
<td>eHealth Ontario</td>
</tr>
<tr>
<td>List of distribution of copies of paper material classified as Restricted</td>
<td>eHealth Ontario</td>
</tr>
<tr>
<td>List of vulnerability and configuration scanning tools which are approved by eHealth Ontario</td>
<td>eHealth Ontario</td>
</tr>
<tr>
<td>Logs of any instance in which keys, key components, or related materials for their identity provider services and data contribution endpoints are generated, removed from storage or loaded to a cryptographic device</td>
<td>HIC &amp; eHealth Ontario</td>
</tr>
<tr>
<td>Log of all requests for user IDs that they administer and will have access to the identity provider services and data contribution end point infrastructure connected to EHR</td>
<td>HIC</td>
</tr>
<tr>
<td>Log of all requests for IDs that they manage and that could be used to access EHR</td>
<td>eHealth Ontario</td>
</tr>
<tr>
<td>List of all IDs that have access to [the EHR Solution]</td>
<td>eHealth Ontario</td>
</tr>
<tr>
<td>Log of requests to make, modify or withdraw a Consent Directive (including identification and contact information)</td>
<td>HIC &amp; eHealth Ontario</td>
</tr>
<tr>
<td>Log of receipt of a request for Consent Directive</td>
<td>HIC &amp; eHealth Ontario</td>
</tr>
<tr>
<td>Log of notices provided to individuals for Consent Directives</td>
<td>HIC &amp; eHealth Ontario</td>
</tr>
<tr>
<td>List of all agents who are the subject of an Agent Consent Directive</td>
<td>eHealth Ontario</td>
</tr>
<tr>
<td>Logs related to responses to Requests for Access</td>
<td>HIC &amp; eHealth Ontario</td>
</tr>
<tr>
<td>Logs related to responses to Requests for Correction</td>
<td>HIC &amp; eHealth Ontario</td>
</tr>
<tr>
<td>History of all Corrections of records of PHI in the EHR</td>
<td>eHealth Ontario</td>
</tr>
<tr>
<td>Notices and reports of privacy breaches/ security incidents</td>
<td>eHealth Ontario</td>
</tr>
<tr>
<td>Privacy Breach Management Investigation Report/ Security Incident Reports</td>
<td>eHealth Ontario</td>
</tr>
<tr>
<td>Log of Privacy Breaches</td>
<td>eHealth Ontario</td>
</tr>
<tr>
<td>Log of Security Incidents</td>
<td>HIC</td>
</tr>
<tr>
<td>Privacy Breach Management Remediation Report</td>
<td>eHealth Ontario</td>
</tr>
<tr>
<td>Status of Privacy Breach Management Remediation Report</td>
<td>eHealth Ontario</td>
</tr>
<tr>
<td>Documented Inquiries (including contact information)</td>
<td>eHealth Ontario</td>
</tr>
<tr>
<td>Log of receipt of Inquiries</td>
<td>eHealth Ontario</td>
</tr>
<tr>
<td>Copy of response or log of responses to Inquiries</td>
<td>HIC &amp; eHealth Ontario</td>
</tr>
<tr>
<td>Log of receipt of Complaints</td>
<td>eHealth Ontario</td>
</tr>
<tr>
<td>Resources developed by eHealth Ontario in respect of the EHR</td>
<td>Privacy and Security Training Template</td>
</tr>
<tr>
<td></td>
<td>Notice for Obtaining Consent Template</td>
</tr>
<tr>
<td>Assurance-related documents</td>
<td>Privacy Impact Assessment Recommendation Report and associated decisions and directions</td>
</tr>
<tr>
<td></td>
<td>Privacy Impact Assessment and associated decisions and directions</td>
</tr>
<tr>
<td></td>
<td>Threat and Risk Assessment (including TRA summaries)</td>
</tr>
</tbody>
</table>

---

EHR Retention Policy / Doc ID: 4033 / Version No. 2.0
<table>
<thead>
<tr>
<th>Information Type</th>
<th>Responsible</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy and Security Readiness Self-Assessment and associated decisions and directions</td>
<td>HIC &amp; eHealth Ontario</td>
</tr>
<tr>
<td>Privacy and Security Operational Self- Attestation and associated decisions and directions</td>
<td>HIC &amp; eHealth Ontario</td>
</tr>
<tr>
<td>Remediation Plans and associated decisions and directions</td>
<td>eHealth Ontario</td>
</tr>
<tr>
<td>Status of Remediation Implementation Report</td>
<td>eHealth Ontario</td>
</tr>
<tr>
<td>Remediation Attestation</td>
<td>HIC &amp; eHealth Ontario</td>
</tr>
<tr>
<td>Non-Compliance Reports and associated recommendations</td>
<td>HIC &amp; eHealth Ontario</td>
</tr>
<tr>
<td>Compliance Monitoring Reports</td>
<td>HIC &amp; eHealth Ontario</td>
</tr>
<tr>
<td>Audit Reports and associated recommendations and decisions and directions</td>
<td>HIC &amp; eHealth Ontario</td>
</tr>
<tr>
<td>Asset Listing for the EHR</td>
<td>eHealth Ontario</td>
</tr>
<tr>
<td>Risk Listing of threat and vulnerability ratings for EHR</td>
<td>eHealth Ontario</td>
</tr>
<tr>
<td>End User Agreement Template</td>
<td>eHealth Ontario</td>
</tr>
<tr>
<td>Business Continuity Plan</td>
<td>HIC &amp; eHealth Ontario</td>
</tr>
<tr>
<td>eHealth Ontario Business Documentation</td>
<td></td>
</tr>
<tr>
<td>Applicable privacy and security committee Meeting Minutes</td>
<td>eHealth Ontario</td>
</tr>
</tbody>
</table>