Electronic Health Record Retention Policy and Procedure

Policy Level Approval:	Chief Executive Officer
Policy Category:	Corporate Policy
Policy Number:	INF-009.02-PP
Sensitivity Level:	Public
Policy Sponsor (or Sponsors):	Chief, Strategy, Planning, Privacy & Analytics
Original Date of Approval:	December 8, 2016
Date of Posting: This Policy is effective on the date of its posting or as otherwise noted in the Policy	July 22, 2025
Version Approval Date:	June 10, 2025
Next Scheduled Year Review (MM/YY):	28/29

1 Purpose, Objectives and Scope

1.1 Purpose

1.1.1 This policy and procedures outline Ontario Health's (**OH**) practices with respect to the retention period of paper and electronic Records held by OH under it's its authority as a Prescribed Organization under the *Personal Health Information Protection Act, 2004* (**PHIPA)**, including:

1.1.2 Records of personal health information (**PHI**) received by OH from a health information custodian (**HIC**) for the purpose of developing or maintaining the electronic health record (**EHR**) subject to *PHIPA*; and

1.1.3 Records of personal information (**PI**) received or created by OH which are subject to *Freedom of Information and Protection of Privacy Act, 1990 (***FIPPA***).*

1.2 Objectives

1.2.1 To enable OH as a Prescribed Organization to:

- Meet its obligations under *PHIPA, FIPPA* and associated regulations; and
- Comply with the requirements set out in the Information and Privacy Commissioner of Ontario's *Manual for the Review and Approval of Prescribed Organizations* **(IPC PO Manual**)*;* and
- To protect the privacy of individuals and the confidentiality of their PHI and PI.

1.3 Scope

1.3.1 This policy applies to non-union Employees, people leaders, board members, unionized Employees, secondees, consultants, individuals acting on behalf of OH (**OH Agents),** and Health Information Custodians (**HICs**) that provide or access PHI to OH for the purposes of the EHR.

1.3.2 This policy applies to the secure retention of Records of PI and PHI received by OH for the purpose of developing or maintaining the EHR as follows:

- PHI that is accessible by means of the EHR;
- PI to support the Provider Registry;
- Electronic records OH is required to keep further to paragraphs 4, 5 and 6 of s. 55.3 of PHIPA;
- Documents created and/or received in relation to the following:
    - Requests to make, withhold or withdraw Consent Directives;
    - Inquiries or complaints regarding compliance with *PHIPA* and its regulations;
    - Requests for access and/or corrections made under the *PHIPA.*
    - 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 and PI;
- Documents created, collected and retained for legal, regulatory or business purposes including:
  - Templates or resources developed in respect of the EHR;
  - Assurance-related documents; and
  - Business-related documents.

Note: Copies of Records of PHI made from the EHR and retained by HIC(s) or the custodian's agent/electronic service provider are out of scope of this Policy.

1.4 Compliance, Audit, Enforcement and Exemptions

1.4.1 Compliance with this Policy in its entirety is mandatory unless an exception to a specific section is approved by the Chief Privacy Officer (**CPO**) or delegate in writing. Failure to comply with the requirements of this Policy, without a written exception, may result in disciplinary action up to and including revocation of appointment, termination of employment or termination of contract without notice or compensation.

1.4.2 Compliance will be audited in accordance with and as per the frequency outlined in the *Privacy Audit and Compliance Policy*.

1.4.3 At the first reasonable opportunity upon identifying or becoming aware of a breach of this Policy, employee(s), or other OH Agents as well as HICs must notify the Privacy Office by reporting the breach to Enterprise Service Desk Phone: 1-866-250-1554; or Email: oh-servicedesk@ontariohealth.ca

1.4.4 Breaches of this Policy will be managed in accordance with the *Privacy Incident Management Policy and Procedure* and *EHR Privacy Incident Management Policy and Procedure.*

1.4.5 Compliance will be enforced in accordance with the *Progressive Discipline Policy*.

1.5 Terminology

1.5.1 The words "include" and "including" when used are not intended to be exclusive and mean, respectively, "include, without limitation," and "including, but not limited to".

1.5.2 Words and terms in this Policy that have meanings differing from the commonly accepted definitions are capitalized and their meanings are set out in the Definition and Acronyms section (Section 5).

2 Policy

2.1 Retention schedule

2.1.1 OH must ensure that Records of PI and PHI received by OH are retained for only as long as necessary for the purpose of developing or maintaining the EHR.

2.1.2 How long Records are retained by OH is determined in accordance with *PHIPA*, *FIPPA* and respective agreements with the HIC. *See Appendix A: Retention Schedule (for both paper and electronic format)* for Records of PI and PHI in both paper and electronic format, including various categories thereof.

2.2 Secure retention

2.2.1 OH is committed to retaining records of PHI in a secure manner. OH ensures that records of PI and PHI are retained in a secure manner in accordance with the *Personal Health Information Handling Standard* and industry security standards and best practices. The VP, Innovations for Connected Health is responsible for ensuring the secure retention of these records.

2.2.2 The form (identifiable/de-identified) in which the PI and PHI is retained will be determined and implemented in accordance with the purpose of developing and maintaining the EHR and the *Personal Health Information Handling Standard*.

2.2.3 The precise methods by which Records of PI and PHI in paper and electronic format are securely retained, including Records retained on various media is determined and implemented in accordance with the *Personal Health Information Handling Standard*, *Information Classification and Handling Standard* and the *Information Classification and Handling Guidelines*.

2.2.4 Employees or other OH Agents must take steps that are reasonable in the circumstances to ensure that the retained Records of PHI accessible by means of the EHR are not Collected without authority and are protected against theft, loss and unauthorized Use or Disclosure, and that Records of the PHI accessible by means of the EHR are protected against unauthorized copying, modification or disposal.

2.2.5 The *Information Security Risk Management Standard* identifies the OH Agent(s) responsible for retaining the system control and audit logs and where the system control and audit logs will be retained.

2.3 Use of Third-Party Service Providers

2.3.1 OH must ensure that any third party it retains to assist in providing services for the purpose of developing or maintaining the EHR agrees to comply with the restrictions and conditions that are necessary to enable OH to comply with Part V.1 of PHIPA.

2.3.2 Should OH choose to contract or otherwise engage with a Third-Party Service Provider to retain Records of PHI, it must ensure that written agreement executed with the third-party service provider contain obligations, restrictions and conditions in accordance with *Privacy Use and Disclosure Policy*, requirements set out in IPC PO Manual, applicable OH privacy and security policies, *PHIPA* and related regulations.

2.4 HIC's obligations

2.4.1 HICs must have in place policies, procedures and practices in respect of privacy and security that are necessary to enable them to comply with their obligations under *PHIPA*, *FIPPA* or the *Municipal Freedom of Information and Protection of Privacy Act, 1990,* where applicable.

2.4.2 HICs who use electronic means to Collect, Use, modify, Disclose, retain or dispose of PHI are required to comply with the prescribed requirements made under *PHIPA*.

2.4.3 A HIC shall 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 the prescribed requirements under *PHIPA*.

2.4.4 A HIC that has custody or control of PHI that is the subject of a request for access under s. 53 of PHIPA must retain the information 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.

2.4.5 A HIC is responsible for PHI in the custody or control of the HIC and may permit its agents to Collect, Use, Disclose, retain or dispose of PHI on the custodian's behalf only if,

(a) The custodian is permitted or required to Collect, Use, Disclose, retain or dispose of the information, as the case may be;

(b) The Collection, Use, Disclosure, retention or disposal of the information, as the case may be, is necessary in the course of the agent's duties and is not contrary to *PHIPA* or another law; and

(c) The prescribed requirements, if any, are met.

2.5 Secure transfer and disposal of Records

2.5.1 OH has in place safeguards to ensure the secure transfer and disposal of PI and PHI. Accordingly, all transfer and disposal of applicable Records of PI and PHI no longer required to fulfill the identified purpose must be handled in accordance with the OH's *Personal Health Information Handling Standard, Secure Transfer of Sensitive Information Standard, Media Destruction, Sanitization and Disposal Standard, Information Classification and Handling Standard, Information Classification and Handling Guidelines* and applicable EHR security policies.

2.5.2 OH must put in place reasonable safeguards to ensure that the Records of PHI that have been received for the purpose of developing or maintaining the EHR are securely disposed of in a secure manner following the retention period or the date of termination set out in any documentation and/or agreements executed prior to the receipt of the PHI.

2.5.3 The SVP, Digital Excellence in Health, or delegate, is responsible for ensuring that the records of PHI that have been received to develop and maintain the EHR are either securely returned or securely disposed of, as the case may be, following the retention period or the date of termination set out in applicable documentation and/or agreements executed prior to the PO's receipt of the PHI.

2.5.4 If the records of PHI are required to be securely returned to the person or organization from which they were received, OH will transfer the records in a secure manner and in compliance with the *Secure Transfer of Sensitive Information Standard*.

2.5.5 If the records are to be disposed of, OH will dispose of the records in a secure manner and in compliance with the *Media and Data Destruction, Sanitization and Disposal Standard.*

3 Procedures

3.1 General procedures

3.1.1 OH and HICs must ensure the Records identified in this policy are retained in accordance with the schedule outlined in in *Appendix A: Retention Schedule (for both paper and electronic format).*

3.1.2 At the end of the retention schedule specified in *Appendix A: Retention Schedule (for both paper and electronic format)*, PHI will no longer be made available by means of the EHR to HICs, OH and applicable agents and electronic service providers.

3.1.3 The Cyber Security Office of OH in collaboration with applicable business units must ensure that Records of PHI that have been received for the purpose of developing or maintaining the EHR are securely disposed of in a secure manner following the retention period or the date of termination set out in any documentation and/or agreements executed prior to the receipt of the PHI.

3.1.4 Where the contractual obligations between OH and HIC is terminated, OH will engage with the HIC to address the disposition of the Records of PI and PHI provided in accordance with *PHIPA*, *FIPPA,* applicable agreements and related privacy and security policies.

3.1.5 Where the PHI described in 3.1.3 has been Collected by a HIC other than the custodian that provided the PHI, the Record of PHI will be retained in the EHR for the time period specified in *Appendix A: Retention Schedule (for both paper and electronic format)*. Those Records will be subject to further Collection, Use and Disclosure by HICs, OH and applicable agents and electronic service providers.

4 Responsibilities

4.1 Ontario Health Chief Privacy Officer

4.1.1 Ensure compliance with *FIPPA* and *PHIPA* and ensuring relevant OH policies and, procedures are put in place.

4.1.2 Responsible for the overall accountability and the day-to-day operations of the Privacy Program.

4.2 SVP, Digital Excellence in Health, or delegate

4.2.1 Responsible for ensuring that records provided to OH are disposed of or returned to the person who provided the records in a secure manner and in accordance with applicable retention period.

4.3 Ontario Health Privacy Office

4.3.1 Support the development of OH policies and program related to EHR Retention.

4.3.2 Author and manage required updates to this Policy.

4.4 Managers/Supervisors

4.4.1 Ensure that employees and other OH Agents are in compliance with this Policy.

4.4.2 Support the management of Privacy Office and privacy program including all activities related to the retention of Records of PHI in the EHR.

4.5 Employees and other OH Agents

4.5.1 Ensure compliance in accordance with the procedures set out in this Policy.

4.5.2 Support the implementation of this Policy including all activities related to retention of Records of PHI in the EHR.

4.6 HICs who provide PHI to OH

4.6.1 Ensure 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 the prescribed requirements under PHIPA and this Policy.

5 Definitions and Acronyms

Defined terms are capitalized throughout this document.

Term / Acronym	Definition
Collect	Has the meaning set out in section 2 of PHIPA with respect to PHI; and in respect of PI has the same meaning. "Collect" means to gather, acquire, receive, or obtain the information by any means from any source, and "Collection" and "Collected" has a corresponding meaning.
Consent Directive	Means a directive, made in accordance with s. 55.6 of PHIPA, that withholds or withdraws, in whole or in part, an individual's consent to the Collection, Use and Disclosure of their PHI by means of the EHR by a HIC for the purposes of providing or assisting in the provision of health care to the individual.

Term / Acronym	Definition
CPO	Chief Privacy Officer
Disclose	Has the meaning set out in s. 2 of PHIPA with respect to PHI in the control of a HIC or a person; and in respect of PI has the same meaning. "Disclose" means to make the information available or to release it to another HIC or to another person, but does not include to Use the information, and "Disclosure" has a corresponding meaning.
EHR or Electronic Health Record	Has the meaning set out in s. 55.1 of PHIPA and generally means the electronic systems that are developed and maintained by OH pursuant to Part V.1 of PHIPA for the purpose of enabling HICs to Collect, Use and Disclose PHI by means of the systems.
Employee	A person employed and compensated by OH as an Employee, and is classified as either permanent full-time, permanent part-time, temporary full-time, temporary part-time, paid student or casual, as set out in the *Employee Classification Guideline*. A consultant or contractor is not an Employee.
FIPPA or *Freedom of Information and Protection of Privacy Act,1990*	Ontario legislation with two main purposes: 1) to make provincial government institutions more open and accountable by providing the public with a right of access to records; and 2) to protect the privacy of individuals with respect to their Personal Information held by provincial government organizations. References to FIPPA include the regulations made thereunder, as may be amended or replaced from time to time.
HIC or Health Information Custodian	Has the meaning set out in s. 3 of PHIPA and generally means a person or organization that has custody or control of personal health information for the purpose of health care or other health-related duties. Examples include physicians, hospitals, pharmacies, laboratories and the MOH, but does not include OH.
Individual	Has the meaning set out in section 2 of PHIPA with respect to PHI; and in respect of PI has the same meaning. "Individual" means the individual, whether living or deceased, with respect to whom the information was or is being collected or created.
IPC	Information and Privacy Commissioner of Ontario
IPC PO Manual	IPC Manual for the Review and Approval of Prescribed Organizations
Minister	Minister of Health
MOH	Ontario Ministry of Health
O. Reg. 329/04	Ontario Regulation 329/04 made under PHIPA
OH	Ontario Health, the agency of the Government of Ontario to which this Policy applies.

Term / Acronym	Definition
OH Agent	A person that acts for or on behalf of OH for the purposes of OH, and not for the Agent's own purposes, whether or not the Agent has the authority to bind OH, whether or not the Agent is employed by OH, and whether or not the Agent is being remunerated.
PHI or Personal Health Information	Has the meaning set out in section 4 of PHIPA. Specifically, it is "identifying information" in oral or recorded form about an individual that: • Relates to the physical or mental health of the individual, including information that consists of the health history of the individual's family; • Relates to the provision of health care to the individual, including the identification of a person as a provider of health care to the individual; • Is a plan that sets out the home and community care services for the individual to be provided by a health service provider or Ontario Health Team pursuant to funding under section 21 of the Connecting Care Act, 2019; • Relates to payments or eligibility for health care or eligibility for coverage for health care in respect of the individual; • Relates to the donation by the individual of any body part or bodily substance of the individual or that is derived from the testing or examination of any such body part or bodily substance; • Is the individual's health number; and/or • Identifies an individual's substitute decision-maker. PHI also includes identifying information about an individual that is not PHI listed above but that is contained in a record that includes PHI listed above. Information is "identifying" when it identifies an individual or when it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify the individual.
PHIPA or *Personal Health Information Protection Act, 2004*	The Ontario health privacy law. It establishes rules for the management of PHI and the protection of the confidentiality of that information, while facilitating the effective delivery of healthcare services. References to PHIPA include the regulation made thereunder, as may be amended or replaced from time to time.

Term / Acronym	Definition
PI or Personal Information	Has the meaning set out in section 2 of FIPPA. Specifically, it means recorded information about an identifiable individual, including: • information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual; • information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved; • any identifying number, symbol or other particular assigned to the individual; • the address, telephone number, fingerprints or blood type of the individual; • the personal opinions or views of the individual except where they relate to another individual; • correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence; • the views or opinions of another individual about the individual; and • the individual's name where it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual. Personal Information also includes information that is not recorded and that is otherwise defined as Personal Information when considering the manner of collection, notice to public, privacy impact assessments and safeguards.[1]
PIA	Privacy Impact Assessment.
Prescribed Organization or PO	The organization prescribed in Ontario Regulation 329/04 as the organization for the purposes of Part V.1 of PHIPA. The Prescribed Organization has the power and the duty to develop and maintain the EHR in accordance with Part V.1 of PHIPA and the regulations made thereunder.

[1] Section 38 (1) FIPPA

Term / Acronym	Definition
Privacy Incident	Any event where the Privacy Office is notified or becomes aware that a Privacy Breach may have occurred. This includes events that are reviewed/investigated and: 1. confirmed to be a Privacy Breach 2. confirmed not to be a Privacy Breach 3. it cannot or has not been determined if a Privacy Breach occurred (Suspected Privacy Breach). **Note:** Privacy Incidents include events involving PI and PHI, as well as De-identified Information and Business Identity Information as these events require investigation in accordance with this Policy to confirm if they are Privacy Breaches as defined below. OH shall investigate these incidents involving De-identified Data and Business Identity Information, considering factors such as the 1) risk of re-identification and related de-identification guidelines for De-identified Data, as well as 2) the context for handling data that OH received as Business Identity Information, to confirm that it does not constitute PI, respectively.

Term / Acronym	Definition

Privacy Breach	A Privacy Breach includes:
	1) Privacy Breach of PHI or PI (Privacy PHI/PI Breach) means an event where:
	• The Collection, Use, or Disclosure of PHI or PI is not in compliance with PHIPA or its regulation, or with FIPPA or its regulations (i.e., without legal authority); and/or
	• The Viewing, handling or otherwise dealing with PHI provided to OH is not in compliance with PHIPA, or its regulation;
	• PHI or PI is stolen, lost or subject to unauthorized Collection, Use or Disclosure or where records of PHI or PI are subject to unauthorized copying, modification, or disposal.
	Note: A Privacy PHI/PI Breach does not include a breach of De-identified Information, or Business Identity Information, if the event does involve PI or PHI.
	2) Privacy Breach of Privacy Policy or Agreement (Privacy Policy/Agreement Breach) means an event where:
	• There is a contravention of OH's privacy policies, procedures, or practices; and/or
	• There is a contravention of a privacy-related[2] term or condition in a:
	  ○ data sharing agreements,
	  ○ research agreements,
	  ○ confidentiality agreements, or,
	  ○ agreements with third-party service providers retained by OH to handle PHI or PI,
	  ○ written acknowledgements acknowledging and agreeing not to use PHI or PI which has been de-identified and/or aggregated, to identify an individual; and
	• Does not include a privacy breach of PHI or PI
	Note: A Privacy Policy/Agreement Breach may include a breach that involves De-identified Information or Business Identity Information, if the breach relates to privacy controls in an agreement or a privacy policy, procedure or practice related to handling of De-identified Information or Business Identity Information.

Record	Has the same meaning set out in s. 2 of PHIPA and s. 2 of FIPPA.
SDM or Substitute Decision Maker	Has the meaning set out in s. 5 of PHIPA and in relation to an individual, means, unless the context requires otherwise, a person who is authorized under PHIPA to consent on behalf of the individual to the collection, use or disclosure of PHI about the individual.
Third-Party Service Provider	A third-party contracted or otherwise engaged to provide services to OH, including Electronic Service Providers.

[2] A privacy-related term or condition, includes terms or conditions that relate to privacy requirements from law (including, for example, FIPPA, PHIPA and GOLA), the IPC PP/PE Manual, the IPC PO Manual, IPC guidelines and orders, OH's privacy information practices or other controls to protect the privacy of individuals or the confidentiality of their PI and PHI.

Term / Acronym	Definition
Use	In relation to PHI or PI in the custody or under the control of a HIC or a person, "Use" means to view, handle or otherwise deal with the information, but does not include to Disclose the information, and "Use", as a noun, has a corresponding meaning. For the purposes of PHIPA, the providing of PHI between a HIC and an agent of the HIC is a Use by the HIC, and not a Disclosure by the person providing the information or a Collection by the person to whom the information is provided.

6 Review Cycle

This Policy is to be reviewed by Ontario Health at least within 3 years of its effective date or earlier if required in accordance with the *Privacy Audit and Compliance Policy.*

7 References and/or Key Implementation Documents

- Personal Health Information Protection Act, 2004; Ontario Regulation, 329/04.
- Freedom of Information and Protection of Privacy Act, 1990
- Municipal Freedom of Information and Protection of Privacy Act
- Manual for the Review and Approval of Prescribed Organizations
- Privacy Audit and Compliance Policy
- Privacy Incident Management Policy and Procedure
- Information Classification and Handling Standard
- Information Classification and Handling Guidelines
- Information Security Risk Management Standard
- Personal Health Information Handling Standard
- Media Destruction, Sanitization and Disposal Standard
- Applicable EHR security policies.

8 Appendices

- *Appendix A: Retention Schedule (for both paper and electronic format)*

9 Policy Consultations

The following were consulted in the development of this Policy:

- Managers and responsible staff members of OH business units responsible for implementing and/or complying with this Policy.

10 Policy Review History

Date of Review MM/YYYY	Itemize section changed and description of change (if no changes made, indicate N/A	New policy number	Date of Approval DD/MM/YYYY	Approver
1/7/2025	• Updated IT contact information. • Updated roles and responsibilities to reflect changes in organizational structure. • Added/edited information throughout Policy as per the updated IPC Manuals; • Revised definitions of Personal Health Information, Personal Information, Privacy Breach and Privacy Incident • Updated compliance will be enforced in accordance with the Progressive Discipline Policy	INF-009.02-PP	10/06/2025	CEO

11

12 Policy Repeal

1) Date of Repeal:
2) Reason for Repeal:
3) Date of Approval of Repeal:
4) Approver:

Ontario Health

Appendix A: Retention Schedule (for both paper and electronic Record)

Ontario Health (OH) and health information custodians (HICs) must retain Records identified below in accordance with the corresponding retention period and ensure that the Records are disposed of in a secure manner as soon as reasonably possible after retention period noted below.

Record type	Responsible organization	Retention period
Personal health information (PHI) accessible through the electronic health record (EHR)		
PHI received from health information custodians (HICs)	OH	The longer of the following time periods: • As long as the HIC that provided the PHI to the EHR retains the PHI in its local systems in accordance with their retention schedule; • In accordance with the retention schedule of the HIC that created and contributed the PHI to the EHR; • 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

Record type	Responsible organization	Retention period
		health care; or 10 years after the patient has expired; or • In accordance with any applicable court order or court action or other legal requirements.
Personal health information (PHI) provided by HICs for the electronic health record (EHR)		
PHI received from health information custodians (HICs) for the purpose of data validation activities prior to contribution to the EHR	OH	No longer than 6 months unless otherwise authorized by OH.
Electronic records, audit logs and reports that contain PHI created for compliance purposes under *PHIPA*		
• As per ss. 55.3(4) (i), electronic record of all instances where all or part of the PHI is viewed, handled or otherwise dealt with by Employees or other persons acting on behalf of OH or by HIC or their agents. • As per ss. 55.3(4) (ii), electronic record of all instances where PHI is transmitted to a HIC where the HIC has requested the transmission. • As per ss. 55.3(5), electronic record of all instances where a Consent Directive is made, modified or withdrawn. • As per ss. 55.3(6), electronic record of all instances where a Consent Directive is overridden under s. 55.7. • Auditing and monitoring reports related to the electronic records that OH is required to keep under paragraphs 4, 5 and 6 of s. 55.3. • Electronic record of all instances where a notice of a Consent Directive is provided to a HIC pursuant to ss. 55.6 (7). • Notices of Consent Overrides provided to HICs pursuant to ss. 55.7(6). • Notices related to logging and auditing.	OH	The longer of 30 years after the record was created or when PHI is removed from the EHR.

Record type	Responsible organization	Retention period
Audits logs and reports created for troubleshooting and other operational purposes		
Audit reports that contain PHI created and maintained for troubleshooting and other operational purposes	OH	No longer than 60 days unless otherwise authorized by OH.
Archival Records		
Archival copies of PHI in the EHR	OH	Equals the retention period of the PHI in the EHR (see above).
Archival copies of audit logs and audit reports containing PHI		The longer of 30 years or when PHI is removed from the EHR.
Back-up Records		
• Backups of the PHI in the EHR • Backups of audit logs and audit reports containing PHI	OH	According to the schedule of the Electronic Service Provider, but no longer than 2 years.
Records related to access, correction, consent directives and inquires/complaints		
Information received and/collected in relation to the following: • Requests to make, withhold or withdraw Consent Directives; • Inquiries, concerns or Complaints regarding compliance with PHIPA and its regulations; and • Requests for access and/or corrections made under the PHIPA.	OH and applicable HICs responsible for responding under PHIPA.	2 years after the request, inquiry or complaints has been closed by the HIC, OH or the IPC, whichever is longer.
Records related to investigation of privacy breaches and/or security incidents		
Information created about an individual as part of an investigation related to privacy breaches and/or security incidents.	OH and HIC	2 years after the privacy breach has been closed by the HIC, OH or IPC, whichever is longer.
Templates or resources developed by OH in respect of the EHR		

Record type	Responsible organization	Retention period
• Privacy and security training template. • Notice for obtaining consent template.	OH	2 years
Assurance-related documents		
• Privacy impact assessment recommendation (**PIA**) report and associated decisions and directions. • PIA and associated decisions and directions. • Threat and risk assessment (**TRA**) including TRA summaries.	OH	10 years
• Privacy and security readiness self-assessment and associated decisions and directions. • Privacy and security operational self- attestation and associated decisions and directions.	OH and applicable HIC	
• Remediation plans and associated decisions and directions. • Status of remediation implementation report.	OH	
• Remediation attestation. • Non-compliance reports and associated recommendations. • Compliance monitoring reports. • Audit reports and associated recommendations and decisions and directions.	OH and HIC	
• Asset listing for the EHR. • Risk listing of threat and vulnerability ratings for EHR. • End user agreement template.	OH	
• Business continuity plan.	OH and HIC	

Record type	Responsible organization	Retention period
Information collected for identity provider identification or registration that contains PI	OH	7 years after last use
End User Credential Information where HIC is an Identity Provider	HIC	Permanent
Authentication Events where HIC is an Identity Provider	HIC	60 days online, 24 months total in archive
OH business related documentation		
Applicable committee meeting minutes	OH	7 years
System-level logs of the EHR, tracking logs, reports and related documents for privacy and security tasks that do not contain PHI		
Log of all system-level access to EHR	OH	2 years
Log of information system events on the EHR	OH	
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	OH and HIC	
Log of all activities of administrators and operators on their identity provider services and their data contribution end points	OH and HIC	
Log of all information system events found in the *Harmonized Security Logging and Monitoring Policy Appendix A* performed by the HIC, their agents or Electronic Service Providers	OH	
Log of all activities of their information system administrators and information system operators	OH	
List of all agents or Electronic Service Providers who have authorized access to identity provider technology and data contribution endpoints logs	OH	

Record type	Responsible organization	Retention period
List of all agents or Electronic Service Providers who have authorized access to logs	HIC	
Log of the destruction of the PHI in the EHR	OH	
List of distribution of copies of paper material classified as 'restricted'	OH	
List of vulnerability and configuration scanning tools which are approved by OH	OH	
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	OH and HIC	
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	OH	
List of all IDs that have access to [the EHR Solution]	OH	
Log of requests to make, modify or withdraw a Consent Directive (including identification and contact information)	OH	
Log of receipt of a request for Consent Directive	OH	
Log of notices provided to individuals for Consent Directives	OH and HIC	
List of all agents who are the subject of an agent Consent Directive	OH	
Logs related to responses to requests for access	OH	
Logs related to responses to requests for correction	OH	

Record type	Responsible organization	Retention period
History of all corrections of Records of PHI in the EHR	OH	
Notices and reports of Privacy Breaches/Security Incidents	OH	
Privacy breach management investigation report/Security incident report	OH	
Log of Privacy Breaches	OH and HIC	
Log of Security Incidents	OH and HIC	
Privacy breach management remediation report	OH	
Status of Privacy Breach management remediation report	OH	
Documented Inquiries (including contact information)	OH	
Log of receipt of Inquiries	OH	
Copy of response or log of responses to Inquiries	OH and HIC	
Log of receipt of Complaints	OH	