EHR Security Reference Guide

For Viewing Organizations using ONE ID or ClinicalConnect accounts

Version: 2.4

**Table of Contents**

[Key Terms Defined 4](#_Toc519063950)

[Introduction 6](#_Toc519063951)

[Solution Overview 7](#_Toc519063952)

[Developing your Information Security Program 9](#_Toc519063953)

[Key Roles & Responsibilities 10](#_Toc519063954)

[Getting Connected - Security Steps in Implementation and Adoption 11](#_Toc519063955)

[Quick Reference Guide to the EHR Security Policies 12](#_Toc519063956)

[1. Information Security Policy 12](#_Toc519063957)

[2. Acceptable Use of Information and Information Technology Standard 13](#_Toc519063958)

[3. Cryptography Standard 16](#_Toc519063959)

[4. Electronic Service Provider Standard 17](#_Toc519063960)

[5. Information and Asset Management Standard 18](#_Toc519063961)

[6. Information Security Incident Management Standard 19](#_Toc519063962)

[What is an incident? 19](#_Toc519063963)

[Reacting to an incident 19](#_Toc519063964)

[Roles & Responsibilities 19](#_Toc519063965)

[Four phases of Security Incident Management 20](#_Toc519063966)

[Incident Identification/Triage Details 20](#_Toc519063967)

[Incident Response Details 20](#_Toc519063968)

[Incident Recovery Details 21](#_Toc519063969)

[Incident Follow-up Details 21](#_Toc519063970)

[Evidence Gathering 21](#_Toc519063971)

[7. Local Registration Authority Practices Standard 22](#_Toc519063972)

[a. Registration Authority 22](#_Toc519063973)

[b. Legally Responsible Person (LRP) 22](#_Toc519063974)

[c. Local Registration Authority (LRA) 22](#_Toc519063975)

[d. Sponsor 23](#_Toc519063976)

[Sponsoring Clinical Access 23](#_Toc519063977)

[Sponsoring Administration Access 23](#_Toc519063978)

[Re-enrollment 23](#_Toc519063979)

[No access for Research Purposes 23](#_Toc519063980)

[Enrolling users in multiple roles 23](#_Toc519063981)

[8. Network and Operations Standard 23](#_Toc519063982)

[Network Zones 24](#_Toc519063983)

[Security Gateways 24](#_Toc519063984)

[Protect Against Malicious Code 24](#_Toc519063985)

[9. Physical Security Standard 24](#_Toc519063986)

[Hazard Protection 25](#_Toc519063987)

[Appendix A: Resource Index 26](#_Toc519063988)

[Appendix B: Confidentiality Agreement SAMPLE 28](#_Toc519063989)

[Appendix C: Information Security Incident Report TEMPLATE 29](#_Toc519063990)

[Appendix D: Information Security Policy SAMPLE 29](#_Toc519063991)

[Appendix E: Electronic Service Provider List TEMPLATE 29](#_Toc519063992)

[Appendix F: Incident Workflows 30](#_Toc519063993)

[Appendix G: Role Definitions & Responsibilities 32](#_Toc519063994)

# Key Terms Defined

| Term | Definition |
| --- | --- |
| Assurance Level 2 (AL2) | A Level of Assurance refers to the level of confidence that can be placed in an identity claim.  Assurance Level 2 is required 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.  Specific requirements are found at:  [***https://www.ehealthontario.on.ca/images/uploads/services/resources/eHealth\_Ontario\_Federation\_Identity\_Provider\_Standard.pdf***](https://www.ehealthontario.on.ca/images/uploads/services/resources/eHealth_Ontario_Federation_Identity_Provider_Standard.pdf) |
| Cryptography/ Encryption | Involves arranging ordinary text in a form that cannot be read by unauthorized people. This is referred to as encryption; the data is, in effect, locked prior to being transmitted; and then decrypted or unlocked only by an authorized individual. |
| Cryptographic key or key component | Used to arrange ordinary text into cryptographic text to decode cryptographic text to ordinary text. Often a password is applied to encrypt (lock) or decrypt (unlock) the data. In many cases, this key must remain private to ensure security of the data. HICs must ensure that each cryptographic key or key component has the fewest number of key custodians necessary. |
| Key custodian | An Agent or Electronic Service Provider who has been authorized to handle all or part of a cryptographic key throughout the key’s lifecycle from creation to destruction. |
| Information security incident | 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. |
| 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, standards, 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. |
| [The EHR Solution] | The term [The EHR Solution] is used to describe the solution and supporting systems that enable electronic PHI to be stored and made available to HICs. Supporting systems may include those that are subcontracted or leveraged in electronic service provider relationships. This does not include any participating HIC’s information systems or information technologies where they act in a Health Service Provider role.  Within [the EHR Solution] includes Provider Portal components used by healthcare providers to facilitate patient care, as well as Administrative Portal components used by individuals to manage administrative components such as Privacy Reporting, Consent Management, error queue management, etc. |
| Viewing Site | An organization that views data from [the EHR Solution] in accordance with the authorized permitted purposes. The organization accesses 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. |

# Introduction

This guide is intended for use by you, the health information custodian, to assist in understanding and managing the security requirements of connecting your community-based offices to [the EHR Solution], while ensuring Personal Health Information (PHI) is safeguarded and handled in an appropriate manner. It introduces the overall process of getting connected, what the solution looks like, who is involved and what roles each play, as well as how to manage your continued participation as it relates to information security.

A large part of this guide summarizes the EHR Security Policy and its Standards vital to help protect the confidentiality, integrity, and availability of personal health information (PHI) stored in or processed by [the EHR Solution]. It offers examples and tips on how your organization can implement and comply with the Policy and Standards. Refer to EHR Security Policies for Viewing Sites for detailed requirements.

Security of the EHR is important to minimize the chance of a data breach and upholding it demonstrates your organization’s commitment to the people of Ontario. This means implementing best-practice policies, standards, and controls to protect personal health data. Attesting that your organization complies with the Policy and Standards means that these have been implemented and communicated the staff to follow, now and in the future. Participating organizations all have a responsibility to each other to protect patient data when participating in the electronic health record solution.

# Solution Overview

[The EHR Solution] makes information from external health care organizations available to authorized representatives at your organization. The solution provides a web-based portal that allows an end user to search for a patient and access data. *Figure 1* shows the web-based portal of ConnectingOntario, as an example.

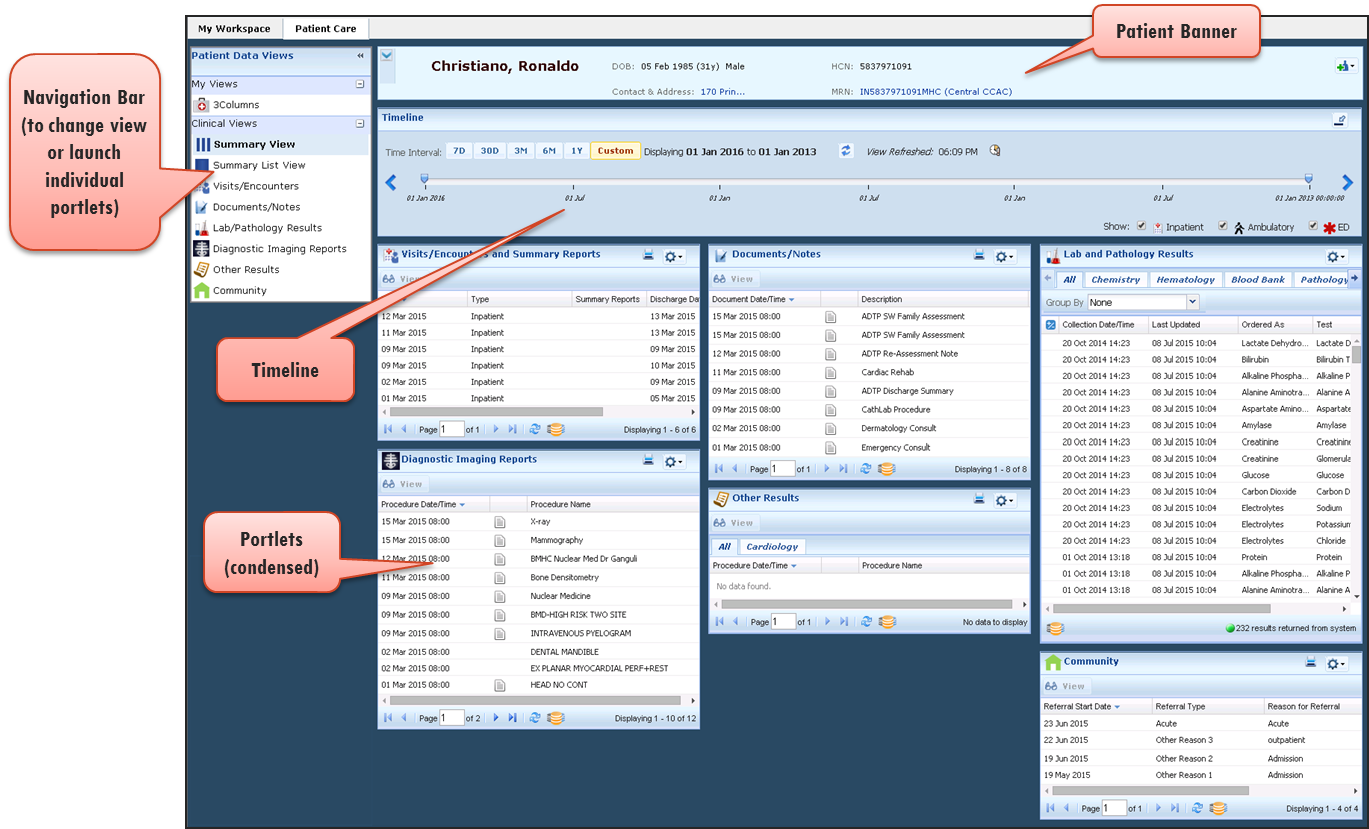


Figure 1. [the EHR Solution] portal

The ClinicalConnect Viewer is also shown in *Figure 2* for illustrative purposes.

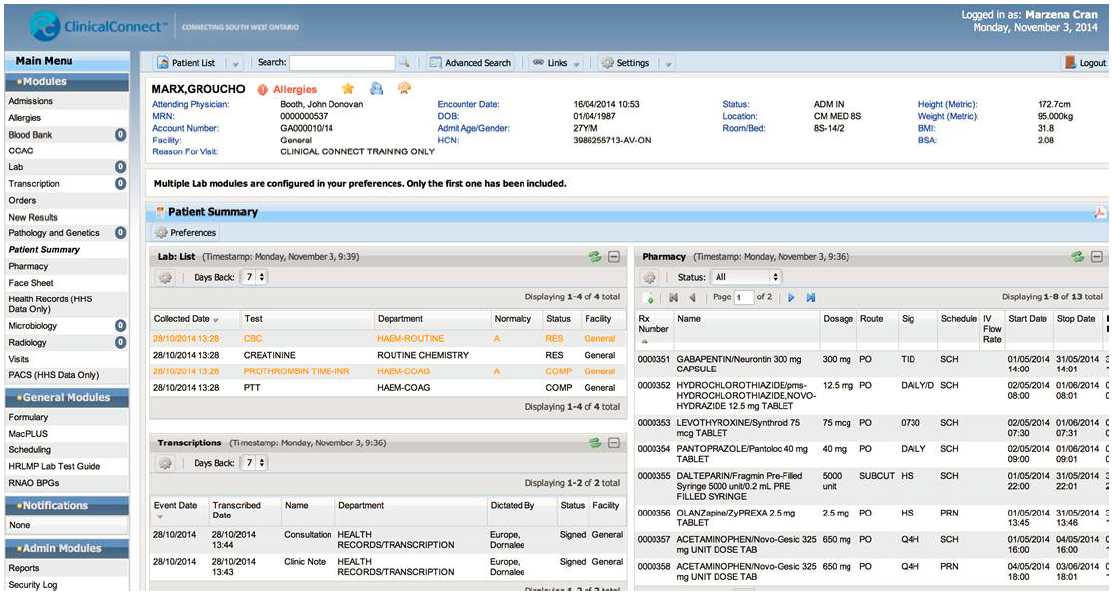


Figure . ClinicalConnect Viewer

# Developing your Information Security Program

The Personal Health Information Protection Act, 2004 (PHIPA) is Ontario’s health-specific privacy legislation. PHIPA governs the manner in which personal health information (PHI) may be collected, used, and disclosed within the health care system. While all staff plays a role in information protection, PHIPA makes Health Information Custodians (HICs) and their Agents responsible for information security.

You may need to develop or enhance an information security program within your office to support your organization’s compliance with the EHR Security Polices and participation in [the EHR Solution]. This means assessing the way you currently address security-related issues and applying best practices to them. Document and distribute these agreed-upon practices to everyone on your team.

When we speak about information security, it is generally centered on protecting sensitive information (e.g., PHI, passwords) and processes such as sensitive email communications, user registration, and security incident reporting. It is useful to remember these core principles when considering information security:

• **Confidentiality** – ensuring that sensitive information is made available or disclosed only to authorized individuals and remains confidential during its lifecycle.

• **Integrity** – making certain that sensitive information is accurate, complete and remains valid during its lifecycle.

• **Availability** – ensuring information is accessible to authorized individuals, when and where required.

Building an information security program requires that your organization develop a security policy; define roles and responsibilities for information protection; ensure that all staff are trained; monitor compliance with the Policy and its Standards; and be prepared to deal with unexpected incidents.

Review the roles integral to creating a security program, listed in *Figure 2* and consider who within your organization is the most appropriate individual or group to be responsible for those functions. *Table 2* in *Appendix G: Role Definitions & Responsibilities* outlines the roles in more detail.

# Key Roles & Responsibilities

Key HIC roles inherent to building an Information Security Program and managing your organization’s participation in [the EHR solution] are defined in *Figure 3*.Information Security best practices include the designation of individuals with these roles and responsibilities to ensure that information assets under their care are adequately protected and supporting security processes are followed. In community-based offices, there are several roles relevant to the Information Security Program and protection of sensitive information, and in some cases, the same person may play multiple roles.

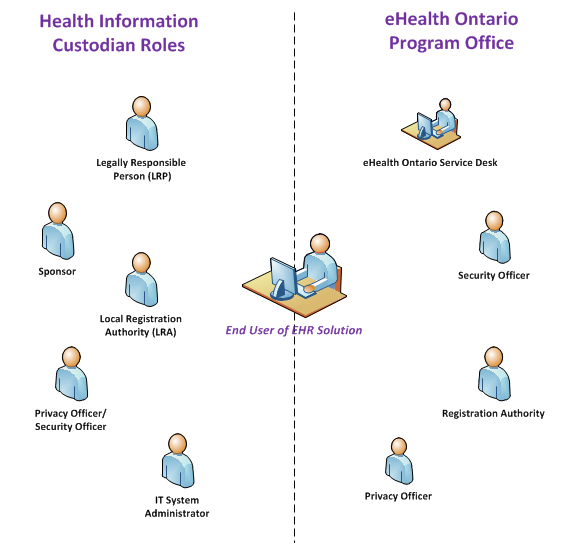


Figure 3. HIC Roles & Responsibilities

# Getting Connected - Security Steps in Implementation and Adoption

The ConnectingOntario Security team has developed steps involved in getting connected, as shown in *Figure 4*:



Figure 4. Steps in Getting Connected

The high-level process for the Viewing Site is summarized as follows:

* Attend or review the Security Webinar that provides a plain language overview to prepare for your organization’s participation in [the EHR Solution].
* Complete or refresh the registration training available. It is recommended that key roles who are involved in completing the Security Assessment (i.e., Privacy/Security Officer, Local Registration Authority) take the Privacy and Security training courses first before starting the Security Assessment.
* Complete the Security Assessment which measures your organization’s compliance and identifies gaps.

Declare any area of non-compliance in your signed EHR Security Assessment form.

# Quick Reference Guide to the EHR Security Policies

There are nine EHR Security Policies used as the basis for preparing a HIC for connection to [the EHR Solution] in a *Viewing* role; these can be found in the all-in-one *EHR Security Policies for Viewing Sites* document.

Presented in this section is a high-level summary of each of theEHR Security Policies.

**EHR Security Policy and Standard Listing for View Only Sites**

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

## Information Security Policy

An information security program is anchored in an Information Security Policy. The Information Security Policy is a document available to all staff which outlines the roles, responsibilities and expectations for security within your organization.

Your organization may already have an existing Information Security Policy; if so, review the requirements of the EHR Security Policies and determine if there are any gaps that may need to be addressed. For example, your existing Information Security Policy may need to be amended to list shared systems as part of its scope. If your organization does not have an Information Security Policy, consider using the [*Sample Information Security Policy*](#_Appendix_D:_Information)as your organization’s policy.

You may also need to refresh your internal privacy and security training. If your organization does not have privacy and security training, consider using the [*ConnectingOntario Privacy and Security Training Modules*](http://www.ehealthontario.on.ca/en/initiatives/resources) in whole or in part.

Ensure that you have formally assigned roles under the policy to individuals within your practice. See *Figure 2* for a list of HIC roles and *Table 2* in *Appendix G: Role Definitions & Responsibilities* for more details. Where changes in your organization affect compliance with the EHR Security Policies, such changes must be communicated to [the EHR Solution] Program Office Privacy and Security Team.

## Acceptable Use of Information and Information Technology Standard

The Acceptable Use of Information and Information Technology Standard outlines the requirements for users, whether they are a Clinician, Local Registration Authority, Security Officer, etc. The behaviour-based requirements are included in the [*ConnectingOntario Privacy and Security Training Modules*](http://www.ehealthontario.on.ca/en/initiatives/resources). When users first log on to [the EHR Solution], and annually thereafter, they will be asked to acknowledge the terms of an [*End-user Agreement*](http://www.ehealthontario.on.ca/images/uploads/regional_partners/EHR_Portal_User_Agreement_En.pdf) which will bind them to commitments made by your organization. The agreement will require them to confirm that they have completed training and will abide by the terms of the agreement.

A subset of technical requirements are included in the standard which can be implemented by your IT Service Provider (i.e., configuring acceptable HIC-approved tools permitted to access [the EHR Solution]; disk encryption on mobile machines; antivirus software; configuring passwords on end user workstations, etc.). See *Table 1* for controls to comply with regarding user accounts and passwords and general controls in *Table 2*.

Table 1. Account Usage and Password Controls

| **Account Usage and Password Controls** | |
| --- | --- |
| **Do** | **Examples / Notes** |
| HICs, their Agents and Electronic Service Providers must always use assigned credential to access [the EHR Solution]. | Includes the following criteria:   * Never share or borrow credentials. * All persons are accountable for any actions performed on [the EHR Solution] with their ID. |
| Create strong, hard-to-guess passwords & keep your password a secret! | “IL0v3EatingP!zza1” |
| Use phrases when creating your password.  Passwords must be eight characters long, containing at least three of the following:   * One number * One uppercase letter * One lowercase letter, or * One special character | “IL0v3EatingP!zza1” |
| Commit your password to memory—only record it if it can be stored securely. | Write only the password down on a piece of paper and lock it in your desk drawer; do not include the user ID. |
| Always change passwords used to participate in [the EHR Solution] at initial login. | In situations where a user is provided with a temporary password as part of the account creation or password reset process, the user must immediately change their password on logging into the system. |
| **Do not** | **Examples / Notes** |
| Use all or part of your ID, personal information, three consecutive characters, or change passwords to a recognized pattern. | * Birthdays, hobbies, “AAA”, pet names * Do not change “IL0v3EatingP!zza1” to “IL0v3EatingP!zza2” |
| Use passwords which are the same as other accounts. | Do not use the same passwords as your Hotmail, Gmail, Online Banking, etc. |
| Allow another person to use your credentials (IDs and passwords) to access [the EHR Solution]—no sharing—you are accountable for any actions tracked to your login account! | |
| Include your ID or password in any automated single sign-on process except if you have an approved SSO management system**.** | Do not store ID or password in a macro or function key; Do not allow your browser to store or remember you password. |

Table 2. General Controls when using the EHR Solution

| **General Controls when using the EHR Solution** | |
| --- | --- |
| **Do** | **Examples / Notes** |
| Access [the EHR Solution] only when and how your role requires you to do so. | You are only allowed to use the system to provide or assist in the provision of health care. Do not access the system to snoop for information about, friends, family, neighbours, famous persons, etc., and do not use it to look up information about yourself. |
| Use only HIC-approved devices or processes to participate [the EHR Solution]. | Computers, laptops and mobile devices which have been reviewed by the HIC and configured to follow the secure practices (i.e., disk encryption for remote machines, strong passwords required on start-up, antivirus configured, up to date system) |
| Only store the minimum amount of PHI necessary on a mobile/portable device.  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. | The solution allows users to download PHI to their local machines. This may also be done by the user unknowingly. For example, in some instances, in order to view a PDF or image certain browsers download a local copy onto the machine. Users should be advised to regularly clean out their browser’s “downloads” or “temporary files” folder in order to remove these files.  Encrypt or password-protect specific folders or files where PHI is stored on mobile machines. Full disk encryption is the preferred option. |
| Emails containing PHI must be encrypted and sent using a secure approved file transfer solution or email system. | ONE MAIL can be used to securely send sensitive information to [the EHR Solution] Program Office or other ONE MAIL users; otherwise, encryption must be applied when sending sensitive information over email. Microsoft Office allows for documents to be encrypted using a strong password; other third party software such as WinZip can be used to apply a password to sensitive information in an attachment. Ensure the password to decrypt the data is communicated over a different channel (i.e., telephone). |
| When connecting to [the EHR Solution] remotely, (i.e., connecting from outside the HIC’s local network), a HIC-approved remote access solution must be used. | The HIC must designate appropriate devices to be used, such as those configured with disk encryption, strong passwords, antivirus, up to date system. Alternate methods can be used, such as terminal services / Citrix which can be configured to keep data on the local system. The technical specification provides further direction as to recommended and minimum configurations (see [*Configuration Requirements for ConnectingOntario*](https://www.ehealthontario.ca/portal/server.pt/gateway/PTARGS_32_55520_217_0_-1_47/http%3B/wcicollab.phportal.prod.ont.gss%3B11930/collab/docman/download/259158/0/0/0/CO_Configurations%20Requirements%20.pdf)). |
| When disconnecting from a remote connection, properly disconnect, rather than simply closing the application. | Log out of the application rather than only closing the window. |
| **Do not** | **Examples / Notes** |
| Disable, bypass or override any information security controls. | Virus protection is an example of a security control which should not be bypassed. |
| Do something that you know will interfere with the system’s normal operations or the integrity of the data processed by the system. | |
| Attempt to exploit a known or suspected security weakness. | |
| Use your personal email to send, or receive PHI. | Those used for personal banking, email, shopping, etc. (e.g., Gmail, Hotmail, BestBuy, etc.). |
| Leave a computing device in public places or in your car in plain view – take it with you or lock it in your trunk. | |
| Share PHI with anyone except as authorized and required for your job. | |
| Discuss or access PHI in public places where others may see the information. | |
| Leave your login open and unattended. | Log off or lock your computer if you have to leave it. |
| Take a picture of data displayed on [the EHR Solution]. | |

## Cryptography Standard

To protect the confidentiality and integrity of PHI that is accessed through [the EHR Solution], you as the HIC, must understand and employ cryptographic solutions on your relevant information systems. This means ensuring that incoming and outgoing electronic data on your systems is encrypted (locked), so that in the event that this information is intercepted or compromised, the data will remain protected.

There are a few common places where encryption is used:

* **Hard Drive of HIC-Approved Tools** –Encrypt the disk drive of mobile/portable HIC-approved tools used by end users to participate in [the EHR Solution]. The solution allows end users to download PHI to their computer and in some cases, such as when viewing a report or image, this may be done without the user’s knowledge. Therefore, it is important to ensure the disk is encrypted with an adequate encryption algorithm and strong password in the event it is lost or stolen.
* **Email** – Use encryption when emailing sensitive data to [the EHR Solution] Program Office to support privacy or security correspondence. This can be implemented by using the ONE MAIL solution which automatically encrypts data in transit to other ONE MAIL users or by using built-in encryption features of Microsoft Office (File Menu 🡪 Info Menu 🡪 Protect Document). Ensure that end users select a strong password to encrypt the contents of the document. Passwords should not be sent via email, but through other means, such as telephone.
* **Browsers** – The HIC-approved tools (i.e., computers) will automatically establish an encrypted session with [the EHR Solution] when browsing its website. It is important to use an up-to-date Operating System and Internet Browser on your HIC-approved tool that can utilize the most current encryption mechanisms to best protect the data in transit between your computer and [the EHR Solution].
* **Network Devices** –A HIC may also offer a wireless network (WIFI) for its users. It is important to configure the wireless network to use a current encryption algorithm to protect data from being intercepted.

Only use [the EHR Solution]-approved cryptographic algorithms with [the EHR Solution]. A list of approved cryptographic algorithms can be found the [*All-in-one EHR Security Policies for Viewing Sites*](http://www.ehealthontario.on.ca/images/uploads/support/EHR_All_Security_Policy_for_Viewing_Organizations_EN.pdf) document.

Organizations need to ensure that they are using the appropriate strength of encryption and managing the “keys” (i.e., passwords) used to decrypt information.

## Electronic Service Provider Standard

Organizations may leverage an Electronic Service Provider (ESP) to provide services which supports their participation in [the EHR Solution]. Examples may include but are not limited to:

* Local desktop, laptop, device support
* Network connectivity support

ESPs must protect and maintain confidentiality, integrity, and availability of systems and services which support the HIC’s participation in [the EHR Solution]. The HIC’s responsibilities with regard to the ESP are outlined in *Table* 3.

Table 3. HIC responsibilities for ESP

| **HIC Responsibilities** | **Examples** |
| --- | --- |
| Maintain a list of support contracts, agreements, and service levels for all providers of electronic services. | Define and document all information systems and services to be provided by a new ESP, or on renewal of service agreements for all application service providers, network service providers, storage service providers, etc. |
| Maintain formal documentation (e.g., contracts, agreements and service levels). | * Require agreements, contracts which specify the technical and organizational relationship covering the ESP roles and responsibilities under the PHIPA legislation and under the HIC’s privacy and information security policies, standards, and procedures. * Roles and responsibilities for implementing, maintaining and supporting the information systems or services that the ESPs are required to fulfill. * Service goals (e.g., the dates and times when the service is required). * Expected deliverable (e.g., break/fix support). * Document representatives of Electronic Service Providers (i.e., subcontractors). |
| Assess the potential information security and privacy risks posed by a new ESP prior to engaging in a contractual relationship with that ESP. Identify mitigation plans for any risks identified. | |
| Establish a consistent method for handling the termination of relationships with ESPs. | * Designating agents responsible for managing the termination * Revocation of physical and logical access rights to the organization’s information, and * Secure return, transfer or destruction of all assets (e.g., back-up media storage, documentation, hardware, and authentication devices). |
| Require a new ESP to implement applicable security and privacy controls prior to the ESP being granted access to [the EHR Solution]. | |

## 

## Information and Asset Management Standard

Ensure that PHI 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 with encryption, using HIC-approved tools, etc.).

For example, during a security or privacy incident, you may be required to communicate sensitive information to [the EHR Solution] Program Office. This must be done in a secure manner by applying encryption (see [*All-in-one* *EHR Security Policies for Viewing Sites*](http://www.ehealthontario.on.ca/images/uploads/support/EHR_All_Security_Policy_for_Viewing_Organizations_EN.pdf)If email is used, ONE Mail is an acceptable method to communicate PHI, as it automatically provides encryption in transit to other ONE Mail users.

If your organization does not use ONE Mail, you can request access by contacting the eHealth Ontario Enterprise Service Desk or apply encryption to the data in transit, either through a strong password in a MS Office document (*File Menu 🡪 Info Menu 🡪 Protect Document)* or by using other third party tools. Ensure that the password is communicated in an out-of-band method (i.e., telephone). See password requirements in the *Acceptable Use of Information and Information Technology Standard* section of the [*All-in-one* *EHR Security Policies for Viewing Sites*](http://www.ehealthontario.on.ca/images/uploads/support/EHR_All_Security_Policy_for_Viewing_Organizations_EN.pdf).

## Information Security Incident Management Standard

### What is an incident?

An incident is 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.

Examples may include:

* The unauthorized disclosure, destruction, modification, or withholding of information
* A failure to comply with the organization’s security requirements
* Unauthorized access, use, or probing of information resources
* An attempted, suspected, or actual security compromise
* Waste, fraud, abuse, theft, loss of or damage to computing resources

### Reacting to an incident

Organizations must implement an information security incident (“incident”) management process to:

* Quickly and effectively identify and resolve incidents
* Minimize incident impact
* Reduce the risk of similar incidents from occurring

These phases are described in the Information Security Incident Management Standard as:

1. Identification/Triage
2. Response
3. Recovery
4. Follow-up

**Note**: The EHR Privacy Policies also require sites to implement a privacy breach management policy. In cases where there is a breach of PHI, the privacy breach management process takes precedence and must be followed.

### Roles & Responsibilities

* **Point of contact** - Individual or team to which actual or suspected incidents are reported. This may be your local Service Desk, an Office Manager, or other individual designated by your organization. The point of contact may be the same as the Incident Response Lead.

* **Incident response lead or team** - Initiates the triage, response, recovery, and follow-up activities for incidents. The incident response lead or team may be the same as the point of contact. The response team may include the IT Service Provider or an Electronic Service Provider who is tasked with incident management functions.
* **[the EHR Solution] Program Office Privacy and Security Operations Team** –The privacy and security team typically consisting of [the EHR Solution]’s Agents who support security incident functions in an effort to coordinate activities and notifications among HICs and other stakeholders.

### Four phases of Security Incident Management

#### Incident Identification/Triage Details

|  |
| --- |
| * Immediately report suspected or confirmed information security incidents to the point of contact at your site (i.e., a help desk or Privacy/Security Officer). This contact might also be your manager or supervisor, who in turn must report it to the information security incident initial point of contact.   **Point of contact:**   * Generates an incident ticket or log for all reported incidents. Minimum information elements include: * Time and date of the reported incident * Name and contact information of the agent or ESP that reported the incident * Incident details (e.g., type, how it was detected) * Impact and any actions undertaken to contain the incident * Sends all incident tickets to the incident response lead to verify whether or not an incident has occurred. |
| **Incident response lead or team:**   * Classifies and prioritizes all actual incidents according to severity. * Initiates an incident report related to [the EHR Solution] Program or [the EHR Solution]. * Notifies [the EHR Solution] Program Office Privacy and Security Team and any affected HICs by the end of the next business day of confirmed incidents that are classified as Severity 1 or Severity 2. Includes minimum notification elements. * If an incident affects multiple HICs or [the EHR Solution], [the EHR Solution] Program Office Privacy and Security Team may assume leadership of the incident management activities and/or notifications to other HICs. * [the EHR Solution] Program Office Privacy and Security Team will notify the Connecting Security Committee and/or the Applicable Oversight Body within **72 hours** of notification for any incident. |

#### Incident Response Details

|  |
| --- |
| **Incident response lead or team:**   * Tries to limit the scope and magnitude of an incident. Mitigation activities may include: * Backing up the information system * Discontinuing operations * Changing passwords or modifying access control lists on the compromised information system * Restricting connectivity * Depending on the severity of an incident it may be necessary to activate the organization’s business continuity plans. |

#### Incident Recovery Details

|  |
| --- |
| **Incident response lead or team:**   * Remediates affected information systems so that they return to 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 * Monitoring information systems to verify normal operations without further information system or data compromise |

#### Incident Follow-up Details

|  |
| --- |
| **Incident response lead or team:**   * Investigates incidents to identify the cause of the incident (e.g., by performing a root cause analysis). * Once an incident has been resolved (e.g., all remediation activities have been implemented and affected information systems and technology has returned to full and normal operations), the incident response lead or team must complete the security incident report. Regular status updates may be requested and required depending on the length of an investigation. * Archives incident reports for a minimum of 24 months. * Provides [the EHR Solution] Program Office and any other impacted HICs with an incident report within 72 hours of the incident report being requested. * Sends final incident reports for review to [the EHR Solution] Program Office Privacy and Security Team so that they can be presented to the Connecting Security Committee, and if necessary, the Applicable Oversight Body. * Implements a mechanism to review security incidents which occur at your organization’s location, at a minimum, monthly to identify trends. This will help determine whether any preventative actions can be taken to reduce the likelihood of similar incidents from occurring in the future. |

#### Evidence Gathering

|  |
| --- |
| **Incident response lead or team:**   * Develops procedures for collecting evidence for the purposes of disciplinarily or legal action against agents or ESPs. |

1. A Security Incident Management Template is available to help document the required details of a security incident and can double as the final report to satisfy the standard requirements. Refer to *Appendix F: Incident Workflows* for two different ways to process incidents, depending on whether other HICs are involved or not.

## Local Registration Authority Practices Standard

This standard ensures the appropriate and secure enrollment of users and agents authorized to access [the EHR Solution]. There are four roles involved:

1. Registration Authority (RA)
2. Legally Responsible Person (LRP)
3. Local Registration Authority (LRA)
4. Sponsor

### Registration Authority

A top level entity that has overall accountability for a network of organization’s providing registration and identity management functions. This entity is responsible to work with Legally Responsible Persons (LRP) at HIC locations to register Local Registration Authorities (LRAs). [The EHR Solution] or its delegate acts 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/or identity management system (e.g., The ONE ID Program acts as the Registration Authority for users of ONE ID).

### Legally Responsible Person (LRP)

The LRP is 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 processes. The LRP signs the legal agreements on behalf of an organization. If your organization will use ONE ID to connect to [the EHR Solution], your LRP has the option to delegate their responsibilities to another individual by submitting an LRP Delegation Form (from the [ONE ID Implementation Package)](https://www.ehealthontario.ca/portal/server.pt/gateway/PTARGS_0_95092_17880_717_89964_43/docman/download/205100/0/0/0/ONE%20ID%20Implementation%20Package.pdf) to eHealth Ontario.

The LRP is the only one within the HIC site who has the authority to modify a LRAs status. The exception is if you are a ONE ID user, eHealth Ontario's ONE ID team, acting as the RA, may revoke a LRAs status.

The LRP identifies at least one or more persons to act as LRA to manage the enrollment of its agents and ESPs who require access to [the EHR Solution]. The LRP also identifies at least one or more persons, groups or roles to acts as a Sponsor to approve access by Agents to [the EHR Solution].

### Local Registration Authority (LRA)

The LRA is responsible for managing the enrollment of users, to ensure that users are enrolled correctly and have passed the necessary due diligence prior to being given access (e.g., training, approved by a valid Sponsor, identity proofing).

LRAs must take the LRA training course and be registered according to the Assurance Level 2 (AL2) requirements of the Standard. ONE ID LRAs have been registered to the AL2 requirements.

For ONE ID users, LRA nominations must be submitted by the LRP (or their Delegate) to eHealth Ontario. Refer to the LRA Nomination Form (from the [ONE ID Implementation Package](https://www.ehealthontario.ca/portal/server.pt/gateway/PTARGS_0_95092_17880_717_89964_43/docman/download/205100/0/0/0/ONE%20ID%20Implementation%20Package.pdf)).

In granting access, the LRA must validate the identity of the user. It is possible to leverage previous Human Resource records for this so as to eliminate the need for face-to-face validation; however, there must a record of the original identity validation.

### Sponsor

#### Sponsoring Clinical Access

The Sponsor has the authority to grant access to the solution in accordance to the Local Registration Authority Practices Standard. The Sponsor must only provide access to clinical components for users whose purpose of access is to collect PHI for providing or assisting in the provision of healthcare. 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
* Residents providing care to patients
* Administrative staff who pull charts for physicians
* Ward clerks who review and flag abnormal results for physicians

#### Sponsoring Administration Access

The Sponsor must only provide access to administration components of [the EHR Solution] for users and ESPs whose purpose of access is to provide support for defined and permitted functionality within the administration roles of [the EHR Solution] (e.g., Privacy Officers, System Administrators).

#### Re-enrollment

If a user has had their access revoked, they must re-enroll into the service to get access. Although the individual may have had their identity validated, they must receive approval from the Sponsor to gain access again; this record must be tracked. Organizations leveraging ONE ID should refer to *Registration Support and Maintenance, Section 7* of the [*LRA Procedures Manual*](file:///C:/Users/mark.carter/Documents/InfoSec/Connecting%20Ontario/Task%20Force/Plain%20Language/PTARGS_0_95092_17880_717_89964_43/docman/download/205100/0/0/0/ONE%20ID%20Implementation%20Package.pdf) for complete descriptions of the Revoke, Suspend, and Reinstate processes.

#### No access for Research Purposes

Sponsors must not provide access to the HIC, or its agent or ESP, if access is requested for purposes other than providing or assisting in the provision of healthcare e.g. providing access for the purposes of:

* Program planning, evaluation, or monitoring
* Risk or error management
* Improving the quality of care, programs, and services
* Education and training (unless the individual is a student or resident who requires access to provide care)
* For processing payments
* Research

#### Enrolling users in multiple roles

An agent or ESP might have multiple roles (e.g., both a clinician and a risk manager). The Sponsor may assign that person with access 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.

Follow the specific procedures established by the ONE ID Program for registration and enrollment.

Note that Data Sharing Agreements with HICs of the data indicate that access can only be provided for specific purposes.

## Network and Operations Standard

This standard is concerned with the way information is accessed and transmitted between computing devices and the network. Controls must be implemented to secure your network infrastructure, and procedures established to secure the management and operation of your identity provider services and data contribution endpoints. You may need to contact your Electronic Service Provider for more information and help.

### Network Zones

With access to PHI comes the responsibility to prevent unauthorized users from accessing it. All networking devices (e.g. firewalls, routers, and switches) must be deployed in such a way as to segregate your internal network from the Internet or other untrusted networks. This is referred to as implementing network zones, which securely separate 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

One way to protect your network zone is to offer a Guest network (e.g., free wifi) for patients and other visitors. This should be separate from your office’s network to prevent unauthorized individuals from accessing the data there.

Further separation may be desirable if, for example, office space is sub-contracted to another entity. In this case, the networks should be separate to ensure a trusted environment is used to access the EHR solution.

### Security Gateways

The traffic between network zones (e.g., guest network, office network) should be separated by a security gateway which typically is a firewall with specific rules configured to protect the network. Typically, a firewall would be deployed with configurations to protect the internal computers from threats.

Review your organization’s security gateway configurations at least annually. The process should ensure that:

* Network rules (permitted/denied) are legitimate
* Unnecessary, expired, or conflicting rules are analyzed and adjusted
* Duplicate or obsolete network objects (e.g., computers) are removed

See [*Configuration Requirements for ConnectingOntario*](https://www.ehealthontario.ca/portal/server.pt/gateway/PTARGS_32_55520_217_0_-1_47/http%3B/wcicollab.phportal.prod.ont.gss%3B11930/collab/docman/download/259158/0/0/0/CO_Configurations%20Requirements%20.pdf) for more details.

### Protect Against Malicious Code

Malware detection and repair software tools (e.g., antivirus software) or equivalent solution:

* Implement these tools on HIC-approved tools, processes, and workstations that are used to access [the EHR Solution] to protect PHI from malicious code which may compromise the data.
* Keep antivirus software up-to-date to best detect malicious software that may be able to compromise the network and PHI. Often, this software can be configured to check for updates automatically and scan the HIC-approved tool.
* Other options to protect from malicious code may include application whitelisting or utilization of thin computing client implementations which restrict writeable capabilities. This may include blocking access to sites that are known or suspected to host malicious code or applications.

## Physical Security Standard

This standard defines the requirements to view, handle or otherwise deal with personal health information (PHI). The controls must be implemented to prevent unauthorized physical access, damage and interference to the Agency’s information and information processing facilities.

* HICs must implement physical security perimeters to protect identity provider services and data contribution endpoints from unauthorized physical access and environmental damage.
* 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:
  + Fitting vulnerable doors and windows with locks or bolts.
  + Installing and monitoring closed-circuit television (CCTV).
  + Employing security guards.
  + Installing intruder detection systems on external doors and testing accessible windows regularly.
* HICs must ensure that highly sensitive facilities that house identity provider services and data contribution endpoints are not accessible to the public. Details about highly sensitive facilities should be kept confidential (e.g., by using discrete signs or excluding details from directories or telephone books).
* HICs should ensure that visitors to highly sensitive facilitates are: 1.4.1. Permitted physical access only for specific, authorized purposes.
  + Monitored by recording arrival and departure times.
  + Obliged to wear visitor badges at all times.
  + Supervised at all times.
  + Made aware of behaviour or actions that are prohibited (e.g., filming or photography).

### Hazard Protection

HICs should consult with their Electronic Service Providers to ensure working areas are secure and equipment must be accessible by authorized individuals. Physical controls should be implemented and monitored to protect against common and environmental threats.

* HICs should ensure that highly sensitive facilities hosting data contribution endpoints and identity provider services are protected from natural and man-made hazards (e.g. in an area with a low risk of flooding, fire, explosion, or damage from neighbouring activities).
* HICs should minimize the impact of hazards in highly sensitive facilities hosting data contribution endpoints and identity provider services by:
  + Locating fire extinguishers so that minor incidents can be tackled without delay.
  + Training agents, and where appropriate Electronic Service Providers, in the use of fire extinguishers, other emergency/safety equipment, and in emergency evacuation procedures.
  + Monitoring and controlling the temperature and humidity.
* HICs should ensure that fire alarms in highly sensitive facilities hosting data contribution endpoints and identity provider services are monitored continuously, tested regularly and serviced in accordance with manufacturer specifications.
* HICs should ensure that existing data centre facilities and those being acquired by lease, purchase, or construction hosting data contribution endpoints and identity provider services are periodically assessed to ensure that physical security controls are in place to physically protect the information stored or processed in that data centre.
* HICs should layer physical security zones in data centres hosting data contribution endpoints and identity provider services to provide for defence in depth protection.
* HICs must ensure that physical access points in data centres hosting data contribution endpoints and identity provider services, such as delivery and loading areas and other points where unauthorized persons may enter the premises are controlled and, if possible, isolated from areas that house highly sensitive information systems to avoid unauthorized physical access.
* HICs should require their agents and Electronic Service Providers to obtain approval before leaving the data centre premises with technology used to operate identity provider services and data contribution endpoints.

# Appendix A: Resource Index

| **Seq.** | **Type** | **Document(s)** | **Comments** |
| --- | --- | --- | --- |
| **Part A** | | | |
| 1. | Security Guide (this document) | Security Guide for Connecting to [the EHR Solution] | Primary reference source provided at the time of the Webinar training.   * Developing your Information Security Program * Onboarding process steps * Roles, Responsibilities and Key Terms * Information Security Policies |
| 2. | Webinar | EHR Security Overview Webinar for organizations using ONE ID or ClinicalConnect access methods | Security introduction and overview for Viewing sites participating in [the EHR Solution]. Webinar provides:   * Overview of the Privacy and Security governance structure * EHR Security Policy overview:   1. Tips how to prepare   2. How to complete the assessment, * Key process flow diagrams |
| 3. | Policies | EHR Security Policies for organizations using ONE ID or ClinicalConnect access methods (all-in-one) | An all-in-one policy document tailored to the Viewing role. This document summarizes all applicable standards in one document. |
| 4. | Supporting Templates | 1. Sample Information Security Policy 2. Sample Incident Management Template | 1. Provided for use by Health Information Custodian (HIC) if the organization does not have an existing information security policy. May be adopted and used as the organization’s security policy with minimal effort. This document aligns with the EHR Security Policies. 2. Provided for use by Health Information Custodian (HIC) to keep a record of an information security incident. This document has fields which can be populated to capture the required information according to the EHR Security Policy - Information Security Incident Management. |
| 5. | Other | [Configuration Requirements for ConnectingOntario](https://www.ehealthontario.ca/portal/server.pt/gateway/PTARGS_32_55520_217_0_-1_47/http%3B/wcicollab.phportal.prod.ont.gss%3B11930/collab/docman/download/259158/0/0/0/CO_Configurations%20Requirements%20.pdf) | Lists recommended and minimum local configurations for ConnectingOntario. |

| **Seq.** | **Type** | **Document(s)** | **Comments** |
| --- | --- | --- | --- |
| **Part B** | | | |
| 5.a | eLearning Module | [ConnectingOntario Technical Support Privacy & Security Training](https://www.ehealthontario.on.ca/images/uploads/initiatives/resources/ConnectingOntario_Technical_Support_Privacy_and_Security_Training/story.html) | Targets Technical Support (Testers, Administrators, Helpdesk, etc.) |
| 5.b | eLearning Module | [Privacy and Security Training for Clinical End Users of Ontario’s Electronic Health Record](file:///C:/Users/mark.carter/Documents/InfoSec/Connecting%20Ontario/Task%20Force/Plain%20Language/ges/uploads/initiatives/resources/Privacy_and_Security_Training_for_Clinical_End_Users_of_Ontario_EHR/story.html) | Targets Clinical End Users (i.e., those using the solution) |
| 5.c | Reference document | Privacy & Security Training for Local Registration Authorities (LRAs) | Stand-alone training for LRAs |
| 5.d | Reference document | [ONE ID Training for LRA](https://www.ehealthontario.ca/portal/server.pt/community/home/717) | Provided by the ONE ID team which gives an overview of the specific ONE ID processes. |
| 5.e | Webinar | [Privacy and Security Training for Privacy and Security Officers](http://www.ehealthontario.on.ca/images/uploads/initiatives/resources/Privacy_and_Security_Training_for_Clinical_End_Users_of_Ontario_EHR/story.html) | Delivered in-person/over Webex which outlines the responsibilities for Privacy and Security Officer participating in [the EHR Solution]. |

| **Seq.** | **Type** | **Document(s)** | **Comments** |
| --- | --- | --- | --- |
| **Part C** | | | |
| 6 | Assessment | EHR Security Assessment  for organizations using ONE ID or ClinicalConnect access methods | The security assessment tool used to measure the organization’s compliance with the EHR Security Policies. This is submitted to eHealth Ontario as part of the onboarding process. |

# Appendix B: Confidentiality Agreement SAMPLE

Confidentiality Agreement

In consideration of working at this office, I acknowledge the importance of protecting the confidentiality and integrity of any personal or personal health information7 to which I have access. I agree not to collect, use or disclose such information to any person or organization except as necessary in the course of providing my services.

Further, I: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Acknowledge that I received, read and understood this office’s security policy

1. Acknowledge that I received, read and understood the Security Quick Reference Guide, as well as a statement of my own responsibilities with regard to protecting the confidentiality of information
2. Agree that this office’s policy and supporting instructions form part of my terms of employment or my contract, and that any violation of this Security Acknowledgement and Confidentiality Agreement may result in disciplinary action, up to and including termination of my employment or contract
3. Agree that I will immediately notify the person with overall responsibility for security in the office in the event that I become aware of any violation of this office’s security policy, or accompanying instructions, including any unauthorized collection, use, disclosure, or disposal of personal health information, other than in accordance with this office’s Security Policy, as amended from time to time.

# Appendix C: Information Security Incident Report TEMPLATE



# Appendix D: Information Security Policy SAMPLE



# Appendix E: Electronic Service Provider List TEMPLATE

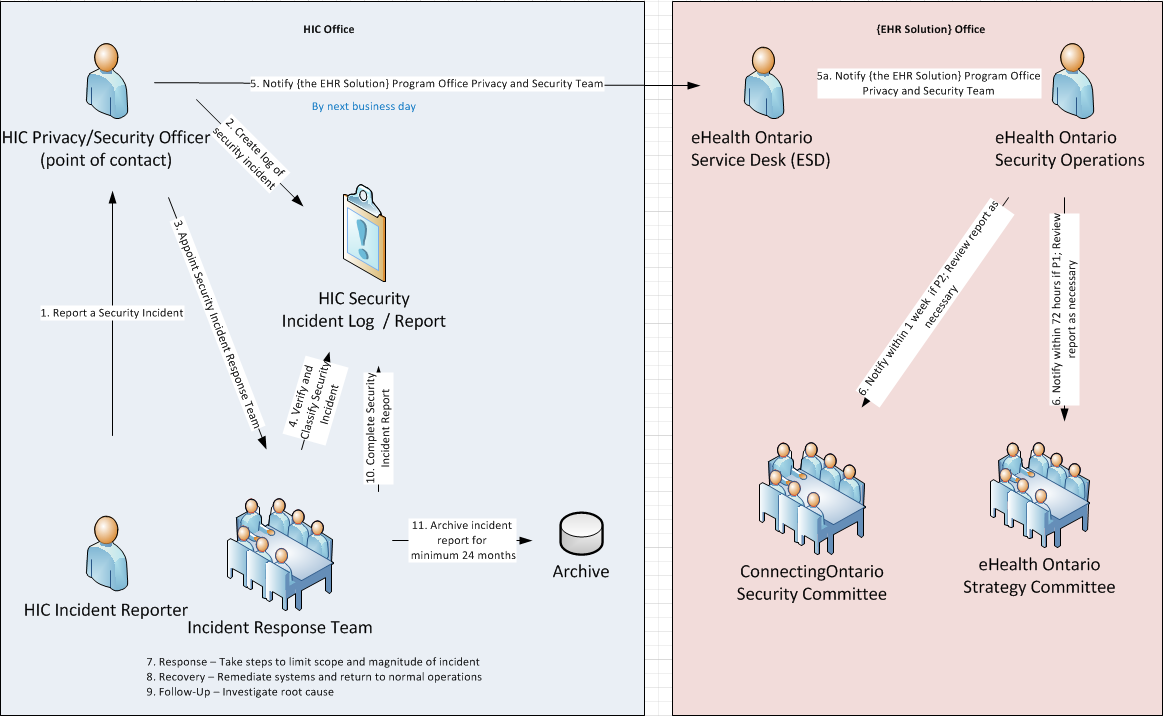


# 

# Appendix F: Incident Workflows

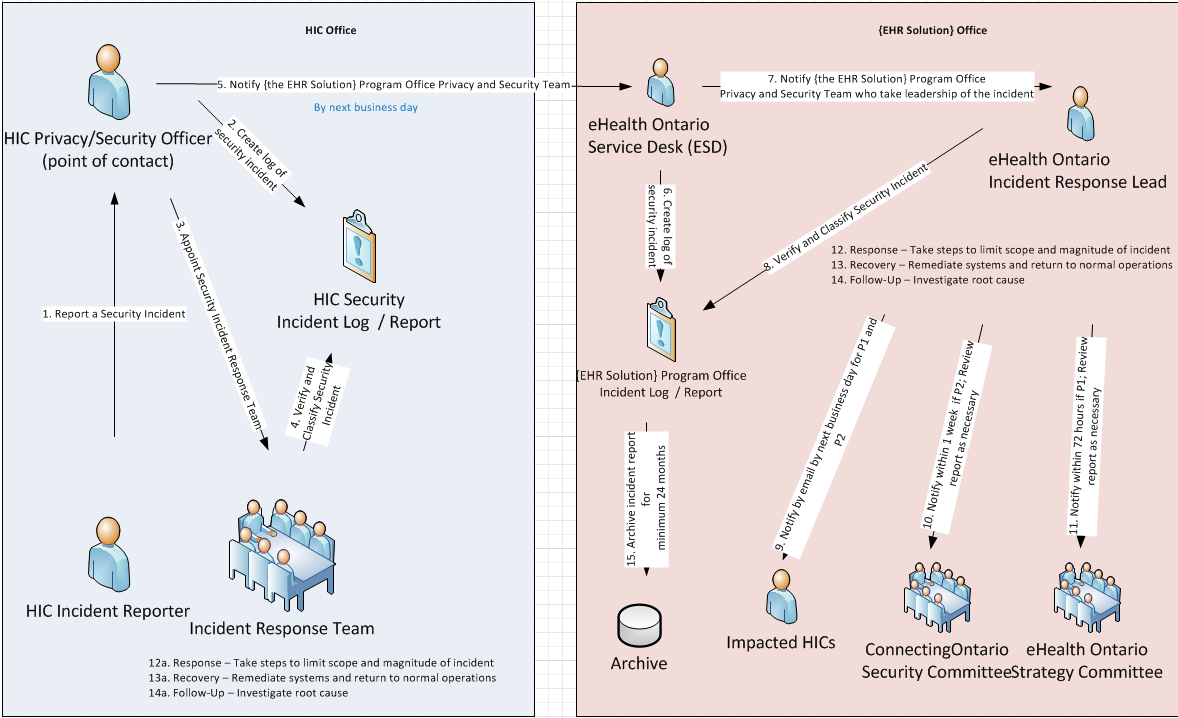
Two typical security incident workflows are shown: 1) HIC-led, in which the incident is localized and doesn’t affect other HICS, as shown in *Figure 5*; and 2) [the EHR solution] Program Office-led in which other HICs are affected, as shown in *Figure 6*.

**1. HIC-led incident**



**Figure 5. HIC-led incident**

**2. [The EHR Solution] Program Office Privacy and Security Team-led security incident**



**Figure 6. [EHR solution]-led incident**

1. If, at any point in the incident management process, the HIC realizes that the incident has resulted in a Privacy Breach, the incident must be handled in accordance with the [***Privacy Breach Management Policy***](http://www.ehealthontario.on.ca/images/uploads/regional_partners/cGTA/privacy_policies_and_procedures/EHR_Privacy_Policies.pdf).

# Appendix G: Role Definitions & Responsibilities

**Table 1. HIC Roles & Responsibilities within [the EHR Solution]**

| HIC Roles | Definitions & Responsibilities |
| --- | --- |
| Agent (i.e., End User) | A person that, with the authorization of the health information custodian, acts for or on behalf of the custodian in respect of PHI. For example, an agent may be an employee or contractor that performs Local Registration Authority functions, or a physician who cares for patients on the HIC’s behalf.  **Responsibilities**   * Read and comply with the policies, standards, and procedures set out by the HIC in the protection of sensitive information. * Read, sign and comply with *Appendix B: Confidentiality Agreement Sample* where your organization leverages this. * Follow clean desk practices especially in unattended workspaces. * Lock filling cabinets, when unattended and secure mobile computing devices such as laptops. * Question unfamiliar individuals entering restricted areas. * Secure information and computers used outside the office as per the IPC fact sheet [*Encrypting Personal Health Information on Mobile Devices*](https://www.ipc.on.ca/English/Resources/Educational-Material/Educational-Material-Summary/?id=613)*.* * Avoid accidently exposing sensitive information through conversations, exposed computer screens and unattended desks. * Dispose of hard copy personal health information and digital media as per IPC fact sheet [*Secure Destruction of Personal and Personal Health Information*](https://www.ipc.on.ca/English/Resources/Educational-Material/Educational-Material-Summary/?id=451)*.* * Before sending a fax, confirm the number is still valid and was dialed correctly. * Only access the system for the purposes of providing care or assisting in the provision of care. * Report all security incidents to the security officer. |
| Electronic Service Provider (ESP)/  IT Service Provider/  IT System Administrator | A person or organization that provides goods or services that enable a HIC to electronically collect, use, modify, disclose, retain or dispose of PHI; and includes a health information network provider. This could be your IT Systems Administrator or a third party provider who provides tech support.  For example, an individual or a company providing IT services to the medical office, such as installing and servicing computers, installing new software and providing network connectivity.  **Responsibilities**   * Support the HIC in meeting the PHIPA and EHR Security Policy requirements. * Sign a confidentiality agreement with the practice prior to access to confidential information, where applicable. * Read the security policy and sign the *Appendix B: Confidentiality Agreement Sample where applica*ble before starting any work. * Locate computer(s) in a secure location to minimize the risks of modification, loss, access, theft, view and disclosure by unauthorized individuals, * Ensure each user is provided a unique user ID and that they select their own password. * Instruct staff members to use strong passwords that are 8–10 characters long and are a combination of uppercase and lowercase letters, numbers and special characters. * Enable security features such as passwords and a locked screen saver. * Install and manage hard drive encryption, where applicable. Refer to the IPC fact sheet [*Health Care Requirements for Strong Encryption*](https://www.ipc.on.ca/English/Resources/Educational-Material/Educational-Material-Summary/?id=969). * Install security software such as anti-virus, anti-spam, anti-spyware and personal firewall from a reputable vendor and keeping them up- to- date. * Apply security patches and updates to computers on a regular basis. * Connect the computers to an uninterruptable power supply (UPS) where required. * Ensures the security officer responsible for the overall office security understand the security features installed and what actions to take in case of an incident. |
| Health Information Custodian (HIC) | The health information custodian, typically a health care practitioner who has custody or control of personal health information as a result of or in connection with performing the person’s or organization’s powers or duties.  **Responsibilities**   * Safeguard PHI, ensuring it is: * accurate and up-to-date for the purposes for which the information is used * protected against theft, loss and unauthorized use or disclosure * protected against unauthorized copying, modification or disposal * retained, transferred, and disposed of in a secure manner * Notifies patients as soon as possible if the patient’s PHI is stolen, lost or accessed by unauthorized persons. * Ensures that all Agents and ESPs who have access to [the EHR Solution] have an end user agreement in place that includes confidentiality and accountability provisions. * Develops, implements, and maintains an Information Security Policy that sets requirements, assigns responsibilities, and demonstrates the organization’s commitment to protecting PHI. * Designates an Information Security Lead to ensure compliance of all staff as well as Agents and ESPs who have access to [the EHR Solution] Services. |
| Legally Responsible Person (LRP) | Often a senior executive within the organization, such as the Chief Information Officer.  **Responsibilities**   * 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 LRP 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 access control processes, procedures, policies, standards, and identity management systems. 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].  **Responsibilities**   * Register and enroll HIC’s Agents or Electronic Service Providers * Verify the identity of the Agent or Electronic Service Provider requesting access. |
| Security Officer | Staff member appointed by the organization with overall responsibility to manage the security program on a day-to-day basis including reporting incidents to [the EHR Solution] Program Office. In an office setting, a security officer can be the nurse, medical office assistant or other health care professional who has been delegated these responsibilities.  **Responsibilities**   * Ensures ongoing security compliance of your organization * Communicate with [the EHR Solution] Program Office in the event of an incident. * Arrange assistance in leading the investigation, if necessary, and ensure required remediation is completed. * Ensure the security policy is posted in a prominent place within the office so that it is available to both staff and patients as required. * Ensure staff and contractors are aware of the security policy and informed on how it should be interpreted and put into action. * Ensure all staff are trained on their security responsibilities. * Where leveraged, collect and file the signed and dated Confidentiality Agreement (see [*Appendix B: Confidentiality Agreement SAMPLE*](#_Appendix_B:_Confidentiality)*)* from all Agents, staff and Electronic/IT Service Providers. * Ensure disposal of personal and personal health information meets security standards as given in the IPC fact sheet [*Secure Destruction of Personal and Personal Health Information*](https://www.ipc.on.ca/English/Resources/Educational-Material/Educational-Material-Summary/?id=451)*.* * Ensure staff have access to a shredding machine to securely dispose of personal health information that is no longer required. * Instruct staff how to create strong passwords, one that is easy to remember but difficult to   guess, and never to share their passwords.   * Ensure that staff understands that they are not to install unauthorized software, connect unauthorized devices to their computers, or use their computers for unauthorized purposes. * Revoke or suitably adjust (physical, network, system and application) access and change   shared passwords as soon as employees leave or change responsibilities.   * Direct the IT service provider to set up security safeguards on all office computers including strong encryption, security patches and antivirus solutions. * Ensure the IT service provider provides a written description of the service provided. * Monitor and perform spot checks on a regular basis to ensure all staff are following the   Security Policy. Take appropriate action if not followed. |
| 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.  **Responsibilities**   * Approve access to [the EHR Solution] to those who meet the criteria as outlined in agreements. |

**Table 2. Roles & Responsibilities within [the EHR Solution] external to the HIC (i.e. often facilitated by eHealth Ontario or its delivery partners)**

| External Roles | Definitions & Responsibilities |
| --- | --- |
| Applicable Oversight Body | Comprised of senior-level executives who oversee all aspects of [the EHR Solution].  **Responsibilities**   * Review security related materials such as Threat Risk Assessments and Major Incidents to ensure appropriate action is taken. |
| Connecting Security Committee | The provincial security forum consisting of senior security representatives from across the regions and eHealth Ontario  **Responsibilities**   * Responsible for establishing a functional and usable information security governance framework for participating organizations in the EHR. |
| Privacy and Security Committee (PSC) | The Privacy and Security Committee (PSC) is a committee comprised of Agents from participating HICs.  **Responsibilities**   * Support the privacy and information security governance structure within [the EHR Solution]. |
| [The EHR Solution] Privacy and Security Operations Team | Made up of [the EHR Solution] agents who support [the EHR Solution]’s privacy and security-related activities, initiatives, and processes.  **Responsibilities**   * Support privacy and security assessment work * Support privacy and security incident coordination among HICs and other stakeholders participating in [the EHR Solution] * Support threat risk assessment work * Support privacy and security operational work |
| Program Office | [The EHR Solution] Program Office consists of the internal resources and external contracted resources that support the core EHR solution.  **Responsibilities**  This group runs a central function which coordinates activities such as new releases, top level privacy and security incident oversight, managing infrastructure and uptime for [the EHR Solution]. |
| Registration Authority (RA) | A top level entity that has overall accountability to provide registration and identity management functions. Responsible for registering Local Registration Authorities (LRAs).  [The EHR Solution] or its delegate will act as the RA for all agents and Electronic Service Providers requesting access to the solution. (i.e. ONE ID acts as the Registration Authority) |

**Copyright Notice**

Copyright © 2017, eHealth Ontario

**All rights reserved**

No part of this document may be reproduced in any form, including photocopying or transmission electronically to any computer, without prior written consent of eHealth Ontario. The information contained in this document is proprietary to eHealth Ontario and may not be used or disclosed except as expressly authorized in writing by eHealth Ontario.

**Trademarks**

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