eHealth Ontario
It's working for you

EHR All-in-One Security Policy

For Viewing Organizations using ONE ID or ClinicalConnect accounts

Version: 2.2

Ontario
eHealth Ontario

Table of Contents

Introduction

Purpose

This document is primarily designed to provide the applicable EHR Security Policy and its Standard requirements for viewer sites when accessing [the EHR Solution].

The requirements as set out in the Policy and its Standards are intended to help protect the confidentiality, integrity, and availability of personal health information (PHI) stored in or processed by [the EHR Solution].

Original control numbers are referenced in the format {1.1} to aid in compliance activities.

Scope

The Policy and its Standards stated in this document apply to:

- All HICs, who are defined as Viewers within the context of [the EHR Solution] as well as their agents and Electronic Service Providers who view or have access to [the EHR Solution].

The applicable EHR Security Standards for "Viewer" sites are:

1. Acceptable Use of Information and Information Technology Standards
2. Cryptography Standards
3. Electronic Service Provider Standards
4. Information Asset Management Standards
5. Information Security Standards
6. Information Security Incident Management Standards
7. Local Registration Authority Practices Standards
8. Network and Operations Standards
9. Threat Risk Management Standards

This policy should be read in conjunction with the EHR Privacy Policies and their associated procedures, as amended from time to time.

The EHR Privacy Policies, as well as joint privacy and security policies that are referred to this document, can be found on the eHealth Ontario website: http://www.ehealthontario.on.ca/images/uploads/regional_partners/cGTA/privacy_policies_and_procedures/EHR_Privacy_Policies.pdf

Definitions

Agent: In relation to a health information custodian, means a person that, with the authorization of the custodian, acts for or on behalf of the custodian in respect of personal health information for the purposes of the custodian, and not the agent's own purposes, whether or not the agent has the authority to bind the custodian, whether or not the agent is employed by the custodian and whether or not the agency is being remunerated. For example, an agent may be an organization, employee or contractor that validates identities of the EHR users on behalf of a HIC; an Agent may perform data correction services for a HIC on their data contribution endpoint.

Applicable Oversight Body: The Applicable Oversight Body is comprised of senior-level executives who oversee all aspects of [the EHR Solution]. See *Policy Governance Structure* section below.

Connecting Security Committee (CSC): The provincial security forum consisting of senior security representatives from across the regions and eHealth Ontario. This is a decision making body responsible for establishing a functional and usable information security governance framework for participating organizations in the EHR.

Electronic Service Provider: A person that 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.

Information Technology: Any asset (physical or logical) that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. It includes, but is not limited to, hardware, software, firmware, ancillary equipment, and related resources.

Legally Responsible Person (LRP): Often a senior executive within the organization, such as the Chief Information Officer. This person is legally responsible for the enrollment process at their HIC. The LRP is responsible for authorizing Sponsors and LRAs to act on behalf of the HIC in the enrollment and enrollment processes.

Local Registration Authority (LRA): A person who has been authorized by a HIC's Legally Responsible Person to manage the registration and/or enrollment process for the HIC's agents and Electronic Service Providers to obtain access to [the EHR Solution] through the HIC's access control processes, procedures, policies, standards, and identity management system. LRAs are registered with [the EHR Solution] Program or its delegate and enroll and register agents and Electronic Service Providers on behalf of [the EHR Solution]. To note, the definition of LRA applies in the context of this standard and [the EHR Solution].

May: The requirement is only a recommendation, or provided as an implementation example and is not intended on being exhaustive.

Privacy Breach: A privacy breach includes circumstances where:

- A provision of the Personal Health Information Protection Act, 2004 (PHIPA) or its regulations has been or is about to be contravened;
- The privacy provisions of the [Applicable Agreements] or any other agreement in respect of [the EHR Solution] have been or are about to be contravened;
- The privacy policies, procedures and practices implemented in respect of [the EHR Solution] have been or are about to be contravened;
- Personal health information (PHI) in [the EHR Solution] is lost or stolen or has been or is about to be accessed by an unauthorized person; or
- Records of PHI in [the EHR Solution] have been or are about to be copied, modified or disposed of in an unauthorized manner.

Privacy and Security Operations Team: The Privacy and Security Operations Team is made up of [The EHR Solution] agents who support [the EHR Solution] privacy and security-related activities, initiatives and processes.

Shall/Must: Used for absolute requirements (e.g. they are not optional).

Should: Used when valid reasons exist in certain circumstances not to implement the requirement; however, the implementer must understand the implications before choosing a different course and must consider implementing compensating controls.

[The EHR Solution]: [The EHR Solution] and supporting systems designed to store and make available specified electronic PHI from the electronic health information systems of HICs that may not be available in planned provincial or regional repositories so as to act as a single repository of such information to reduce the load on source systems. This does not include any participating HIC's information systems or information technologies.

Registration Authority (RA): The person or entity that is responsible for registering Local Registration Authorities (LRAs). [The EHR Solution] or its delegate will act as the RA for all HICs whose agents and Electronic Service Providers will be provided access to [the EHR Solution] through the HIC's access control processes, procedures, policies, standards, and identity management system.

Sponsor: Any person who has the authority to authorize the access of agents and Electronic Service Providers to [the EHR Solution]. Typically, LRPs authorize persons such as managers to act as Sponsors; this may also be delegated to a LRA. To note, the definition of Sponsor applies in the context of this standard and [the EHR Solution].

Viewer: An organization that views data from [the EHR Solution] in accordance with the authorized permitted purposes. The organization leverages ONE ID credentials or credentials issued by an Identity Provider (e.g. a partner hospital organization, [the EHR Solution] provider, etc.) to access the solution in a read-only capacity. Viewer organizations may store some PHI locally on an ad-hoc basis but do not integrate data locally or relocate data from [the EHR Solution] to their local solution (e.g. EMR).

Within the context of eHealth Ontario solutions, these organizations typically sign the EHR Practice Agreement or EHR Access Services Schedule.

Enforcement

All instances of non-compliance will be reviewed by the Applicable Oversight Body.

The Applicable Oversight Body has the authority to impose appropriate penalties, up to and including termination of the Agreements with the HIC, Electronic Service Providers, or termination of the access privileges of agents, and to require the implementation of remedial actions.

Policy Governance Structure

EHR Solution	Applicable Oversight Body
Connecting Ontario CDR	eHealth Ontario Strategy Committee
Digital Health Drug Repository	eHealth Ontario Strategy Committee
Diagnostic Imaging Common Services	eHealth Ontario Strategy Committee
Primary Care CDR	eHealth Ontario Strategy Committee

Information Security Policy

Do (✓):

Principles

Acceptable Use of Information and Information Technology

✓ [The EHR Solution] Program and HICs must define behavioural requirements governing the acceptable use of information and information technology to which [the EHR Solution]'s agents and Electronic Service Providers, and HICs, their agents, and Electronic Services Providers with access to [the EHR Solution] must adhere. {1.1}

Refer to the Acceptable Use of Information and Information Technology.

Cryptography

✓ HICs must implement cryptographic solutions on their relevant information systems to protect the confidentiality and integrity of PHI that is accessed through [the EHR Solution]. {1.6}

Refer to the Cryptography Standard.

Electronic Service Providers

✓ HICs must ensure that their Electronic Service Providers who will have access to their identity provider services or data contribution endpoints, or who manage or provide support to these systems have adequate information security controls in place to protect and maintain the level of confidentiality, integrity and availability. {1.16}

Refer to the Electronic Service Provider Standard.

Information and Asset Management

✓ [The EHR Solution] Program must classify and define protection requirements for PHI in [the EHR Solution] in a manner that protects its confidentiality, integrity, and availability in any from (e.g. paper or electronic) throughout its information lifecycle. {1.7}

Refer to the Information and Asset Management Standard.

Information Security Incident Management

✓ [The EHR Solution] Program and HICs must implement an information security incident management process to identify and resolve information security incidents related to [the EHR Solution] or [the EHR Solution] quickly and effectively, while minimizing their impact and reducing the risk of similar information security incidents from occurring. {1.21}

Refer to the Information Security Incident Management Standard.

Information Security Training

- ✓ [The EHR Solution] Program and HICs must foster an information security-positive culture. This may be achieved by implementing an information security awareness and education program to help all persons with access to [the EHR Solution] to understand their information security-related obligations. {1.2}

  Refer to the Privacy and Security Harmonized Training Standard.

Network and Operations

- ✓ HICs must implement controls to secure their network infrastructure, and establish procedures to secure the ongoing management and operation of their identity provider services and data contribution endpoints. {1.12}

  Refer to the Network and Operations Standard.

Privacy and Security Assurance

- ✓ HICs must identify and mitigate privacy and security risks and areas of non-compliance in respect of [the EHR 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. {1.22}

  Refer to the Privacy and Security Harmonized Assurance Standard.

Threat Risk Management

Refer to the Threat Risk Management Standard.

Health Information Custodian Responsibilities

All HICs must:

- ✓ Develop, implement, and maintain an information security policy for their organization that upholds the principles of this policy and any other applicable information security policies, standards, and supporting documents. {3.4.1}

- ✓ Designate an information security lead to ensure compliance with the principles outlined in this policy. The information security lead may be the same person as the appointed contact person required by Personal Health Information and Protection Act, 2004 (PHIPA) section 15 or the site contact identified in the participation agreement. {3.4.2}

- ✓ Ensure that all agents and Electronic Service Providers who have access to [the EHR Solution] Services are appropriately informed of their information security responsibilities. {3.4.3}

- ✓ Require all agents and Electronic Service Providers who have access to [the EHR Solution] to agree to an end user agreement that includes confidentiality provisions before being provided with access to [the EHR Solution]. {3.4.4}

- ✓ Hold individual agents and Electronic Service Providers accountable for unauthorized or inappropriate access, collection, use, disclosure, disposal, destruction, modification, or interference with [the EHR Solution], or their information systems. {3.4.5}

Acceptable Use of Information and Information Technology Standard

Do (✓) and Do Not (X)

HICs, their agents and Electronic Service Providers ("all persons") must:

- ✓ Always use their assigned credentials to access [the EHR Solution]. {1.1}
- ✓ Abide by the terms and conditions of [the EHR Solution]. {1.7}
- ✓ Use a [the EHR Solution] or HIC-approved tools and processes to access [the EHR Solution]. {1.9}
- ✗ Never allow another person to use their credentials to access [the EHR Solution]. All persons are accountable for any actions performed on [the EHR Solution] with their ID. {1.2}
- ✗ Never access [the EHR Solution] unless their role requires them to do so, they are expressly authorized to do so, or it is necessary to do so (e.g. to provide or assist in the provision of healthcare), and then only in accordance with their respective HIC's or [the EHR Solution]'s privacy policies. {1.3}
- ✗ Never disable, override or willfully bypass any information security control on [the EHR Solution]. {1.4}
- ✗ Never attempt to exploit any suspected security weakness on [the EHR Solution], even to explore that such a weakness may exist, unless it is part of their assigned job duties or responsibilities and they are explicitly authorized to do so. {1.5}
- ✗ Never knowingly perform an act that will interfere with the normal operations of [the EHR Solution], or try to disrupt [the EHR Solution] by either intentionally making the solution unavailable or by affecting the integrity of the data being stored in or processed by [the EHR Solution]. {1.6}
- ✗ Never take a picture of data displayed on [the EHR Solution]. {1.10}

All persons should:

- ✓ Lock their computing devices when leaving their device unattended while logged on to [the EHR Solution] within the HIC's premises. {1.8}

Emailing PHI[1]

All persons must:

- ✓ Only email PHI to [the EHR Solution] Program Office when it is necessary for the purposes of providing or assisting in the provision of health care or [the EHR Solution] business, and is acceptable under their respective HIC's and [the EHR Solution]'s policies, standards or procedures. {1.11}
- ✓ Either encrypt emails that contain PHI, use a secure file transfer solution or use a secure email system approved by their respective HIC or [the EHR Solution]. {1.12}

[1] This section only applies to emailing PHI to [the EHR Solution] Program Office, it does not apply to internal HIC practices related to email.

- ✗ Never use external email accounts (e.g. Hotmail, or Gmail) to send PHI to or receive PHI from [the EHR Solution]. {1.13}

Creating and Protecting Passwords[2]

All persons should:

- ✓ Where possible, use phrases (e.g. "ILov3EatingP!zza") when creating passwords used to access [the EHR Solution]. {1.14}

All persons must:

- ✓ Always create passwords used to access [the EHR Solution] that are at least eight characters long and include at least three of the following: {1.15}
  - One number {1.15.1}
  - One uppercase letter {1.15.2}
  - One lowercase letter, or {1.15.3}
  - One special character {1.15.4}
- ✓ Choose passwords used to access [the EHR Solution] that are easy to remember but hard to guess by someone else. {1.17}
- ✓ Ensure their passwords used to access [the EHR Solution] are different from their password(s) used to access other accounts (e.g. corporate email account, personal banking, etc.). {1.19}
- ✓ Commit passwords used to access [the EHR Solution] to memory. All persons must avoid keeping a record of their passwords (e.g. on paper, or stored on in a file), unless it: {1.20}
  - Can be stored securely, and {1.20.1}
  - Does not indicate the associated ID or that it is for [the EHR Solution]. {1.20.2}
- ✓ Keep their passwords used to access [the EHR Solution] a secret, never telling anyone their password, including a system administrator, help desk personnel or a manager. {1.21}
- ✓ Immediately change their password used to access [the EHR Solution] if they suspect or confirm that their password has been disclosed or compromised and notify their information security incident initial point of contact (e.g. a helpdesk or Privacy Officer) of the security incident, see "Reporting Information Security Incidents Related to [the EHR Solution]" below. {1.22}
- ✓ Always change any password used to access [the EHR Solution] that is provided to them at initial login and as directed by their Identity Provider. {1.24}
- ✗ Never create passwords used to access [the EHR Solution] that include: {1.16}
  - All or part of their ID. {1.16.1}
  - Easily obtained personal information about themselves (e.g. names of family members, pets, birthdays, anniversaries, or hobbies). {1.16.2}
  - Three consecutive characters (e.g. "AAA"). {1.16.3}
- ✗ Never change passwords used to access [the EHR Solution] in an easily recognized pattern (e.g. changing "ILov3EatingP!zza1" to "ILov3EatingP!zza2"). {1.18}

[2] This section only applies to passwords used to directly access [the EHR Solution].

- ✗ Never include their ID or password used to access [the EHR Solution] in any automated single sign-on process (SSO) (e.g. stored in a macro or function key) except [EHR Solution] approved SSO management systems. {1.23}

Working Remotely

All persons must:

- ✓ Use a [the EHR Solution] or HIC-approved remote access solution (e.g. through a virtual private network or terminal services) to remotely access [the EHR Solution]. {1.25}

- ✓ Follow the proper procedures to disconnect from a remote access connection used to access [the EHR Solution] (e.g. if the remote access solution has a disconnect option, use this option to disconnect rather than simply closing the application). {1.26}

- ✓ When required to leave their mobile computing device in a vehicle, lock it in the trunk or place it out of view before getting to your destination. If you get to the destination before securing the device you should take it with you instead. {1.29}

- ✓ Ensure that if personal health or personal information is downloaded onto a mobile device from [the EHR Solution], the location where the data is stored is encrypted or the end user tool utilizes full disk encryption. Full disk encryption is the preferred option on mobile devices however containerized implementations of encryption on shared personal and corporate devices are also acceptable. {1.30}

- ✗ Never access [the EHR Solution] in an area where unauthorized individuals can view the information (e.g. Internet cafés, public transit, and other non-private settings). {1.27}

- ✗ Never leave their mobile computing device that has the ability to access [the EHR Solution] unattended in a public place. {1.28}

Reporting Information Security Incidents Related to [the EHR Solution]

All persons must:

- ✓ Immediately report suspected or confirmed information security incidents related to [the EHR Solution] to their information security incident initial point of contact (e.g. a help desk or Privacy Officer). Alternatively, HICs may instruct agents to report the incident to their manager or supervisor, who in turn must report it to the information security incident initial point of contact. {1.31}

  Examples of information security incidents include, but are not limited to:

  - Unauthorized disclosure of PHI.
  - Theft or loss of information technology that contains PHI or has access to [the EHR Solution] even if it is encrypted.
  - Virus or malware infection on a device that has access to [the EHR Solution].
  - Attempts (either failed or successful) to gain unauthorized access to [the EHR Solution].
  - Compromised password (e.g. another individual knows your password that is used to access [the EHR Solution]).

- ✓ Provide their full cooperation to [the EHR Solution] Program Office, their agents or Electronic Service Providers with any information security incident investigation. {1.32}

Cryptography Standard

Do (✓)

- ✓ HICs must only use [the EHR Solution] approved cryptographic algorithms for connections established with [the EHR Solution]. A list of approved cryptographic algorithms can be found in *Appendix A: Approved Cryptographic Algorithms*. {1.1}

- ✓ HICs must ensure that each cryptographic key or key component has the fewest number of key custodians necessary. {1.35}

Electronic Service Provider Standard

Do (✓):

- ✓ HICs should identify Electronic Service Providers and categorize them according to supplier type (e.g. application service provider, network service provider, storage service provider, etc.) and criticality of the services they provide. {1.1}

- ✓ HICs should maintain formal documentation of the: {1.2}
  - o Technical and organizational relationship covering the Electronic Service Provider's roles and responsibilities under the Personal Health Information Protection Act and its regulation (PHIPA) and under the HIC's privacy and information security policies, standards, and procedures {1.2.1}
  - o Roles and responsibilities for implementing, maintaining and supporting the information systems or services that the Electronic Service Providers are required to fulfill {1.2.2}
  - o Service goals {1.2.3}
  - o Expected deliverables, and {1.2.4}
  - o Representatives of Electronic Service Providers. {1.2.5}

  Formal documentation may include contracts, agreements and service levels.

- ✓ HICs must assess the potential information security and privacy risks posed by all new Electronic Service Providers to [the EHR Solution] prior to engaging in a contractual relationship with that Electronic Service Provider. {1.3}

- ✓ HICs must define and document all information systems and services to be provided by new Electronic Service Providers or on renewal of service agreements. Service agreements should specify: {1.4}

  - o Roles and responsibilities under PHIPA and under the privacy and information security policies, standards, and procedures implemented in respect to [the EHR Solution] {1.4.1}
  - o Roles and responsibilities for implementing, maintaining and supporting the information systems or services to be provided {1.4.2}
  - o The level of criticality of the service {1.4.3}
  - o The dates and times when the service is required {1.4.4}
  - o The capacity requirements of systems and networks {1.4.5}
  - o Maximum permissible down-time and service level objectives {1.4.6}
  - o Service level reports and frequency {1.4.7}
  - o Critical timescales (e.g. the timescale beyond which a loss of service would be unacceptable to the HIC) {1.4.8}

- 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 {1.4.9}
- Minimum information security and privacy controls. {1.4.10}

✓ HICs must require new Electronic Service Providers to implement applicable information security and privacy controls prior to the Electronic Service Provider being granted access to [the EHR Solution]. {1.3}

✓ HICs should establish a consistent method for handling the termination of relationships with Electronic Service Providers, which may include: {1.6}

- Designating agents responsible for managing the termination {1.6.1}
- Revocation of physical and logical access rights to the organization's information, and {1.6.2}
- Secure return, transfer or destruction of all assets (e.g. back-up media storage, documentation, hardware, and authentication devices). {1.6.3}

Information and Asset Management Standard

Do (✓):

✓ HICs must ensure that all PHI that is transmitted to [the EHR Solution] Program Office or [the EHR Solution] is done in a secure manner (e.g. through the use of secure email, encryption, or virtual private network tunnel). {1.1}

Information Security Incident Management Standard

Do (✓):

✓ HICs must implement an information security incident ("incident") management process that covers all phases of the incident management process to deal with incidents related to [the EHR Solution]: {1.1}

- Identification/Triage
- Response
- Recovery, and
- Follow-up

(See *Appendix I: Information Security Incident Management Process* diagram)

✓ If at any point in the incident management process a HIC realizes that the incident has resulted in a privacy breach, then the incident must be handled in accordance with the Privacy Breach Management Policy. {1.2}

Identification/Triage

✓ HICs must establish a point of contact to which actual or suspected incidents related to [the EHR Solution] are reported. Most often, the point of contact is a service desk. {1.3}

✓ HICs must ensure that their agents and Electronic Service Providers are aware of their responsibility to immediately report actual or suspected incidents. {1.4}

- ✓ The point of contact must generate an incident ticket or log for all reported incidents related to [the EHR Solution]. At a minimum, the incident ticket must contain the following elements: {1.5}

  - o The time and date of the reported incident {1.5.1}
  - o The name and contact information of the agent or Electronic Service Provider that reported the incident {1.5.2}
  - o Details about the reported incident, (e.g. type and how it was detected) {1.5.3}
  - o Any impacts of the reported incident, and {1.5.4}
  - o Any actions undertaken to contain the incident either by the agent or Electronic Service Provider that reported the incident or the point of contact. {1.5.5}

- ✓ HICs must appoint an incident response lead or team who is responsible for initiating the triage, response, recovery and follow-up activities for incidents related to [the EHR Solution] Program or [the EHR Solution]. The incident response lead or team may be the same as the point of contact. {1.6}

- ✓ The point of contact must send all incident tickets related to [the EHR Solution] Program or [the EHR Solution] to the incident response lead or team to review the incident ticket and any supporting information to verify whether or not an incident has occurred. {1.7}

- ✓ The incident response lead or team must classify all actual incidents related to [the EHR Solution] according to severity (See *Appendix B: Incident Severity and Priority Ratings* for severity ratings). {1.8}

- ✓ The incident response lead or team must initiate an incident report related to [the EHR Solution] Program or [the EHR Solution]. (See *Appendix C: Incident Report Details*) {1.9}

- ✓ HICs must ensure that their incident management process requires the incident response lead or team to notify [the EHR Solution] Program Office Privacy and Security Team by email or telephone and any affected HICs by the end of the next business day of confirmed incidents that are classified as Severity 1 or Severity 2 according to *Appendix B: Incident Severity and Priority Ratings*. {1.10}

  At a minimum, the notification must contain the following elements:

  - o The time and date of the reported incident {1.10.1}
  - o The name and contact information of the agent or Electronic Service Provider that reported the incident {1.10.2}
  - o Details about the reported incident (e.g. type and how it was detected) {1.10.3}
  - o Any known or suspected impacts of the reported incident, and {1.10.4}
  - o Any actions undertaken to contain the incident either by the agent or Electronic Service Provider that reported the incident, the point of contact, or the incident response lead or team. {1.10.5}

- ✓ If an incident that originates at a HIC affects multiple HICs or [the EHR Solution], [the EHR Solution] Program Office may assume leadership of the incident management activities. {1.11}

- ✓ The team that leads the incident management activities (e.g. HIC or [the EHR Solution] Program Office) must notify the Connecting Security Committee and the Applicable Oversight Body: {1.12}

  - o Within 72 hours of notification for any incident related to [the EHR Solution] and classified as a Severity 1 or {1.12.1}
  - o Within one week of notification for any incident related to [the EHR Solution] and classified as a Severity 2. {1.12.2}

- ✓ HICs should prioritize incidents related to [the EHR Solution] in accordance with their severity rating. {1.13}

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: {1.14}
  - o Backing up the information system {1.14.1}
  - o Discontinuing operations {1.14.2}
  - o Changing passwords or modifying access control lists on the compromised information system, or {1.14.3}
  - o Restricting connectivity. {1.14.4}

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

Recovery

- ✓ HICs must remediate affected information systems so that they return to full and normal operations. Remediation activities may include: {1.15}
  - o Eradicating the cause of the incident (e.g. removing malware) {1.15.1}
  - o Restoring and validating the information system {1.15.2}
  - o Deciding when to restore operations, and {1.15.3}
  - o Monitoring information systems to verify normal operations without further information system or data compromise. {1.15.4}

Follow-up

- ✓ HICs must investigate incidents related to [the EHR Solution] to identify the cause of the incident (e.g. by performing a root causes analysis.) {1.16}

- ✓ Once an incident related to [the EHR Solution] Program or [the EHR Solution] has been resolved (e.g. 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 led by HICs, [the EHR Solution] Program Office or affected HICs may request status updates on the incident investigation in the interim. {1.17}

- ✓ HICs must archive their incident reports related to [the EHR Solution] for a minimum of 24 months. {1.18}

- ✓ HICs must provide [the EHR Solution] Program Office and impacted HICs with an incident report related to [the EHR Solution] within 72 hours of the incident report being requested. {1.19}

- ✓ The final incident reports should be reviewed by the Connecting Security Committee and if necessary the Applicable Oversight Body. {1.20}

- ✓ HICs should implement a mechanism to review their incidents related to [the EHR Solution], 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. {1.21}

Evidence Gathering

- ✓ HICs should develop procedures for collecting evidence for the purposes of disciplinarily or legal action against agents or Electronic Service Providers. These procedures should require: {1.22}
  - Forensics work to be performed on copies of the evidential material {1.22.1}
  - The creation of copies be witnessed {1.22.2}
  - Details of the creation be logged, including: {1.22.3}
    - When and where the copying process was executed {1.22.3.1}
    - Who performed the copying activities, and {1.22.3.2}
    - Which tools or programs were utilized for the copying process. {1.22.3.3}
    - The integrity of all evidential material is protected. {1.22.3.4}

Local Registration Authority Practices Standard

Organizations using ONE ID as their Identity Provider will need to follow the specific procedures established by ONE ID.

Do (✓) and Do Not (X):

Assigning/Modifying the Status of a Local Registration Authority (LRA)

- ✓ Each HIC must ensure that a Legally Responsible Person (LRP) or their delegate identifies at least one or more persons to act as a LRA to manage the enrollment of its agents and Electronic Services Providers who require access to [the EHR Solution]. {1.1}

- ✓ The LRP must ensure that a new LRA: {1.2}
  - Has the time and resources required to perform the duties {1.2.1}
  - Is stable in his or her current position (not subject to reassignment) {1.2.2}
  - Meets Level 2 assurance qualifications according to the Federation Identity Provider Standard, and {1.2.3}
  - Understands the importance of policy adherence, especially privacy and information security. {1.2.4}

- ✓ 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, standards, procedures or agreements. {1.4}

- ✓ If the status of a LRA is revoked or suspended, the LRP must submit a request to lift the suspension before the status may be reinstated. {1.5}

Enrolling an Agent or Electronic Service Provider with Access to [the EHR Solution]

Registration

- ✓ The LRA must validate the identity of End Users or their own Representatives during Registration and before issuing Credentials. The LRA may determine their respective Registration requirements for End Users. However, at a minimum, the LRA must:
  - Validate the Core Identity Information set out in section 3.1.1;
  - Ensure the method(s) used attain(s) the required Level of Assurance; and

- Ensure that each individual being Registered:
    - Is 16 years of age or older;
    - Presents sufficient information to validate identity and positively authenticate the individual upon subsequent access requests to Federated Services.

Organizations must leverage the processes of their Identity Provider. {IDP Standard 3.1}

✓ The LRA must collect the Core Identity Information when Registering and End User:

- Legal name
- Where applicable, all professional designations and license numbers of the individual {IDP Standard 3.1.1}

Assigned Information

✓ The LRA working with their Identity Provider must assign every End User the following:

- A User ID
- The information required to set and maintain passwords
- A Level of Assurance {IDP Standard – 3.2}

Access to Sensitive Information

✓ Access to any Federated Service containing Sensitive Information, including PHI and PI, shall not be provided unless a Registrant has been assigned AL2 or AL3.

Process Requirements for AL3

✓ Identity must be corroborated where an AL3 is required. Identity corroboration may either be by:

- Direct verification by an Authoritative Party (e.g. Vital Statistics Agency, Revenue Canada); and/or
- A trusted third-party professional (e.g. lawyer, doctor, minister).

It may also involve the exchange or confirmation of shared secrets – information that is known by the corroborator about a potential Registrant. For example, as in the passport model, a third-party may be required to confirm the length of time a potential Registrant has continuously resided in Canada. {IDP Standard – 3.4.1}

Documentary Requirements during Registration

✓ The LRA must verify the identity 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. {2.1; IDP Standard – 3.5}

- For example, if a HIC's on-boarding process requires an agent to present at least two identity documents with one of the documents being from the primary identity document list (see Appendix G: Acceptable Identity Documents) and the other from either the primary identity document list or secondary identity document list (see *Appendix G: Acceptable Identity Documents*), *AND* the HIC has a record of these document (e.g. in an agent's file) then the LRA does not need to revalidate their agent's identity. All requests for access to [the EHR Solution] must be approved by a Sponsor.

Documentary Requirements for AL3

✓ To Register at AL3:

- All identity documents must contain a photograph of the End User;
- A copy of the identity document must be taken and retained on record; and

  - End Users must sign their Registration application with a handwritten signature.

- ✓ The LRA must retain a copy of all requests to enroll an agent or Electronic Service Provider with access [the EHR Solution]. {2.2}

Suspension

- ✓ The HIC may suspend an account if:
  - Information is discovered or revealed suggesting a reasonable likelihood that the information, documentation or any other matter provided or done to establish the Registration was misleading, false or fraudulent;
  - An End User has failed to comply with any Federation policy, standard, agreement or the terms and conditions of any Federated Service; or
  - Suspension is requested by an IDP or End User for any reason (e.g. leave of absence). {IDP Standard 2.1.1}

- ✓ An account that has been suspended by the HIC due to possible misleading, false or fraudulent information must not be used or reactivated unless it has been confirmed that the relevant information, documentation or other material facts are true, accurate and complete. {IDP Standard 2.1.3}

- ✓ The IDP must document and retain a record of the reason(s) for a suspension and any resulting actions taken, including any investigation. {2.1.4}

Revocation

- ✓ The HIC 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);
  - It is determined that the account concerned is a duplicate;
  - It is determined that the information, documentation or any other matter provided or done to establish the Registration was misleading, false, or fraudulent; or
  - The identity has been otherwise compromised (e.g. identity theft).
  - Upon request of an End User {IDP Standard – 2.2.1}

- ✓ The IDP must document and retain a record of the reason(s) for a revocation and any resulting actions taken, including any investigation. {IDP Standard 2.2.2}

Reenrollment

- ✓ Once access to [the EHR Solution] has been revoked, agents or Electronic Service Providers must re-enroll in order to have their access to [the EHR Solution] reinstated. {2.3}

- ✓ Refer to *Appendix D: Enrolling an Agent or Electronic Service Provider with Access to [the EHR Solution]* for the process of enrolling new agents or Electronic Service Providers with access to [the EHR Solution]. {2.4}

Entitlement Criteria

- ✓ The LRP must identify a named person(s), group(s), or role(s) that has the authority to act as a Sponsor. {2.5}

- ✓ The Sponsor must only provide access to [the EHR Solution] clinical components to Agents whose purpose of access is to collect PHI for providing or assisting in the provision of healthcare. {2.6}

Examples of end-users who may meet the criteria of providing healthcare or assisting in the provision of healthcare, may include, but are not limited to:

- Regulated health professionals who see patients {2.6.1}
- Residents providing care to patients {2.6.2}
- Administrative staff who pull charts for physicians {2.6.3}
- Ward clerks who review results to flag abnormals for physicians {2.6.4}

✓ The Sponsor must only provide access to [the EHR Solution] administration components to Agents and Electronic Service Providers whose purpose of access is to: {2.7}

- Provide support for defined and permitted functionality within the administration roles of [the EHR Solution] (e.g. Privacy Officers, System Administrators, Agents and Electronic Service Providers) must not be granted access to functionality intended for those providing health care or assisting in the provision of health care (e.g. Clinicians). {2.7.1}

For example, system administrators may require access to error queue management functionality to correct and process messages, privacy officers may require access to privacy reports to generate audit reports, data mapping specialists may require access to the terminology mapping functions to map codes and terminologies. These individuals must not be granted access to functionality intended for those providing healthcare or assisting in the provision of health care (e.g. clinicians).

✓ Sponsors must not provide access to [the EHR Solution] if access is requested for purposes other than providing or assisting in the provision of healthcare, e.g. providing access for the purposes of: {2.8}

- Program planning, evaluation, or monitoring {2.8.1}
- Risk or error management {2.8.2}
- Improving the quality of care, programs, and services {2.8.3}
- Education and training (unless the individual is a student or resident who requires access to provide care) {2.8.4}
- For processing payments. {2.8.5}

✗ Sponsors must not provide access to [the EHR Solution] if access is requested for the purpose of research. {2.9}

✓ If an agent or Electronic Service Provider has multiple roles (e.g. is both a clinician and a risk manager), the Sponsor may assign that person with access to [the EHR Solution] for the purposes of collecting PHI for providing or assisting in the provision of health care and must ensure that the end user understands their permissions and obligations. {2.10}

Network and Operations Standard

Do (✓):

Network Zones

✓ HICs should implement network zones and manage these network zones in a manner that observes the separation of different computing environments. The segregation of networks may be based on criteria, such as: {1.3}

- The classification of information transmitted on the network. {1.3.1}
- The level of assurance required. {1.3.2}

✓ HICs should control traffic between networks zones by using a security gateway at the zones’ perimeter. {1.4}

Security Gateways

- ✓ HICs should implement a process to review security gateway configurations at least annually. The process should ensure the: {1.6}

  - o Review of the rule sets on their security gateways {1.6.1}
  - o Removal of expired or unnecessary rules {1.6.2}
  - o Resolution of conflicting rules, and {1.6.3}
  - o Removal of unused or duplicate objects (e.g. network or computer systems). {1.6.4}

Protection Against Malicious Code

- ✓ Malware detection and repair software or equivalent solution should be implemented on HIC-approved tools, processes and workstations to protect from malicious code. Alternative solutions may include application whitelisting or utilization of thin client implementations which restrict writeable capabilities. Questions regarding the appropriateness of alternative solutions should be directed to the Security lead for [the EHR Solution] which can be put forward to the Connecting Security Committee. {1.20}

- ✓ HICs should keep their malware detection and repair software up-to-date. {1.22}

Physical Security Standard

Do (✓):

- ✓ HICs should ensure that highly sensitive facilities (i.e., buildings or storage areas that house identity provider services and data contribution endpoints) are protected against unauthorized physical access. Methods for preventing physical access may include: {1.2}

  - o Fitting vulnerable doors and windows with locks or bolts. {1.2.1}
  - o Installing and monitoring closed-circuit television (CCTV). {1.2.2}
  - o Employing security guards. {1.2.3}
  - o Installing intruder detection systems on external doors and testing accessible windows regularly. {1.2.4}

- ✓ HICs should ensure that visitors to highly sensitive facilitates are: {1.4}

  - o Permitted physical access only for specific, authorized purposes. {1.4.1}
  - o Monitored by recording arrival and departure times. {1.4.2}
  - o Obliged to wear visitor badges at all times. {1.4.3}
  - o Supervised at all times. {1.4.4}
  - o Made aware of behaviour or actions that are prohibited (e.g., filming or photography). {1.4.5}

References

eHealth Ontario EHR Policy and Standards:

- Information Security Policy
- Acceptable Use of Information and Information Technology Standard
- Access Control and Identity Management Standard for System Level Access
- Local Registration Authority Practices Standard
- Identity Provider Standard
- Business Continuity Standard
- Cryptography Standard
- Electronic Service Providers Standard
- Information Security Incident Management Standard
- Information and Asset Management Standard
- Network and Operations Standard
- Security Logging and Monitoring Standard
- Systems Development Lifecycle Standard
- Physical Security Standard
- Threat Risk Management Standard
- EHR Privacy Policies

Appendices

Appendix A: Approved Cryptographic Algorithms

Algorithm	Minimum Key Length	Appropriate Usage
Symmetric Key Algorithms		
AES	128-bits	Data encryption: • Session • Storage ○ Backup ○ Archival Key encryption: • Session • Storage ○ Backup ○ Archival
Skipjack	80-bits, with 32 iterations	Data encryption: • Session • Storage ○ Backup ○ Archival, < 5 years
Triple DES	112-bits	Data encryption: • Session • Storage ○ Backup ○ Archival Key encryption: • Session • Storage ○ Backup ○ Archival
Asymmetric Key Algorithms		
Elliptic Curve	160-bits	Data encryption: • Session • Storage ○ Backup ○ Archival Digital Signature Key encryption: • Session • Storage ○ Backup ○ Archival Session key establishment
RSA	2048-bits	Data encryption: • Session • Storage ○ Backup ○ Archival Digital Signature Key encryption: • Session • Storage ○ Backup ○ Archival Session key establishment
MACs and Hashes		
AES MAC	128-bits	Message authentication
MD5[3]	128-bits, with 16 iterations	Message authentication and message digest
SHA-1[4]	Not applicable.	Message authentication and message digest
SHA-2	Not applicable	Message authentication and message digest
TDES (Triple DES) MAC	112-bits	Message authentication
Digital Signatures		

[3] All *new* implementations of MACs and hashes must not be based on MD5.

[4] All *new* implementations of MACs and hashes must not be based on SHA-1.

DSA (Digital Signature Algorithm)	1024-bits	Digital Signature
Elliptic Curve DSA	160-bits	Digital Signature
RSA DSA	2048-bits	Digital Signature
Digital Certificates		
X.509 v3 compliant	N/A	Binds a public key with a specific identity.
Key Transport/Agreement Algorithms		
Diffie-Hellman	1024-bits	Digital Session key establishment
Elliptic Curve Diffie-Hellman	160-bits	Digital Session key establishment
Cryptographic Protocols		
TLS 1.1 and higher	N/A	Protocol to authenticate and encrypt communication between authenticated parties.

Appendix B: Incident Severity and Priority Ratings

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 five sessions.	**X**	

Appendix C: Incident Report Details

The following details are required in an information security incident report:

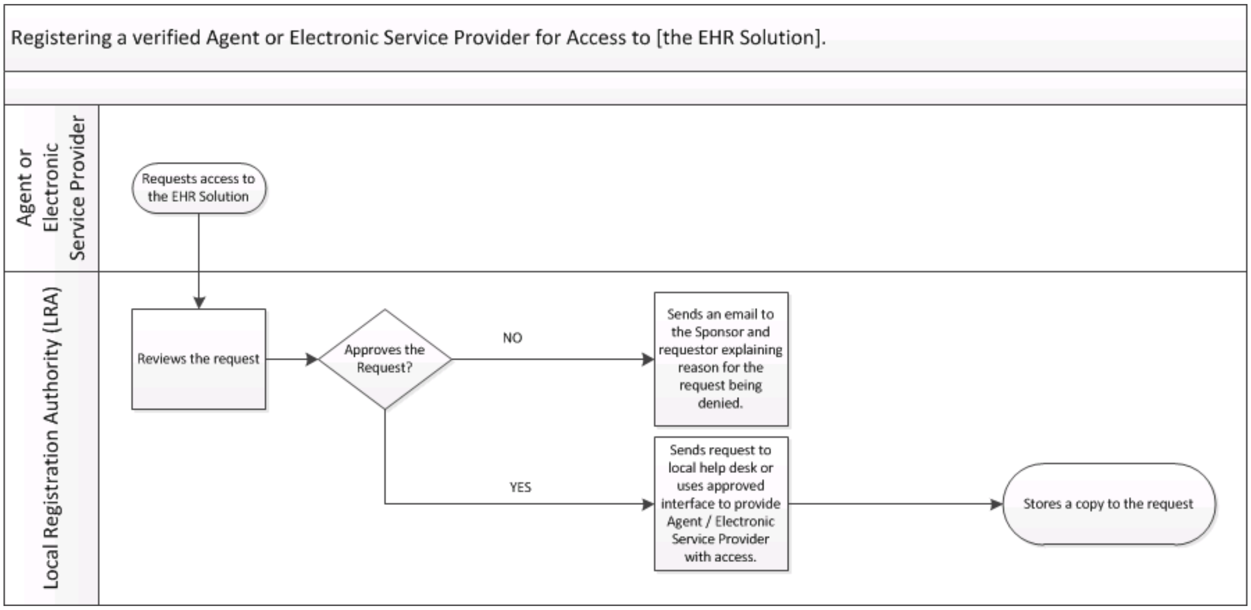
1. Contact Information of the agent or Electronic Service Provider that reported the incident, AND the incident response lead or team
   - Name
   - Unit (e.g. department, division, team) (if applicable)
   - Email address
   - Phone number
   - Location (e.g. mailing address, building and room number)
2. Incident Details
   - Date/time when the incident was discovered
   - Estimated date/time when the incident started
   - Incident ticket number
   - Type of incident (e.g. denial of service, malicious code, unauthorized access, inappropriate usage)
   - Physical location of the incident (e.g. city)
   - Current status of the incident (e.g. ongoing attack)
   - Source/cause of the incident (if known), including hostnames and IP addresses
   - Description of the incident (e.g. how it was detected, what occurred)
   - Description of affected resources (e.g. networks, hosts, applications, data), including information systems' hostnames, IP addresses, and function
   - Operating system, version, and patch level
   - Antivirus software installed, enabled, and up-to-date (yes/no)
   - Mitigating factors
   - Estimated technical impact of the incident (e.g. data deleted, system crashed, application unavailable)
   - Actions performed by the agent or Electronic Service Provider who reported the incident (e.g. shut off host, disconnected host from network)
   - Other organizations contacted (e.g. software vendor)
   - Type of information compromised (if applicable)
3. General Comments[5]
4. Summary of the Incident
5. Contact information for all involved parties
6. Log of containment/mitigation actions taken by incident response lead/team
7. List of evidence gathered
8. Cause of the Incident (e.g. misconfigured application, unpatched host)
9. List of recommended and implemented remediation activities
10. Current Status of the Incident Response

[5] Recommended but not required.

Appendix D: Enrolling an Agent or Electronic Service Provider with Access to [the EHR Solution]

The following is the process for enrolling an agent or Electronic Service Provider with access to [the EHR Solution] where that agent or Electronic Service Provider's identity has already been validated (e.g. via the HIC's on-boarding process). The example below implies a paper based process however an electronic workflow could be used depending on the Identity Provider practices.

Stage	Responsibility	Description
1	Agent or Electronic Service Provider	Requests access to [the EHR Solution]. (HICs may decide the manner in which this is performed, e.g. through a service request or via email directly to LRA). At a minimum, the request should contain the agent or Electronic Service Provider's: • Full Name • Role/Job Title • User ID • Proof of Sponsor's approval • Reason for access
2	LRA	Reviews the request, and if all necessary information is provided, processes the request.
3	LRA	If approved: • Sends the request to the local help desk or utilizes the necessary interface to provide the agent or Electronic Service Provider with access to [the EHR Solution]. If denied: • Sends an email to the Sponsor and Agent or Electronic Service Provider explaining the reason for the request being denied. Stores a copy form request.


Registering a verified Agent or Electronic Service Provider for Access to [the EHR Solution].
Agent or Electronic Service Provider
Local Registration Authority (LRA)
Requests access to the EHR Solution
Reviews the request
Approves the Request?
NO
YES
Sends an email to the Sponsor and requestor explaining reason for the request being denied.
Sends request to local help desk or uses approved interface to provide Agent / Electronic Service Provider with access.
Stores a copy to the request

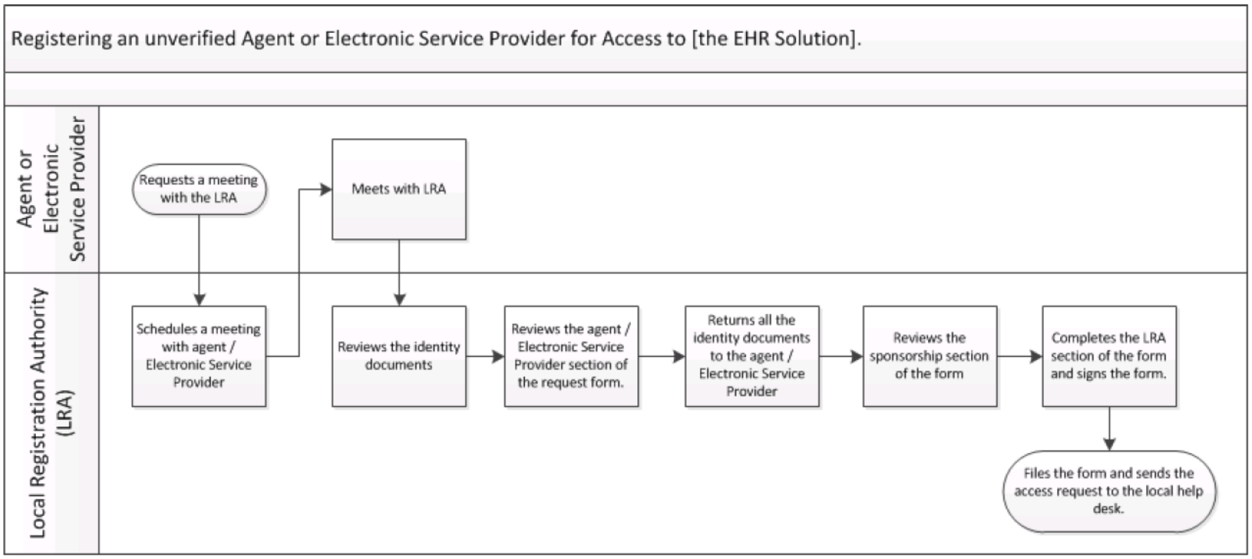
Appendix E: Enrolling an Agent or ESP with access to [the EHR Solution] where the Agent or ESP has NOT already been validated

The following is the process for enrolling an agent or Electronic Service Provider with access to [the EHR Solution] where that agent or Electronic Service Provider's identity has NOT already been validated. The example below implies a paper based process however an electronic workflow could be used depending on the Identity Provider practices.

Stage	Responsibility	Description
1	Agent or Electronic Service Provider	Requests a meeting with the LRA.
2	LRA	Schedules a meeting with the agent or Electronic Service Provider.
3	Agent or Electronic Service Provider	Meets face-to-face with the LRA, bringing a completed and signed [the EHR Solution] End User Enrollment Form (see *Appendix F: [The EHR Solution] End User Registration and Enrollment Form*), along with his/her documents (such as identification, licenses, and disciplines) to the meeting. Alternate processes can be utilized as long as appropriate security measures are in place.
4	LRA	Reviews the identity documents and confirms that: • They are genuine, unaltered, and valid. • They are sufficient to obtain a Level 2 assurance[6]: o At least one is from the primary identity document list (see *Appendix G: Acceptable Identity Documents*). o The other is from either the primary identity document list or secondary identity document list (see *Appendix G: Acceptable Identity Documents*). o At least one includes a photo of the person. o Both show the name of the person. • They are being used by the rightful holder (i.e., the photograph and personal details are those of the person in front of you). ***Note**:* See *Appendix G: Acceptable Identity Documents* for more details on how to validate an agent or Electronic Service Provider's identity Provides the agent or Electronic Service Provider with any relevant training documentation.
5	LRA	Reviews the agent or Electronic Service Provider section of the form for completeness and ensures that: • Combined, the identity documents confirm the core identity information required for e enrollment (i.e., legal name, gender, and date of birth). • Both documents are current. • The first identity document is from the primary identity document list (see *Appendix G: Acceptable Identity Documents*), and the document type, document number, and expiry date (where relevant) are recorded on the form. **Note:** If an Ontario Birth Certificate is used as the primary identity document, it is the certificate number that should be recorded on the form.

[6] For a definition of Level 2 assurance, see the eHealth Ontario Federation - *Identity Provider Standard*.

Stage	Responsibility	Description
		• Only the document type of the secondary identity document needs to be recorded on the form, regardless of whether it is from the primary identity document list or secondary identity document list (see *Appendix G: Acceptable Identity Documents*). • The agent or Electronic Service Provider has signed and dated the form. ** Note – where prior direct or personal interaction between the IDP and the Registrant has taken place to validate the individual's identity has taken place, these steps may be omitted. This direct interaction (e.g. hiring interview) need not be exclusively for the purposes of identity validation, provided that the individual's identity was validated as part of the interaction in accordance to the requirements of the standard.
6	LRA	Returns the all identity documents to the agent or Electronic Service Provider.
7	LRA	Reviews the sponsorship section of the form for completeness and ensures that: • The Sponsor is valid (i.e., on the organization's list of Sponsors, or LRPs). • The Sponsor has signed and dated the form (or provided approval via another means, e.g. email). • An enrollment type is selected in Part 2b – Suspend, Reinstate, Revoke, Enroll New.
8	LRA	Indicates that he/she has reviewed the form and supporting identification by: • Completing the LRA section of the form. • Signing and dating the form.
9	LRA	Files the form and sends a request to the local help desk to provide the agent or Electronic Service Provider with access to [the EHR Solution]. Alternatively, an LRA may have direct access to the entitlement system.


Registering an unverified Agent or Electronic Service Provider for Access to [the EHR Solution].
Agent or Electronic Service Provider
Local Registration Authority (LRA)
Requests a meeting with the LRA
Meets with LRA
Schedules a meeting with agent / Electronic Service Provider
Reviews the identity documents
Reviews the agent / Electronic Service Provider section of the request form.
Returns all the identity documents to the agent / Electronic Service Provider
Reviews the sponsorship section of the form
Completes the LRA section of the form and signs the form.
Files the form and sends the access request to the local help desk.

Appendix F: [The EHR Solution] End User Registration and Enrollment Form

Use this form to enroll an agent or Electronic Service Provider for access to [the EHR Solution]. The example below implies a paper-based process; however, an electronic workflow could be used depending on the Identity Provider practices.

Form Completion Instructions

This form must be completed to enroll each new agent or Electronic Service Provider for access to [the EHR Solution] **if** their identities have **not** already been verified by the HIC in accordance with [the EHR Solution]'s verification requirements. Alternate electronic processes may exist to support this workflow within the IDP.

- The LRA must meet with the applicant to verify their identity documents.
- Complete all fields as specified. Mandatory fields are marked with an asterisk (*). Indicate "Not Applicable" or "N/A" if the field is not applicable.
- The Local Registration Authority must complete Part 3 of the form.
- Once the form is complete, the LRA may enroll the applicant for access to [the EHR Solution].
- The Local Registration Authority must save a copy of the completed form.

Part I - Agent or Electronic Service Provider

1A – Agent or Electronic Service Provider Details

Salutation: ○ Dr. ○ Mr. ○ Ms.	Job Title * *(e.g. CEO, CIO)*	
Legal First Name *	Middle Initial(s)	Legal Last Name *
Business Telephone * *(include ext.)* ( )		Business Email *
Organization Name * *(e.g. University Health Network)*		Site/Location Name *(e.g. ABC Hospital)*
Business Address * *(Number and Street)*		Suite/Unit/Floor
City/Town *	Province *	Postal Code *
System Username or User ID *	Date of Request * *(yyyy-mm-dd)*	

1B – Documents to Support Identity -*To be completed by the **Local Registration Authority**. For privacy reasons, please return the identity document(s) to the agent or Electronic Service Provider and do **NOT** make copies.*

Document 1* - *Provide a document from the primary identity documents list. Recording the expiry date is mandatory for Document 1, if it has one.*

Document Description*	Document Number*	Expiry Date * *(yyyy-mm-dd)*

Document 2* - *Provide a document from either the primary or secondary identity documents lists. Recording the document number and expiry date is not required.*

Document Description*

1C – Notice of Collection-*This section to be completed by the agent or Electronic Service Provider to gain consent for this request.*

I confirm that the details above are correct. I consent to the collection, use, and disclosure of my personal information for the purposes of enrolling for access to [the EHR Solution].

Agent or Electronic Service Provider’s Signature * ____	Date Signed * *(yyyy-mm-dd)*

Part 2 – Sponsor Details

2A – Sponsor Details - This section to be completed by the **Sponsor** or the **Local Registration Authority** on behalf of the sponsor. Specify organization name, location name, and address only if different from the agent or Electronic Service Provider. Contact information (e.g. business telephone and/or business email) must be provided.

First Name *	Legal Last Name *

Title * *(e.g. CEO, CIO)*	Business Telephone * *(include ext.)* ( )	Business Email *

□ Address Same as Agent or Electronic Service Provider *(If checked, the remaining address fields in this section are not mandatory.)*

Organization Name * *(e.g. University Health Network)*	Site/Location Name *(e.g. ABC Hospital)*
Business Address * *(Number and Street)*	Suite/Unit/Floor

City/Town *	Province *	Postal Code *

Part 2b – Type of Request

Type of request: * New Enrollment

Application Role:

*I authorize the agent or Electronic Service Provider's enrollment to [the EHR Solution].

Sponsor’s Signature (if authorization received by other method see below) ____	Date Signed * *(yyyy-mm-dd)*

□ Sponsorship Received via Other Method (e.g. email, memo, fax)	Specify Method:

Part 3 – Local Registration Authority

3A – Local Registration Authority Details - This section to be completed by the **Local Registration Authority**. Specify organization name, location name, and address only if different from the agent or Electronic Service Provider. Contact information (e.g. business telephone and/or business email) must be provided.

First Name *	Legal Last Name *	
Business Telephone * *(include ext.)* ( )	Business Email *	
☐ Address Same as Agent or Electronic Service Provider *(If checked, the remaining Address fields in this section are not mandatory.)*		
Organization Name * *(e.g. University Health Network)*	Site/Location Name *(e.g. ABC Hospital)*	
Business Address * *(Number and Street)*	Suite/Unit/Floor	
City/Town *	Province *	Postal Code *

*I confirm that I have reviewed the agent or Electronic Service Provider's identity documents and this application for enrollment.

LRA's Signature (if authorization received by other method see below) ______________________________	Date Signed * *(yyyy-mm-dd)*

Appendix G: Acceptable Identity Documents

Social Insurance cards and provincial health cards are **NOT** acceptable forms of identification.

Under the Photo and Expiry Dates columns, “Unknown” means that the document may or may not contain a photo or expiry date depending on the origin or version of the document.

Primary Identity Documents

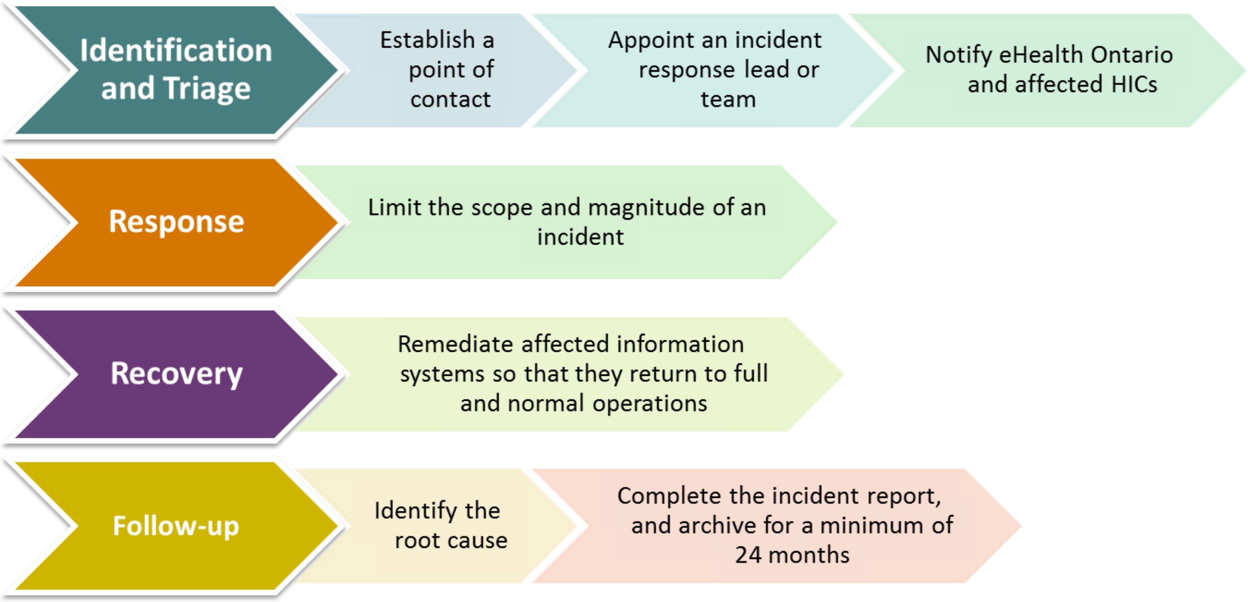
Government Document Type	Photo?	Expiry Date?
Driver’s License (including graduated driver’s license)	Yes	Yes
Canadian Passport	Yes	Yes
Certificate of Canadian Citizenship (paper document or plastic card but excludes commemorative issue)	Yes	No
Birth Certificate issued by a Canadian Province or Territory	No	No
Canadian Certificate of Birth Abroad	No	No
Canadian Certificate of Indian or Metis Status	Yes	No
Canadian Permanent Resident Card	Yes	Yes
Statement of Live Birth from Canadian Province (Certified Copy)	No	No
Certification of Naturalization (paper document or plastic card but excludes commemorative issue)	No	No
Citizenship Identification Card issued by a foreign jurisdiction where these exist (e.g. Mexico, Europe)	Unknown	Unknown
Confirmation of Permanent Resident (IMM 5292)	No	Yes
CANPASS (A Remote Area Border Crossing permit allowing the bearer to cross into Canada at certain remote areas without reporting to a port of entry as long as imported goods are declared)	Yes	Yes
Nexus (A cross-border express pass available to low risk individuals who have passed a stringent Canadian and American security check including a fingerprint biometric, photograph and personal interview with immigration officials. In order to maintain this pass, the individual must reapply every two years.)	Yes	Yes
Firearm Registration License	Yes	Yes
Firearm Registration License	Yes	Yes
A valid Passport issued by a foreign jurisdiction.	Yes	Yes
Immigration Canada - Refugee Claimant ID Document	Yes	Yes
Ontario Photo Card	Yes	Yes

Secondary Identity Documents

Document Type	Expiry Date?
Old Age Security Card	No
Certificate issued by a government ministry or agency, e.g. Marriage, Divorce, Adoption	No
Canadian Convention Refugee Determination Division Letter	No
Canadian Employment Authorization	Yes
Canadian Minister’s Permit	Yes
Canadian Immigrant Visa Card	Yes
Canadian Student Authorization	Yes
Record of Landing (IMM 1000)	Yes
Document showing the registration of a legal change of name accompanied by evidence of use or prior name for the preceding 12 months.	No
Current Registration Document from the College of a Health Profession under the Regulated Health Professions Act, 1991. Audiology and Speech-Language Pathology Chiropody Chiropractic Dental Hygiene Dental Technology Dentistry Denturism Dietetics Massage Therapy Medical Laboratory Technology Medical Radiation Technology Medicine Midwifery Nursing Occupational Therapy Opticianry Optometry Pharmacy Physiotherapy Psychology Respiratory Therapy	Unknown
Current Professional Association License/Membership Card (for any Regulated Health Profession including the following: Association of Ontario Midwives Denturist Association of Ontario Nurse Practitioner Association of Ontario Ontario Association of Medical Radiation Technologists Ontario Association of Naturopathic Doctors Ontario Association of Orthodontists Ontario Association of Speech Language Pathologists and Audiologists Ontario Chiropractic Association Ontario Dental Association Ontario Medical Association Ontario Nurses‟ Association Ontario Opticians‟ Association Ontario Pharmacists‟ Association Ontario Physiotherapy Association Ontario Podiatric Medical Association Ontario Society of Chiropodists Ontario Society of Medical Technologists Registered Nurses‟ Association of Ontario Registered Practical Nurses‟ Association of Ontario Respiratory Therapy Society of Ontario	Unknown
Federal, Provincial, or Municipal Employee Card	Unknown
Current Employee Card from a Sponsoring Organization	Unknown
Union Card	Unknown
Other Federal ID Card, including Military	Unknown
Ontario Ministry of Natural Resources Outdoors Card	Unknown
Judicial ID Card	Unknown
Student Identification Card	Unknown

Document Type	Expiry Date?
BYID Card (Formerly Age of Majority Card)	Unknown
CNIB (Canadian National Institute for the Blind) Photo Registration Card	Unknown
Canadian Police Force Identification Card	Unknown
Blind Persons Right Act ID Card	Unknown

Appendix I: Information Security Incident Management Process


Identification and Triage
Establish a point of contact
Appoint an incident response lead or team
Notify eHealth Ontario and affected HICs
Response
Limit the scope and magnitude of an incident
Recovery
Remediate affected information systems so that they return to full and normal operations
Follow-up
Identify the root cause
Complete the incident report, and archive for a minimum of 24 months

Appendix J: Level of Assurance

Level of Assurance	Information Classification	Description of Level of Assurance
AL1	AL1 is appropriate for information that has a sensitivity level of "unclassified", and is normally used for public information and internal communications, such as internal documents and unclassified communications, normally intended for communication between staff. If compromised, this information could reasonably be expected to cause no significant injury or losses to the parties involved and would require only administrative action for correction. AL1 is insufficient when Personal Health Information (**PHI**) or Personal Information (**PI**) is accessed.	An unverified identity: An individual supplies all identification information, which is taken at face value. No assurance needed as to veracity of identity claim.
AL2	AL2 is appropriate for information that has a high sensitivity level within eHealth Ontario and the health sector environment, and that is intended for use by specific and authorized individuals only. If compromised, this information could reasonably be expected to cause serious injury or financial losses to one or more of the parties involved or would require legal action for correction.	A verified identity: An individual is uniquely identified through a managed registration process and identity claim is verified with documentary evidence, which may be supplemented by contextual evidence in appropriate circumstances.
AL3	AL3 is appropriate for information that is extremely sensitive and of the highest value within eHealth Ontario and the health sector environment. This information is intended for use by named and authorized individuals only. To decide whether an AL3 is required, the Agency and Application Providers shall consider: □ Whether any circumstance(s) or the context surrounding the access or use of the information require(s) additional confirmation of identity than AL2.	A corroborated identity: An individual is uniquely identified through a managed registration process and identity claim is verified and corroborated with authoritative source(s) (e.g. the issuer of the documentary evidence presented).

Copyright Notice

All rights reserved

Trademarks