System Coordinated Access
Security Guide

Find us on the web: **www.systemcoordinatedaccess.ca/privacy**

Published: December 2017

Guide Index

Purpose

To identify the Security processes the organization has in place to protect and manage the personal information and personal health information and systems that store personal information and personal health information in its custody and control.

The Security Operational Policy has been created to comply with the requirements established by the MOHLC, Connecting Ontario and the Information Privacy Commissioner of Ontario and is intended to ensure alignment with eHealth Ontario.

The organization has implemented these controls to the best of our ability given the system functionality available to us. We agree to take actions reasonable to ensure compliance with these policies and processes under the authority provided to us.

The format has been categorized to align with the 14 Connecting Ontario Security Policies as follows:

- Acceptable use of Information and Information Technology
- Access Control and Identity Management
- Electronic Service Provider Management
- Information Asset and Information Security Management
- Security Incident Management
- Security Logging and Monitoring Management
- Local Registration Authority Practices Management
- Network and Operations Management
- Physical Security Management
- System Development and Life Cycle Management
- Threat Risk Management
- Cryptography Management
- Business Continuity Management – may be removed from this policy as managed by ED

Indented Audience:

- Privacy Policy requirements are to be upheld by all staff and agents who have access to personal information or personal health information stored on any electronic devise in the custody or control of the organization.
- Operational Policy requirements that are to be upheld by all staff and agents whose responsibility it is to protect and maintain personal health information stored on any electronic devise in the custody or control of the organization.

Definitions

Personal Health Information (PHI) is generally defined as any identifying information about an individual in oral or recorded form that relates to their physical or mental health. Examples include family health history, health card number, and any information that identifies an individual and links them to a health care provider.

Personal Information (PI) or sensitive **personal information** (SPI), as used in **information** security and privacy laws, is **information** that can be used on its own or with other **information** to identify, contact, or locate a single person, or to identify an individual in context.

Health Information Custodian (HIC) is a person or organization, named in PHIPA, that delivers health care services, as defined in PHIPA. Examples are Physicians, hospitals, pharmacies, laboratories, community care access centres and Long Term Care Facilities.

A HIC has custody or control of PHI as a result of the work it does. The HIC has the right to deal with the PHI and create records, as well as the responsibility to maintain the confidentiality and security of the PHI. Though the HIC is the owner of the materials and systems in which information is recorded (e.g. paper charts, computers or information technology systems), patients are the owners of their PHI.

Health Information Network Provider (HINP) is an individual or organization that provides services to two or more HICs primarily to enable them to use electronic means to disclose PHI to one another. Centre for Family Medicine Family Health Team eHealth Centre of Excellence (CFFM eCE) acts in this capacity in a number of business relationships.

IS Solution is defined as any information system that contains personal information or personal health information under the custody or control of the organization could refer to either internal electronic medical records system, provincial assets or other.

Electronic Service Provider (ESP) is an individual or organization that provides a means of storing &/or sharing PHI electronically such as the electronic medical record contained in your facility.

Provincial Asset is defined as any one or more provincial repository managed through eHealth Ontario or any other organization providing access to Personal Health Information

Indented Audience:
Policy requirements are to be upheld by all staff and agents who have access to personal information or personal health information stored on any electronic devise in the custody or control of the organization and all staff and agents whose responsibility it is to protect and maintain personal health information stored on any electronic devise in the custody or control of the organization.

The requirements of this policy have been included in the organization Confidentiality Forms all staff, agents and service providers sign.

All staff and agents will:

1.1 Always use assigned credentials to access IS Solutions.

1.2 Never allow another person to use their credentials to access the solution. All persons are accountable for any actions performed on a system that contains personal health information with their ID.

1.3 Only access systems that contain personal health information if their role requires them to do so, they are expressly authorized do so, it is necessary to do so (e.g. to provide or assist in the provision of healthcare) and in accordance with the organization`s policies.

1.4 Not disable, override or willfully bypass any information security control on systems containing personal health information.

1.5 Not attempt to exploit any suspected security weakness on systems containing personal health information, even to explore such weakness unless it is part of their assigned role to do so.

1.6 Never knowingly perform an act that will interfere with the normal operations of systems containing PHI, or try to disrupt the systems by either intentionally making the solution unavailable or affect the integrity of the data being stored or processed within the solution.

1.7 Always log out of the solution when not in use.

1.8 Only use equipment/devises approved by the organization to access the solution.

1.9 Never take a picture of data displayed in the solution unless it is within their role to do so or they have been expressly authorized to do so.

1.10 Only use their work email account or IS Solution email account to transmit personal health information unless they have been expressly authorized to use organization`s encrypted alternative.

1.11 Create passwords to access the solution that are easy to remember but hard to guess that meet the following guidelines:

a. Contain at least one number
b. Contain at least one upper case letter, contain at least one lower case letter
c. Not contain 3 consecutive characters (e.g. AAA)
d. Not contain part of your real name or any easily identifiable information such as your birthday
e. Be at least 8 characters long
    - It is recommended that you use phrases when creating passwords such as '!L0V32eAtP1zza'

f. When asked to change your password do not change it in an easily recognized pattern such as '!L0V32eAtP1zza2'
g. Passwords used to access the IS Solution must be different than passwords used to access other systems like corporate email, personal banking etc.
h. Passwords are to be committed to memory and never shared with anyone including a system administrator. If the password must be written down, it should be stored securely and does not reveal the Source identity e.g. "PSS password = !l0v3Mydog"
i. Should you feel your password has been used to access PHI inappropriately you must immediately change your password and notify the Privacy department.
j. No usernames or passwords are to be stored in an automated single sign on function such as a macro or function key unless the functionality has been authorized by the organization.
k. You must never use the temporary password provided at initial sign on to any IS Solution.

1.12 You must only use the approved remote access solution provided through a virtual private network to access the IS Solution remotely and follow the proper procedures to securely disconnect from the remote access solution.
1.13 You must never use access the IS Solution in a public area (e.g. Internet café, public transit and other non-private settings.
1.14 You must never leave your mobile computing device in a public area unattended.
1.15 Should you be required to leave you mobile computing device in a vehicle unattended, the device should be locked in the trunk or placed out of view. If these two options are not available, the device should be taken with you.
1.16 If personal information or personal health information needs to be downloaded onto the mobile computing device the data needs to be encrypted.
1.17 Authorized users are to report privacy/security incidents or suspicion of privacy/security incidents to Privacy Analyst immediately and must provide full cooperation with any information security incident investigation.
1.18 Authorized individuals must continue to uphold the guidelines stipulated in the Privacy Agreement even after employment/affiliation terminates. Failure to do so may result in legal action.
1.19 A researcher/employee must never discuss personal health information with any person that does not have a need-to-know or is not authorized to know the information.

Electronic Service Provider Management

- Electronic service providers are categorized according to supplier type and criticality according to the service they provide. Currently the service providers used by the organization are EMR (IS Solution) and Ontario Lab Information Service (OLIS) and ClinicalConnect.
- All new information systems and services to be provided by new Electronic Service Providers or on renewal of service agreements must be defined and documented. Service agreements should specify:
    - Roles and responsibilities under PHIPA and under the privacy and information protection security policies and procedures implemented in respect to the ID Service
    - Roles and responsibilities for implementing, maintaining and supporting the information systems or services to be provided which includes:

    - The level of criticality of the service
    - The dates and times when the service is required
    - The capacity requirements of systems and networks
    - Maximum permissible down-time and service level objectives
    - Service level reports and frequency
    - Critical timescales (the timescale beyond which a loss of service would be unacceptable to the organization)
    - The penalties to be imposed in the event the Electronic Service Provider fails to deliver the pre-agreed level of service or fails to fulfill its roles and responsibilities and,
    - Minimum information security and privacy controls
- New Electronic Service Providers are to implement applicable information security and privacy controls prior to the Electronic Service Provider being granted access to the IS Solution.
- The organization has a consistent method for handling the termination of relationship with Electronic Service Providers which may include:
    - Designating agent responsible for managing the termination
    - Revocation of physical and logical access rights to the organizations information, and
    - Secure return, transfer or destruction of all assets (backup media storage, documentation, hardware and authentication devices).

Information Asset Management and Information Security Management

Indented Audience:
Policy requirements that are to be upheld by all staff and agents whose responsibility it is to protect and maintain personal health information stored on any electronic devise in the custody or control of the organization.

Requirements:

- All PHI is transmitted in a secure manner through the use of secure email, encryption or virtual private network tunnel.

Information Security Policy

Indented Audience:
Policy requirements that are to be upheld by all staff and agents whose responsibility it is to protect and maintain personal health information stored on any electronic devise in the custody or control of the organization.

Requirements:

- HICs must identify and mitigate privacy and security risks and areas of non-compliance in respect of [the IS Solution], including through privacy and security readiness self-assessments, privacy and security operational self-attestations, auditing and monitoring activities and assurance of agents and Electronic Service Providers.
- All shall/must requirements are mandatory. Any deviation from a mandatory requirement in a [the EHR Solution] information security policy, standard, or supporting document must be approved by the Applicable Oversight Body.
- All information security exemption requests must be assessed by the Privacy and Security Operations Team and then reviewed by the Applicable Oversight Body for approval.

Local Registration Authority Practices Management

Indented Audience:
Policy requirements that are to be upheld by all staff and agents whose responsibility it is to protect and maintain personal health information stored on any electronic devise in the custody or control of the organization.

Requirements:

- Sponsorship of LRA is executed by the organization`s Executive Director
- An appropriately trained Local Registration Authority (LRA) and delegate(s) have been appropriately trained to manage access to the IS Solutions
- Any changes to the LRA or delegate(s) LRA are appointed/reviewed by the organization executive
- The organization will at all times have at a minimum one active trained LRA and one trained delegate
- Modifications to the status of an approved LRA may be based on a request from the LRP, or at the discretion of the RA if it is suspected or discovered that the LRA is non-compliant with relevant policies, procedures or agreements.
- The LRA's identity must be verified of each agent or Electronic Service Provider requesting access to [the EHR Solution]. However, agents or Electronic Service Providers whose identities have already been verified by the HIC in accordance with [the EHR Solution]'s Level 2 assurance requirements do not need have their identities revalidated. The LRA must still ensure that the individual that requested access is the one who was authorized.
- The LRA and delegate must follow the assigned protocol when establishing access for an individual to any IS Solution as follows:
    - Request must be received in writing by either HR representative or Dept. Lead who can visually identify the requested individual
    - The following information must be provided with request:
        - Full name, role, contact information, picture identity (copy of driver's license, passport or Certificate of Canadian Citizenship)
    - Enrolment requests must be retained in electronic file

    - Once access has been revoked, agents or electronic service providers must re-enroll in order to obtain reinstated access
    - Individuals who have multiple roles must be adequately informed of their permissions and obligations when accessing the IS Solution
- The sponsor must only request access it IS Solutions for individuals whose purpose of access is to collect PHI for providing or assisting in the provision of health care or for individuals whose purpose is to provide support for defined an permitted functionality within the administrative roles of the IS Solutions.
- The sponsor must not provide access to any provincial asset if access is requested for purposes other than providing or assisting in the provision of health care e.g. providing access for the purposes of:
    - Program planning, evaluation or monitoring
    - Risk or error management
    - Improving the quality of care, programs or services
    - Education and training (unless the individual is a student or resident who requires access to provide care)
    - For processing payments
- Sponsors must not provide access to any provincial asset if access is required for the purpose of research.
- The sponsor must suspend an account if the information is discovered suggesting that:
    - A Registration was misleading, false or fraudulent.
    - An End User failed to comply with policy, standards agreements or terms and conditions
    - Suspension is requested by a Sponsor or Registration Authority
- An account that has been suspended due to misleading, false or fraudulent information must not be used or reactivated unless the relevant information, documentation or other material facts are true, accurate, and complete.
- Must document and retain a reason for a suspension and any resulting actions take, including any investigation.
- The IDP must revoke the account of an End User if:
    - The individual no longer needs the account (e.g. he/she is deceased; has resigned or retired)
    - Referring the issue to the Health Information Custodian under whose delegation or authority the End User accesses or uses Federated Services; Confirming or requesting additional information or evidence from the End User.
    - It is determined that the information, documentation or any other matter provided or done to establish the Registration was misleading, false, or fraudulent
    - The identity has been otherwise compromised (e.g., identity theft).

Network and Operations Management

Indented Audience:
Policy requirements that are to be upheld by all staff and agents whose responsibility it is to protect and maintain personal health information stored on any electronic devise in the custody or control of the organization.

Requirements:

- The organization has implemented network zones and manages these zones in a manner that observes the separation of different computing environments. The segregation of networks may be based on criteria such as:
    - The classification of information transmitted on the network
    - The level of assurance required
- Traffic is controlled between network zones by using a security gateway at the zones perimeter.
- Security gateway configurations are reviewed annually. The process ensures the:
    - Review of the rule sets on security gateways
    - Removal of expired or unnecessary rules
    - Resolution of conflicting rules, and
    - Removal of unused or duplicate objects, e.g. network or computer systems
- Malware detection and repair software (or equivalent solution) has been implemented on identity provider services and data contribution end points to protect from malicious code.
- Malware detection and repair software has been implemented on HIC approved tools, processes and workstations to protect from malicious code.
- All malware detection and repair software is kept up to date and run at regular intervals.
- Whenever possible, automate virus definition updates and verification capability is in place to ensure that identity provider services and data contribution endpoints are properly updated. Where updates to virus definition files are not automated, identity provider services and data contribution endpoints that have malware detection and repair software installed on them are identified and updated manually in a timely manner.

Threat Risk Management

Indented Audience:
Policy requirements that are to be upheld by all staff and agents whose responsibility it is to protect and maintain personal health information stored on any electronic devise in the custody or control of the organization.

Requirements:

- TRA Executive summaries of provincial assets may be requested. Access to these reports will be restricted to authorize individuals and will be handled in a secure manner.

Cryptography Management

Indented Audience:
Policy requirements that are to be upheld by all staff and agents whose responsibility it is to protect and maintain personal health information stored on any electronic devise in the custody or control of the organization.

Disclaimer: The majority of cryptography requirements require system functionality that is managed directly by EMR Vendor. The organization`s internal policy had been created to reflect appropriate level of responsibility.

Organization`s Requirements/responsibilities:

- Only digital signatures are used for the purpose of signing.
- All digital signatures are revocable.
- Digital certificates are only trusted once it has been cryptographically validated and does not appear on a trusted CRL.

Information Security Incident Management Policy

All actual or suspected incidents are to be **IMMEDIATELY** brought to the attention of the Executive Director and the IT Administrator. A determination is made of whether a breach &/or security incident has actually occurred. The preliminary investigation is to take place as soon as possible but no later than 3 days after report of the incident.

If at any point in the incident management process it is identified that the incident has resulted in a privacy breach, then the incident must be handled in accordance with the Privacy Breach Incident Management Process.

- NOTE: The Security Incident Management Process outlines the process to be followed should the incident happen to a provincial asset or a combination of provincial asset + internal IS Solution. Note that each provincial asset has its own incident reporting processes – refer to the appropriate eHealth Ontario (provincial asset) Guide.

IT Administrator will keep Incident Log and all incident reports stored electronically and will review periodically to identify any patterns or trends in incidents. If patterns or trends are identified the IT Administrator will within a reasonable period of time, identify any administrative, physical or technical safeguards that must be implemented to prevent or minimize the risk of future incidents. Organization`s IT Administrator collaborate with any affected provincial asset to investigate any actual or suspected incidents and will follow appropriate incident management processes where required to remediate the incident.

INFORMATION SECURITY INCIDENT MANAGEMENT

Process	Task
Step 1 Identification/Triage	• Contain/retrieve PHI • Remove/suspend access accounts • Notify Police/authorities/provincial asset(s) if necessary • Conduct investigation of incident/interview breach initiator(s)
Step 2 Response	• PHI Involved • Identify Cause & Extent of Incident • Systems affected by Incident
Step 3 Communication	Notifying affected individuals: • When, How & Who • What should be included in notification • Others to Contact
Step 4 Follow Up	• Audit of technical & physician security • Review of policies & procedures • Review of Employee Training Practices • Review of Service Delivery Partners

Definitions

Privacy Breach is defined as:

- Determined or wilful inappropriate collection, use, disclosure, retention or destruction of PHI
- Any contravention of PHIPA
- Examples:
    - Losing PHI that contains patient identifying information
    - Sharing a patients PHI with a person who is not involved in patient's care
    - Unauthorized (wilful) viewing of PHI for individuals for whom you are not providing health care to or assisting in the provision of health care

Privacy Process Incident is defined as:

- Any contravention of Process established by the organization that governs the collection, use, disclosure, retention or destruction of PHI
- Examples:
    - Sending PHI to the wrong HIC (wrong fax #)
    - Using an unsecure means of emailing PHI to internal HSPs
    - Leaving PHI in plain view (if not viewed by unauthorized individuals)
    - Inappropriate destruction of PHI (if not viewed by unauthorized individuals)

Security Incident Involving PHI is defined as:

- Any violation or imminent threat of violation of information security policies, standards, procedures or practices or any information security event that may compromise operations or threaten the security of an information system or business process
- PHI stored on an unsecure devise being lost or stolen
- Removing or in any way intentionally altering the systems built in security controls
- Allowing unauthorized individuals or assisting with unauthorized individuals gaining access to our secure EMR or any system or data storage device containing PHI
- EMR malfunction

Security Incident is defined as:

- Unlocked building or access to non-public areas
- Loss or theft of equipment (not containing PHI)
- Equipment malfunction (not containing PHI)

Please note that in all incidents/breaches the disciplinary course of action will be decided upon by the organization`s Executive Board and could result in suspension, termination, reporting to regulatory body/college and Information Privacy Commissioner of Ontario which may result in fines.

Internal Process

STEP 1
Identification/Triage

1. Obtain details regarding the incident or suspected incident from the person reporting it and the person suspected of causing the incident.
2. Record details on the Incident Management Reporting Form
3. Determine if the incident is defined as a privacy breach, privacy process incident, security incident involving PHI or security incident and follow correct incident management protocol specific to that type of incident.
4. Provide staff with incident process worksheet which clearly outlines expectations, timelines and contact information
5. IT Administrator must report all Level 1 and Level 2 Incidents involving a provincial asset to the incident response lead or team to review the incident report and any supporting information within the time frames outlined on Appendix A: Incident Severity and Priority Ratings for severity ratings and any affected HICs by the end of the next business day.
6. Incident report will be created and contain the following information:
    - The date and time of the incident;
    - The name of the individual(s) who reported the incident;
    - A description of the nature, scope and cause of the incident;
    - Any impacts of the reported incident;
    - The measures implemented to contain the incident;
    - The measures that have been implemented or will be implanted to remediate and prevent similar incident.

7. If an incident that originates at a HIC affects multiple HICs as well as provincial asset(s) the program office for the provincial asset may assume leadership of the incident management activities.

STEP 2
Response

The incident response lead or team must take steps to limit the scope and magnitude of an incident. Mitigation or containment activities may include:

- Backing up the information system
- Discontinuing operations
- Changing passwords or modifying access control lists on the compromised information system, and
- Restricting connectivity.

When the incident does not involve a provincial asset the IT Administrator should create containment strategies for each major incident type, with criteria clearly documented to facilitate decision-making. Criteria for determining the appropriate strategy may include:

- Potential damage to and theft of resources
- Need for evidence preservation
- Service availability (e.g., network connectivity, services provided to external parties)
- Time and resources needed to implement the strategy
- Effectiveness of the strategy (e.g., partial containment, full containment)
- Duration of the solution (e.g., emergency workaround to be removed in four hours, temporary workaround to be removed in two weeks, permanent solution).

NOTE: Depending on the severity of an incident it may be necessary to activate business continuity plans.

The IT Administrator must remediate all applicable information systems so that they return to full and normal operations. Remediation activities may include:

- Eradicating the cause of the incident (e.g., removing malware)
- Restoring and validating the information system
- Deciding when to restore operations, and
- Monitoring information systems to verify normal operations without further information system or data compromise.

STEP 3
Communication

The IT Administrator will work with your organizations Privacy Lead to notify patients when there has been an incident involving PHI. Refer to section 11.4 in the Privacy Guide for guidance.

Incidents involving provincial asset(s) remediation activities must:

Be approved by:	For incidents classified as
Connecting Security Committee, and Applicable Oversight Body	Severity 1
Connecting Security Committee	Severity 2
[The EHR Solution] Information Security Lead	Severity 3 and Severity 4

STEP 4
Follow Up

- The provincial asset program office or IT Administrator must investigate all incidents to identify the cause of the incident (e.g., by performing root cause analysis.)
- Once an incident has been resolved (i.e., all remediation activities have been implemented and affected information systems and information technology have returned to full and normal operations) the incident response lead or team must complete the incident report. During longer investigations, affected HICs may request status updates on the incident investigation in the interim.
- The provincial asset(s) Program Office or IT Administrator must archive their incident reports for a minimum of 24 months.
- The provincial asset(s) Program Office or IT Administrator must provide participating HIC with any provincial asset incident reports within 72 hours of the request.
- The final incident reports should be reviewed by the Connecting Security Committee and if necessary the Applicable Oversight Body.
- The provincial asset(s) program office or IT Administrator should implement a mechanism to review all of their incidents, at a minimum, monthly to identify trends and to determine whether any preventative actions can be taken to reduce the likelihood of similar incidents from occurring in the future.

Evidence Gathering

The provincial asset(s) program office or IT Administrator should develop procedures for collecting evidence for the purposes of disciplinarily or legal action against agents or Electronic Service Providers. These procedures should require:

- Forensics work to be performed on copies of the evidential material.
- The creation of copies be witnessed
- Details of the creation should be logged, including:
- When and where the copying process was executed
- Who performed the copying activities, and

- Which tools or programs were utilized for the copying process
- The integrity of all evidential material is protected.

Appendix A: Security Incident Management Process

Severity Ratings

Severity	Category and Description	Recommended Maximum Time Frames		
		Triage	Containment	Recovery
1	**Critical** • Critical or multiple sites down • Loss of service poses substantial risk to participating HICs • Posing a public health safety, privacy or security risk • Causing significant adverse impact affecting a large number of internal and/or external systems, e.g., large scale malware outbreak Immediate response and restore – "all hands on deck"	30min	6hrs	72hrs
2	**High** • Single, critical site down • Loss of non- mission-critical service • Help desk unavailable • Remedy Failure • Service degradation affecting HICs Response/restore as quickly as possible - within one business day	2hrs	12hrs	24hrs
3	**Medium** • Application or physical component slowdowns • Minor technical or function problems • Application or component failure affecting single client Restore within the next few business days	4hrs	36hrs	48hrs

4	**Low** • Minimal impact, not time- critical, or work-around exists. Restore within a week	24hrs	36hrs	15 days

Priority Ratings

Incident Type	Priority Rating	
	P2	P1
Access control: Reserved for security incidents related to a potential compromise of access control.		
Privilege account compromised E.g., a Privileged ID (such as system administrators, database administrators, firewall administrators) demonstrates unusual activities/behaviors (e.g., unexplained log-ins, unexplained file accesses)	**X**	
Phishing attack detected – targeting privileged users: E.g., numerous suspicious emails targeting users with privileged access.	**X**	
Asset security: For incidents that involve lost or stolen assets and attacks to an asset causing disruption of service.		
Loss of unencrypted storage media E.g., loss of an unencrypted USB drive containing sensitive data is lost.	**X**	
Denial of Service (DOS) attack against a critical asset detected E.g., a DOS attack has been initiated against a server hosting business critical applications	**X**	
Data security: For incidents that threaten the confidentiality of data.		
Unusually high volume of data access on server(s) hosting sensitive data/applications that process or store sensitive data E.g., a system alarm is triggered that there is a high volume of data transfer during non-business hours (not caused by data back-up)	**X**	
Malware / Virus infection detected– high impact E.g., an alarm is triggered that a virus outbreak was detected	**X**	
Data and System Integrity: Incidents related to a potential compromise of integrity of data and systems		
Major data breach that has attracted media attention: E.g., a major data breach that has attracted media attention.		**X**
Tape back-up failed on over period of time E.g., A tape back-up failed for the past 5 sessions	**X**	

Appendix B - eHealth Ontario EHR Records Retention Schedule

Information Type1	Retention Period
PHI in the [NAME OF REPOSITORY OR SYSTEM]	The longer of the following time periods: • as long as the HIC that created and contributed the PHI to the [NAME OF REPOSITORY OR SYSTEM] retains the PHI in its local systems; • in accordance with the retention schedule of the HIC that created and contributed the PHI to the [NAME OF REPOSITORY OR SYSTEM]; 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 • Created and maintained for troubleshooting	The longer of 30 years or when PHI is removed from the [NAME OF REPOSITORY OR SYSTEM]. 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: • The PHI in the[NAME OF REPOSITORY OR SYSTEM]; and • Audit logs and audit reports containing PHI.	Equals the retention period of the PHI in the [NAME OF REPOSITORY OR SYSTEM] or the audit logs and audit reports respectively.

Backups of: • The PHI in the[NAME OF REPOSITORY OR SYSTEM]; and • 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: • Request for Access or Request for Correction under PHIPA; • Request to make, modify, or withdraw a Consent Directive under PHIPA; or • Inquiries or Complaints under PHIPA.	Two years after the Request for Access, Request for Correction, requests to make, modify, or withdraw a Consent Directive, or an Inquiry has been closed. In the case of Complaints, 2 years after the Complaint has been closed by the HIC, [PROGRAM OFFICE] or the Information and Privacy Commissioner of Ontario, whichever is longer.
Information Type	**Retention Period**
Information created about an individual as part of an investigation of Privacy Breaches and/or Security Incidents.	2 years after the Privacy Breach has been closed by the HIC, [PROGRAM OFFICE] or the Information and Privacy Commissioner of Ontario, whichever is longer.
Information collected for provider identification or registration that contains PI	7 years after last use
End User Credential Information where HIC is an Identity Provider	Permanent
System-level logs, tracking logs, reports and related documents for privacy and security tasks that do not contain PHI	For a minimum of 2 years
Authentication Events where HIC is an Identity Provider	60 days online, 24 months total in archive

Templates or resources developed by [PROGRAM OFFICE] in respect of the [NAME OF REPOSITORY OR SYSTEM];	For a minimum of 2 years
Assurance-related documents	10 years
[PROGRAM OFFICE] business documentation	For a minimum of 7 years