

***eHealth Ontario***

# Retention Policy

Electronic Health Record

Version: 2.0

Document ID: 4033

## **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

APPROVER(S)	APPROVED DATE
ConnectingPrivacy Committee Members	December 8, 2016

## Revision History

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

# Contents

---

- 1 Purpose/ Objective 1**
- 2 Scope 1**
- 3 Policy 1**
  - 3.1 Guiding Policies and Principles .....1
- 4 Procedure 2**
  - 4.1 Procedures Related to Retention of Records .....2
  - 4.2 Procedures Related to the Secure Disposal of Records .....2
  - 4.3 Retention Schedule .....3
- 5 Enforcement 4**
- 6 Glossary and Terms 4**
- 7 References and Associated Documents 5**
- 8 Appendix A 6**

# 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<sup>1</sup>.

## 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.

---

<sup>1</sup> 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 to Retention 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:

Information Type <sup>2</sup>	Retention Period
PHI in the EHR	<p>The longer of the following time periods:</p> <ul style="list-style-type: none"> <li>• as long as the HIC that created and contributed the PHI to the EHR retains the PHI in its local systems;</li> <li>• in accordance with the retention schedule of the HIC that created and contributed the PHI to the EHR; or</li> <li>• 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.</li> </ul>
<p>Audit logs and audit reports that contain PHI:</p> <ul style="list-style-type: none"> <li>• Created and maintained for compliance purposes</li> <li>• Created and maintained for troubleshooting</li> </ul>	<p>The longer of 30 years or when PHI is removed from the EHR.</p> <p>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.</p>
<p>Archival copies of:</p> <ul style="list-style-type: none"> <li>○ The PHI in the EHR; and</li> <li>○ Audit logs and audit reports containing PHI.</li> </ul>	<p>Equals the retention period of the PHI in the EHR or the audit logs and audit reports respectively.</p>
<p>Backups of:</p> <ul style="list-style-type: none"> <li>○ The PHI in the EHR; and</li> <li>○ Audit logs and audit reports containing PHI.</li> </ul>	<p>Securely destroyed according to the schedule of the Electronic Service Provider, but retained no longer than 2 years.</p>
<p>Information collected to respond to individuals related to their:</p> <ul style="list-style-type: none"> <li>○ Request for Access or Request for Correction under PHIPA;</li> <li>○ Request to make, modify, or withdraw a Consent Directive under PHIPA; or</li> <li>○ Inquiries or Complaints under PHIPA.</li> </ul>	<p>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.</p> <p>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.</p>
<p>Information created about an individual as part of an investigation of Privacy Breaches and/or Security Incidents.</p>	<p>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.</p>
<p>Information collected for identity provider identification or registration that contains PI</p>	<p>7 years after last use</p>
<p>End User Credential Information where HIC is an Identity Provider</p>	<p>Permanent</p>
<p>System-level logs, tracking logs, reports and related documents for privacy and security tasks that do not contain PHI</p>	<p>For a minimum of 2 years</p>
<p>Authentication Events where HIC is an Identity Provider</p>	<p>60 days online, 24 months total in archive</p>

<sup>2</sup> Detail on the Information Types can be found in Appendix A.

Information Type <sup>2</sup>	Retention Period
Templates or resources developed by eHealth Ontario in respect of the EHR;	For a minimum of 2 years
Assurance-related documents	10 years
eHealth Ontario business documentation	For a minimum of 7 years

## 5 Enforcement<sup>3</sup>

- 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.

---

<sup>3</sup> References to the applicable privacy and security committee and the applicable oversight body can be found in *Table 1: Applicable Governance Bodies*.



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

**Table 1: Applicable Governance Bodies**

<b>Term or Acronym</b>	<b>Definition</b>
FIPPA	<i>Freedom of Information and Protection of Privacy Act, 1990</i>
HIC	Health Information Custodian
mFIPPA	<i>Municipal Freedom of Information and Protection of Privacy Act, 1990</i>
PHI	Personal Health Information, as defined in the <i>Personal Health Information Protection Act, 2004</i>
PHIPA	<i>Personal Health Information Protection Act, 2004</i>

## 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

Information Type		Responsible
PHI in the EHR	PHI created or contributed in the EHR	eHealth Ontario
Audit logs or audit reports that contain PHI	Log of instances where all or part of the PHI in the EHR is viewed, handled or otherwise dealt with	eHealth Ontario
	Log of instances where all or part of the PHI in the EHR is transferred to a HIC	eHealth Ontario
	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	eHealth Ontario
	Instances where a Consent Directive is made, withdrawn or modified in the EHR	eHealth Ontario
	Notices related to Logging and Auditing	eHealth Ontario
	Report to IPC of 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	eHealth Ontario
	Auditing and Monitoring Reports	HIC & eHealth Ontario
	Archival copies of: <ul style="list-style-type: none"> <li>PHI in the EHR; and</li> <li>Audit logs or audit reports that contain PHI</li> </ul>	Archival copies of PHI in the EHR and audit logs or audit reports that contain PHI
Backup copies of: <ul style="list-style-type: none"> <li>PHI in the EHR; and</li> <li>Audit logs or audit reports that contain PHI</li> </ul>	Backups of PHI in the EHR and audit logs or audit reports that contain PHI	eHealth Ontario
Information collected to respond to individuals related to their: <ul style="list-style-type: none"> <li>Requests for Access or Requests for Correction under the PHIPA;</li> <li>Requests to make, modify, or withdraw a Consent Directive under PHIPA; and</li> <li>Inquiries or Complaints under PHIPA.</li> </ul>	Information created about an individual to respond to Request for Access, Request for Correction, request to make, modify, or withdraw a Consent Directive, Inquiries or Complaints under PHIPA.	eHealth Ontario or HIC who is accountable for producing the record
	Copy of notices provided to individuals for Consent Directives	
	Notices related to Requests for Consent Directives	
	Request for Access form (including identification and contact information)	
	Notices and Responses related to Requests for Access (including the fee estimate)	
	Request for Correction (including identification and contact information)	
	Notices and responses related to Requests for Correction (including the statement of disagreement)	
	Documented Complaints and Inquiries (including contact information)	
Notices and Copies of response to Complaints and Inquiries		
Information created about an individual as part of an investigation of Privacy Breaches and/or Security Incidents	Information created about an individual as part of an investigation of Privacy Breaches and/or Security Incidents	eHealth Ontario or HIC responsible for managing the incident
System-level logs of the EHR, tracking logs, reports and related documents for privacy and security tasks that do not contain PHI	System Troubleshooting Logs	eHealth Ontario
	Log of all system-level access to EHR	eHealth Ontario
	Log of information system events on the EHR	eHealth Ontario
	Log of all access by the HIC, their agents or Electronic Service Providers to EHR	HIC
	Log all information system events on their identity provider services and data contribution endpoints	HIC & eHealth Ontario

<b>Information Type</b>		<b>Responsible</b>
	Log of all information security exception requests	eHealth Ontario
	Log of all activities of administrators and operators on their identity provider services and their data contribution end points	HIC
	Log of all information system events found in the <i>Harmonized Security Logging and Monitoring Policy</i> Appendix A performed by the HIC, their agents or Electronic Service Providers	eHealth Ontario
	Log of all activities of their information system administrators and information system operators	eHealth Ontario
	List of all agents or Electronic Service Providers who have authorized access to identity provider technology and data contribution endpoints logs	HIC
	List of all agents or Electronic Service Providers who have authorized access to logs	eHealth Ontario
	Log of the destruction of the PHI in the EHR	eHealth Ontario
	List of distribution of copies of paper material classified as Restricted	eHealth Ontario
	List of vulnerability and configuration scanning tools which are approved by eHealth Ontario	eHealth Ontario
	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	HIC & eHealth Ontario
	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	HIC
	Log of all requests for IDs that they manage and that could be used to access EHR	eHealth Ontario
	List of all IDs that have access to [the EHR Solution]	eHealth Ontario
	Log of requests to make, modify or withdraw a Consent Directive (including identification and contact information)	HIC & eHealth Ontario
	Log of receipt of a request for Consent Directive	HIC & eHealth Ontario
	Log of notices provided to individuals for Consent Directives	HIC & eHealth Ontario
	List of all agents who are the subject of an Agent Consent Directive	eHealth Ontario
	Logs related to responses to Requests for Access	HIC & eHealth Ontario
	Logs related to responses to Requests for Correction	HIC & eHealth Ontario
	History of all Corrections of records of PHI in the EHR	eHealth Ontario
	Notices and reports of privacy breaches/ security incidents	eHealth Ontario
	Privacy Breach Management Investigation Report/ Security Incident Reports	eHealth Ontario
	Log of Privacy Breaches	eHealth Ontario
	Log of Security Incidents	HIC
	Privacy Breach Management Remediation Report	eHealth Ontario
	Status of Privacy Breach Management Remediation Report	eHealth Ontario
	Documented Inquiries (including contact information)	eHealth Ontario
	Log of receipt of Inquiries	eHealth Ontario
	Copy of response or log of responses to Inquiries	HIC & eHealth Ontario
	Log of receipt of Complaints	eHealth Ontario
Resources developed by eHealth Ontario in respect of the EHR	Privacy and Security Training Template	eHealth Ontario
	Notice for Obtaining Consent Template	eHealth Ontario
Assurance-related documents	Privacy Impact Assessment Recommendation Report and associated decisions and directions	eHealth Ontario
	Privacy Impact Assessment and associated decisions and directions	eHealth Ontario
	Threat and Risk Assessment (including TRA summaries)	eHealth Ontario

<b>Information Type</b>		<b>Responsible</b>
	Privacy and Security Readiness Self-Assessment and associated decisions and directions	HIC & eHealth Ontario
	Privacy and Security Operational Self- Attestation and associated decisions and directions	HIC & eHealth Ontario
	Remediation Plans and associated decisions and directions	eHealth Ontario
	Status of Remediation Implementation Report	eHealth Ontario
	Remediation Attestation	HIC & eHealth Ontario
	Non-Compliance Reports and associated recommendations	HIC & eHealth Ontario
	Compliance Monitoring Reports	HIC & eHealth Ontario
	Audit Reports and associated recommendations and decisions and directions	HIC & eHealth Ontario
	Asset Listing for the EHR	eHealth Ontario
	Risk Listing of threat and vulnerability ratings for EHR	eHealth Ontario
	End User Agreement Template	eHealth Ontario
	Business Continuity Plan	HIC & eHealth Ontario
eHealth Ontario Business Documentation	Applicable privacy and security committee Meeting Minutes	eHealth Ontario