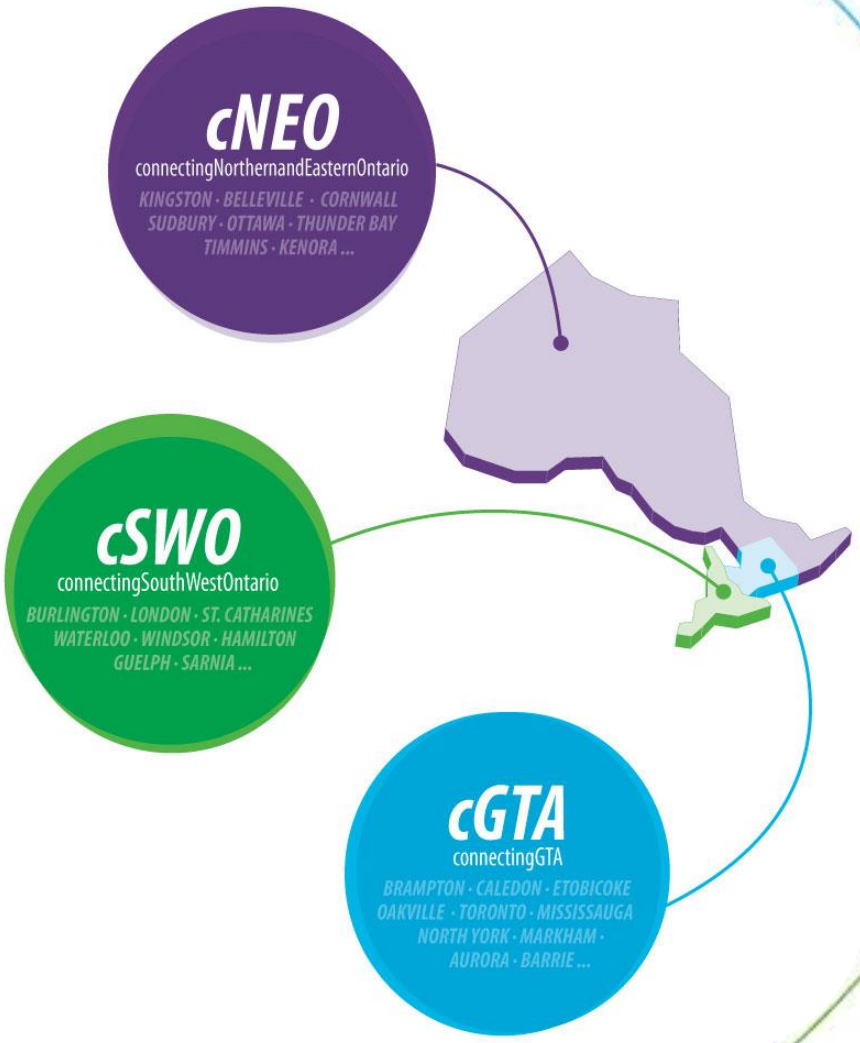


Connecting Ontario
POWERED BY EHEALTH ONTARIO

EHR SECURITY POLICIES & SECURITY SITE ASSESSMENT OVERVIEW WEBINAR

For Viewer Sites

Ontario
eHealth Ontario

Agenda

1	Introduction and EHR Security Policies Background
2	EHR Security Policy Overview
3	EHR Security Policy Assessment Overview
4	Questions
5	Appendix

Connecting Ontario
POWERED BY EHEALTH ONTARIO

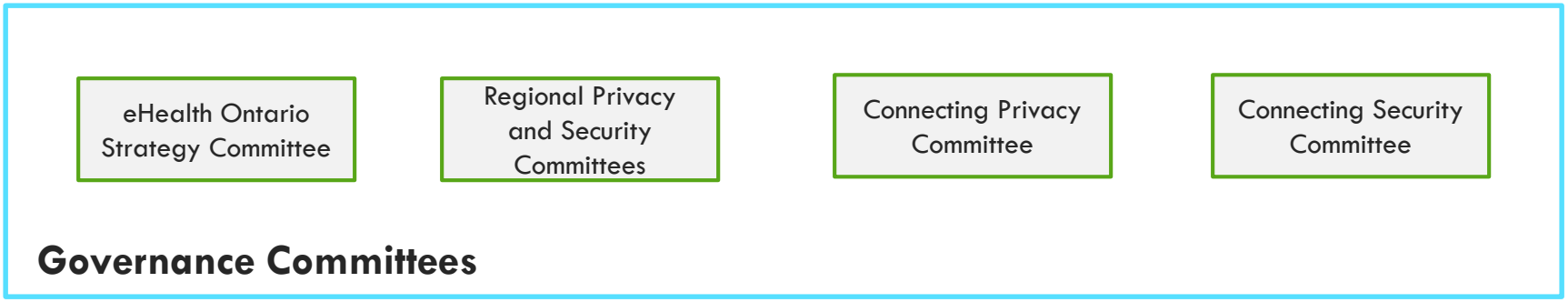
INTRODUCTION & EHR SECURITY POLICIES BACKGROUND

Ontario
eHealth Ontario

Purpose

- Provide an overview of the governance structure for privacy and security.
- Review the high-level obligations and processes required of the EHR Security Policies.
- Provide an overview of steps to ensure readiness to comply with the EHR Security Policies and prepare sites for onboarding to the EHR Solution.

Connecting Ontario Privacy and Security Governance Structure



EHR Security Policies

Policies applicable to Viewer Sites

- Information Security Policy
- Acceptable Use of Information and Information Technology Policy
- Local Registration Authorities Practices Policy
- Cryptography Policy
- Electronic Service Provider Policy*
- Information and Asset Management Policy
- Information Security Incident Management Policy
- Network and Operations Policy
- Physical Security Policy

Policies not applicable to the Viewer Sites

- Access Control and Identity Management Policy for System-Level Access
- Business Continuity Policy
- Physical Security Policy
- Security Logging and Monitoring Policy
- System Development Lifecycle Policy
- Federation Identity Provider Standard

Compliance with mandatory requirements (indicated by the use of "must"/"shall") is required prior to your site going live, unless an exemption has been granted.

Information Security Safeguards

- PHIPA requires PHI to be protected by security safeguards
- Electronic Health Record (EHR) Security Policies establish mandatory and recommended safeguards
- Developed by the Connecting Security Committee (includes representatives from eHealth Ontario, ConnectingGTA, ConnectingSWO, ConnectingNEO and CHI)
- Being standardized across regional and provincial initiatives (e.g., those funded or operated by eHealth Ontario)
- Sites bound to EHR Security Policies through agreements with eHealth Ontario

Connecting Ontario
POWERED BY EHEALTH ONTARIO

EHR SECURITY POLICY OVERVIEW

Ontario
eHealth Ontario

EHR Security Policy Structure

- EHR Security Policies are divided into two sections:
  - 1. Requirements for Health Information Custodians (HIC)
  - 2. Requirements for the Program Office / Solution Operators
- Section 1 requirements are distributed across three roles a typical HIC organization would take on:
  - Data Contributor
  - Identity Provider
  - Viewer
- Section 2 requirements are intended for those organizations who are running an EHR solution or their service providers. (e.g., eHealth Ontario for Connecting Ontario, and Hamilton Health Science Centre for Clinical Connect)

EHR Security Policy Structure

- **Purpose:** Defines the intention/objective of the policy
- **Scope:** Specifies to which technologies the policy applies
- **Definitions:** Provides definitions for key terms used within the policy
- **Policy Requirements:** Lists all the requirements/obligations. Divided into two sections:
  - Requirements for Health Information Custodians, their Agents, and their Electronic Service Providers
  - Requirement for the EHR Solution Program Office, its Agents, and its Electronic Service Providers
- **Exemption:** Refers readers to the Exemption Process found in the Information Security Policy
- **Enforcement:** Outlines measures for dealing with non-compliance
- **References:** Provides list of reference documents

EHR Security Policy Requirement Types

Three types of requirements in the EHR Security Policies:

- **"Must/Shall" Requirements:** Used for absolute requirements, i.e., they are not optional
- **"Should" Requirements:** 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
- **"May" Requirement:** The requirement is only a recommendation, or provided as an implementation example and not intended on being exhaustive

All statements "must/shall, should, & may" requirements are contained in the assessment

Information Security Policy

- **Principles:** High-level principles contained in the policy direct readers to individual sub-policies
- **Information Security Exemption Requirements:** Defines exemption process for instances where an organization cannot comply with a mandatory requirement
- **Roles and Responsibilities:** Defines the role and responsibilities of the
  - Connecting Security Committee
  - Strategy Committee
  - Privacy and Security Operations Team
  - Health Information Custodians (HICs)

Purpose: Outlines the framework for information security governance by:

Defining the information security principles to manage PHI, the EHR Solution, information systems or information technologies that connect to the EHR Solution; and, establishing the roles and responsibilities for ensuring the principles in this policy are implemented and maintained.

Information Security Policy - HIC Responsibilities

- Develop, implement and maintain an information security policy that upholds the principles of the EHR information security policies
- Designate an information security lead to ensure compliance
- Ensure that all agents and Electronic Service Providers (ESPs) are aware of their information security responsibilities
- Require agents and ESPs to agree to an end-user agreement before accessing the EHR Solution
- Hold individual agents and ESPs accountable for their actions

Information Security Policy - How to Prepare

- ✓ Ensure that your site has an internal security policy that upholds the principles of the EHR Security Policies. A sample policy is available to be leveraged by your organization if you do not have an existing policy.
- ✓ Designate a security lead to ensure compliance
- ✓ Ensure that your site has a disciplinary process for dealing with agents and ESPs who are non-compliant with your policies and procedures

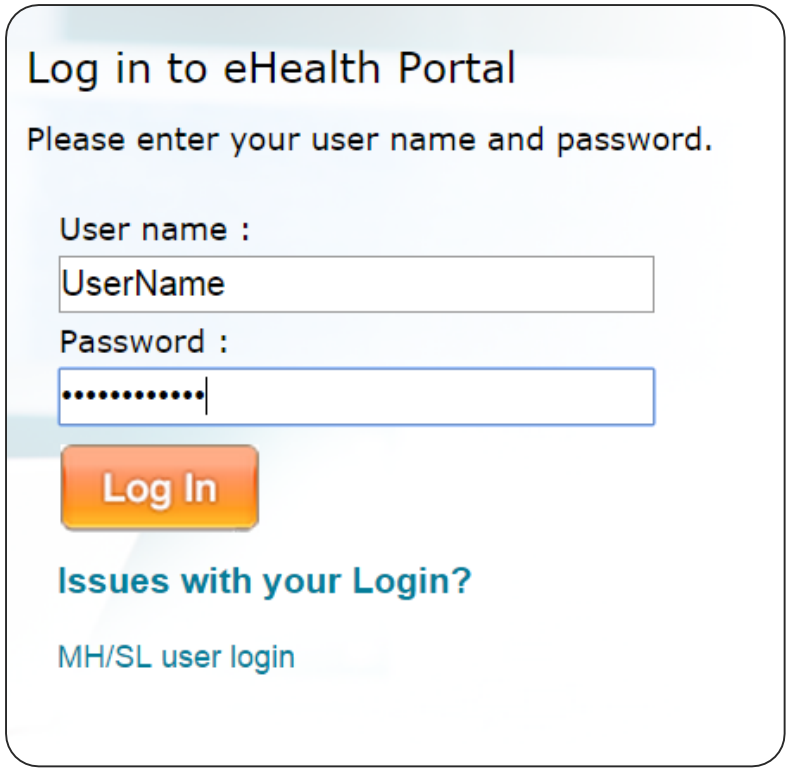
Acceptable Use of Information and Information Technology Policy

- **General**
  - Use only assigned credentials
  - Use only HIC-approved tools
  - Prohibits taking pictures of data
  - Lock workstations when logged in but leaving device unattended*
- **Emailing PHI**
  - Prohibits use of external email accounts to send/receive PHI to/from the EHR Solution Program Team or eHealth Ontario
  - Encrypt emails that contain PHI, use a secure file transfer solution or use a secure e-mail system

Purpose: Defines the behavioral requirements for persons who have access to the EHR Solution.

Acceptable Use of Information and Information Technology Policy

- **Creating and Protecting Passwords**
  - Requires creation of strong passwords
  - Prohibits users from revealing their password to anyone, or writing it down and storing it insecurely.
  - Outlines what to do if they feel their password has been compromised



Acceptable Use of Information and Information Technology Policy

- **Working Remotely**
  - Requires the use of an approved remote access solution
  - Prohibits use in areas where unauthorized individuals can view the information (e.g., Internet cafés, public transit, and other non-private settings)
  - Forbids leaving mobile computing device used to access the EHR Solution unattended in a public place
  - Obliges users to lock mobile computing device in the trunk or place it out of view when leaving it in a vehicle
  - Requires the location where PHI is downloaded onto a mobile device to be encrypted
- **Reporting Information Security Incidents**
  - Requires users to immediately report suspected or confirmed security incidents related to the EHR Solution

Acceptable Use of Information and Information Technology Policy - How to Prepare

- ✓ Review your site's internal policy, awareness, education, and training programs
- ✓ Identify gaps with internal awareness and training messages, i.e., whether or not similar messages are already included in your internal training and awareness programs
- ✓ Consider leveraging the training modules that have been developed for Connecting Ontario which include the messages from this policy

Local Registration Authorities Practices Policy

- **Legally Responsible Person (LRP) must identify:**
  - One or more persons, groups, or roles that has the authority to act as a Sponsor (i.e. the person who approves access)
  - One or more persons to act as a Local Registration Authority (LRA) to manage the enrollment of its agents and Electronic Services Providers who require access to the EHR Solution
- LRAs are responsible for verifying the identity of individuals at your site who require access to the EHR Solution (unless this has already been performed through another established process) and ensure that they receive appropriate authorization to use the system

Purpose: Defines the procedures for enrolling LRAs and for enrolling agents & Electronic Service Providers for access to the EHR Solution.

Note: LRAs for ONE ID sites are registered with eHealth Ontario; section of primary concern is Entitlement Criteria.

Local Registration Authorities Practices Policy

Provider Portal: Only provide access to Agents whose purpose of access is to collect PHI for providing or assisting in the provision of healthcare, which may include:

- Regulated health professionals who see patients
- Residents providing care to patients
- Administrative staff who pull charts for physicians
- Ward clerks who review results to flag abnormals for physicians

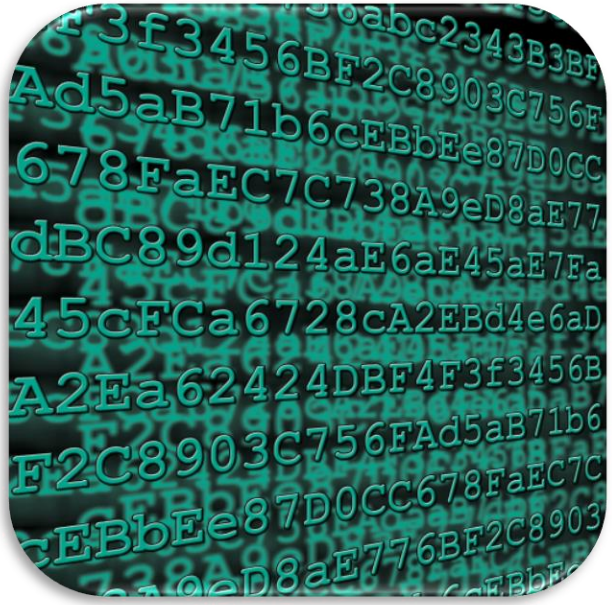
Site Administration Portal: Only provide access to those whose purpose of access is to provide support for defined and permitted functionality, which includes:

- Managing consent directives
- Running reports (e.g., audit reports and operations reports)
- Managing user accounts on the Administration Portal
- Supporting the HIC's HL7 data contribution endpoints (e.g. HL7 data feeds, HL7 error management)
- Managing terminology mapping functions

Local Registration Authorities Practices Policy - How To Prepare

- ✓ Think about who at your site would be appropriate to act as Sponsors and LRAs
- ✓ Review the entitlement criteria and identify possible groups/roles that may require access to the Provider Portal or the Site Administration Portal
- ✓ Review identity verification requirements and determine whether or not this is already being performed at your site

Cryptography Policy



- ✓ Use EHR-approved cryptographic algorithms for connections established with the EHR Solution
- ✓ Designate key custodians

How to Prepare

- ✓ Identify any cryptographic solutions that may be employed to support your site. (e.g. encryption for devices used to access the EHR Solution) Verify whether or not they meet the standard

Purpose: Defines the information security controls that are required to implement and manage cryptographic solutions.

Electronic Service Provider Policy

- Assess the potential information security and privacy risks posed by all new ESPs to the EHR Solution prior to engaging in a contractual relationship
- Define and document all information systems and services to be provided by new ESPs or on renewal of service agreements
- Require new ESPs to implement applicable information security and privacy controls prior to the ESP being granted access to the EHR Solution

How to Prepare

- Review ESP relationships that are to be renewed and ensure that EHR Security Policy obligations are included in new ESP agreements.
- Existing ESP relationships should include the EHR security policies. Organizations will be required to attest where EHR security policy controls are being provided by an ESP.

Purpose: Defines the requirements for managing Electronic Service Providers (ESPs).

Information and Asset Management Policy

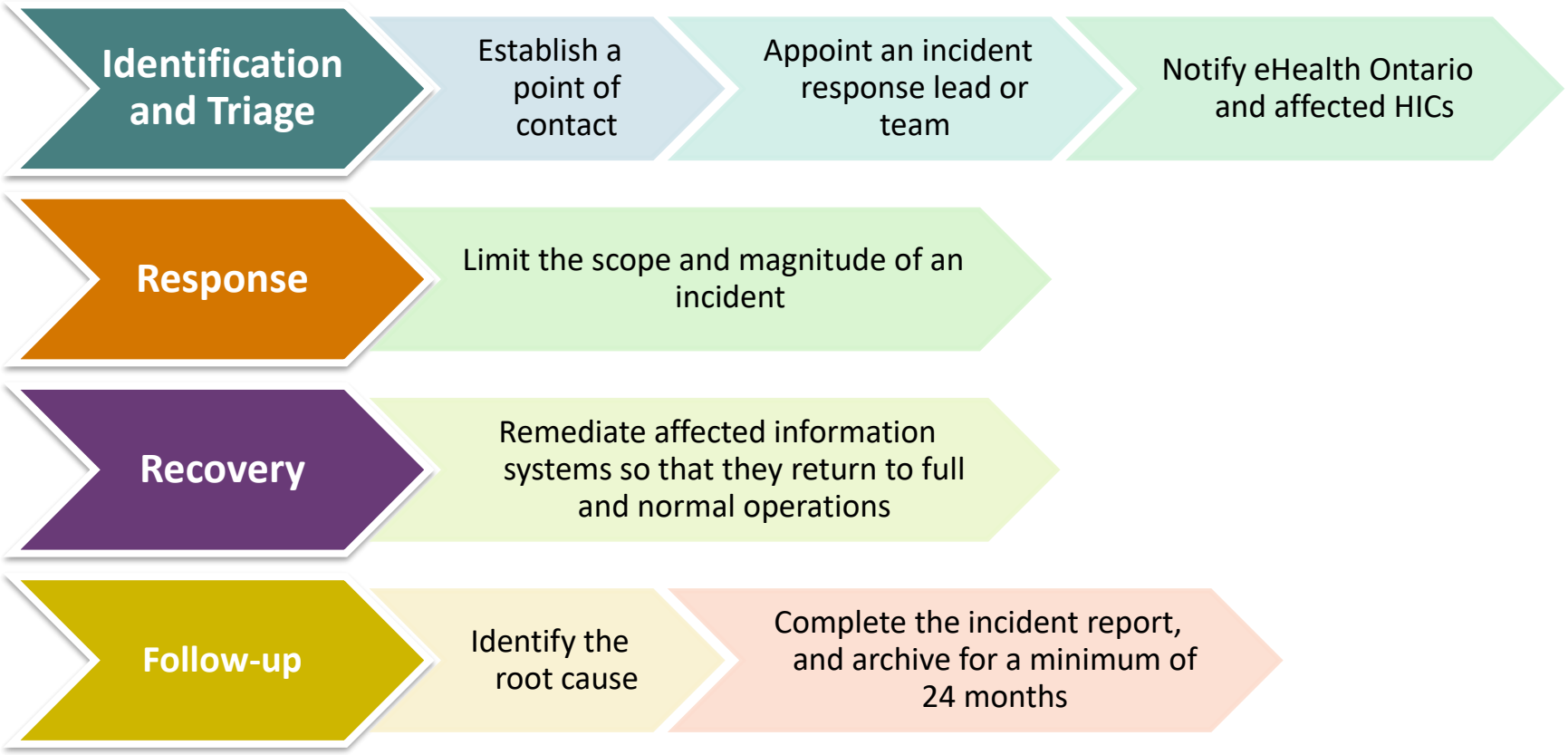
- Requires organizations to ensure that all PHI that is transmitted to eHealth Ontario, the EHR Solution Program Offices, or the EHR Solution is done in a secure manner, e.g., through the use of secure email, encryption, or virtual private network tunnel

How to Prepare

- Determine site's secure methods of transmission of PHI

Purpose: Defines the information security controls that are required to protect information throughout the information lifecycle.

Information Security Incident Management Process



Purpose: Defines the requirements for creating an information security incident ("incident") management process.

Information Security Incident Management Process - How to Prepare

- ✓ Review your site's security incident management process
- ✓ Verify whether or not it can be leveraged to deal with incidents related to the EHR Solution
- ✓ Understand the reporting requirements in the event of a Severity 1 or Severity 2 incident.
- ✓ A sample security incident reporting template is available to track the required information during an incident and can be used to create the final report.
- ✓ If you need assistance with notifications to other impacted HICs, communicate this when reporting the security incident to eHealth Ontario and the Program Office will be able to assist.

Network and Operations Policy

- Implement and manage segregated network zones (e.g. Guest network)
- Control traffic between networks zones (e.g. Internet vs. Internal Network)
- Review security gateway configurations at least annually
- Use of malware detection and repair software or equivalent solution on HIC approved tools, processes and workstations to protect from malicious code
- Keep malware detection and repair software up-to-date

How to Prepare

- Requirements strongly recommended, but not mandatory
- Review current network practices
- Determine whether or not your site utilizes an appropriate malware detection & prevention solution

Purpose: Defines requirements for implementing and maintaining secure networks and information systems that comprise the EHR Solution, and as well as the networks and information systems of health information custodians (HIC) who view PHI in the EHR Solution or contribute PHI to the EHR Solution.

Physical Security Policy

- Implement physical security perimeters to protect IDP services and data contribution endpoints from unauthorized physical access and environmental damage
- Protect power supply for data contribution endpoints and IDP services
- Made aware of behaviour or actions that are prohibited (e.g., filming or photography).
- Protect telecommunications cabling used to transmit information that supports data contribution endpoints and IDP services from interception or damage

Purpose: Defines requirements for the physical security of the EHR Solution, and HIC's identity provider services and data contribution endpoints.

Connecting Ontario
POWERED BY EHEALTH ONTARIO

EHR SECURITY POLICY ASSESSMENT OVERVIEW

Ontario
eHealth Ontario

Security Site Assessment Overview

- The Connecting Security Committee has developed a standard assessment tool, called the "**EHR Security Policy Assessment Template – Viewer Only Version**", to be completed by each site prior to participating in the EHR Solution

Step 1

Complete Site Profile tab:

- Follow instructions to complete requested information

Step 2

Complete Control Analysis tab:

- Read through instructions on how to complete the "Control Analysis" tab

Step 3

Submit Complete Assessment:

- When complete, password protect the document using a **strong** password and submit it to eHealth Ontario's Connecting Ontario Security Team. (See Appendix on **How to Encrypt a Microsoft Excel document and Creating and Communicating a Strong Password**
- Phone the designated Connecting Ontario Security contact with the password to decrypt. (Razi Farooqui – 416-586-4018; Ola Edidi 416-324-0838)

Completing the Security Site Assessment Tool

Step 4

Review with eHealth Ontario:

- eHealth Ontario's Connecting Security Team will review the assessment results and work with the site to understand the plans to resolve any non-compliant controls. The Connecting Ontario Security team can provide consultation advice or additional tips.

Step 5

Exemption Processing and document signoff by the executive sponsor:

- Where required, exemptions may be documented and presented for approval to the eHealth Ontario Strategy Committee. The Connecting Ontario Security Team will work with the sites to document those and to arrange to have the completed assessment and exemptions approved by the executive sponsor.

High Level Steps to Complete the Assessment Tool

[The EHR Solution] Information Security Assessment - Filtered for the Viewer Role

Instructions: 1. For each policy statement below please select a response from the **Status** and **Expected Implementation Date** columns. In the **HIC Comments** column, add sufficient detail about the control implementation at your organization. For example, reference an internal policy, practice or control that has been implemented. This will enable your executive sponsor to attest to the controls your organization has put in place and will allow for future re-use and interpretation of this assessment by members of your organization. Review the **Implementation Guidance** and **Scope Considerations** column for additional assistance. If your organization is using ONE ID, links to the relevant materials and aids have been provided in column N and O.
2. When complete, password protect the document using a strong password and submit it to **connecting.security@ehealthontario.on.ca**, phone the Connecting Security Team contact with the password to decrypt. (Razi Farooqui - 416-586-4018; Ola Edidi - 416-324-0838) If you have any questions, please contact the connecting.security@ehealthontario.on.ca inbox.

Legend

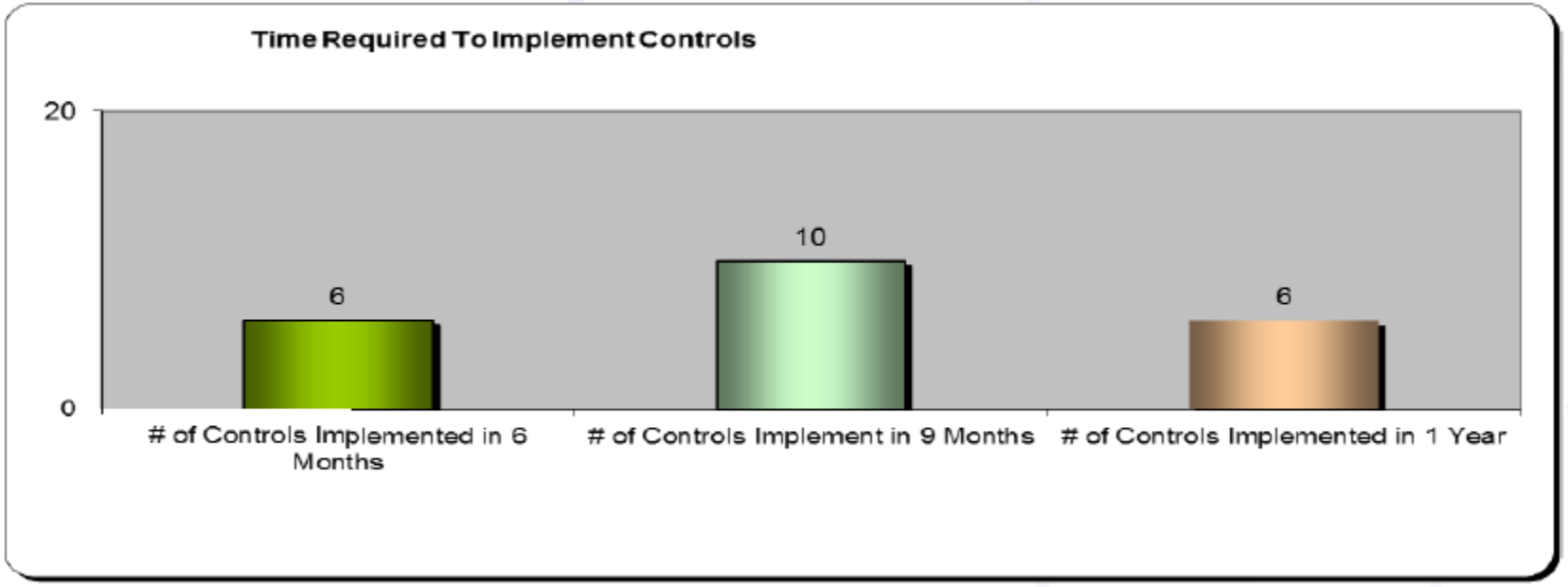
Status Code	Meaning	Must Policy Statement
I	Control is Implemented or similar / equivalent control exists (please describe equivalent or similar controls)	Should Policy Statement
NI	Control is Not Implemented - remediation is required.	
NA (Not Applicable)	Control is Not Applicable for the organization. (please provide rationale for excluding control)	

Policy reference	Source Policy	Control description	Status	Expected Implementation Dat	HIC Comments
	Acceptable Use of Information and Information Technology Policy v1.6				
1.1	Acceptable Use of Information and Information Technology Policy v1.6	HICs, their Agents and Electronic Service Providers must always use assigned credential to access [the EHR Solution].			

1. Review each control and determine if it is "**I**" (Implemented) , "**NI**" (Not Implemented) or **"NA"** (Not Applicable) based on your existing practice. Read through the "Scope Consideration", "Implementation Guidance" and "ONE ID and other Reference Materials" columns J, L, N, & O to help you.

2. Where status is "**NI**", select when you plan to remediate and provide some details in the "HIC Comments" column. If **"NA"** is selected, indicated what compensating controls are in place to support this answer in the "HIC Comments" section.

Graphical Dashboard



A graphical summary of your compliance is automatically compiled on the “dashboard” tab.

Information Security Exemptions

- Any deviation from a mandatory requirement in an EHR security policy, standard, or supporting document must be approved by the Strategy Committee
- All information security exemption requests will be assessed and then reviewed by the Connecting Ontario Security Team, prior to it being sent to the Strategy Committee for approval

Who will have access to my security assessment and how will it be protected?

- Assessments must be encrypted, password protected and shared with eHealth Ontario as per the requirements of the "Electronic Health Record (EHR) Security Policy – Information and Asset Management" and "File Encryption and Transfer Guidelines"
- eHealth Ontario's security analysts and leads will have access to the assessments
- In the course of clarifying questions and assisting hospitals in the mitigation process, the Program Delivery Partner and Service Delivery Partners may need to be aware of assessment content related to conditions or site timing.
- The content of the security assessment is not shared with outside organizations or with other stakeholders.

Who will have access to my security assessment and how will it be protected?

- The security assessment will be stored in an encrypted format on the eHealth Ontario corporate network with access control lists configured to provide access to the authorized individuals.
- The security assessments will be retained at eHealth Ontario in line with the C*onnecting*Privacy Committee (CPC) – Harmonized Retention Policy. This current policy outlines a requirement to store the assurance materials for a period of 10 years.

Connecting Ontario
POWERED BY EHEALTH ONTARIO

THANK YOU!

QUESTIONS?

Ontario
eHealth Ontario

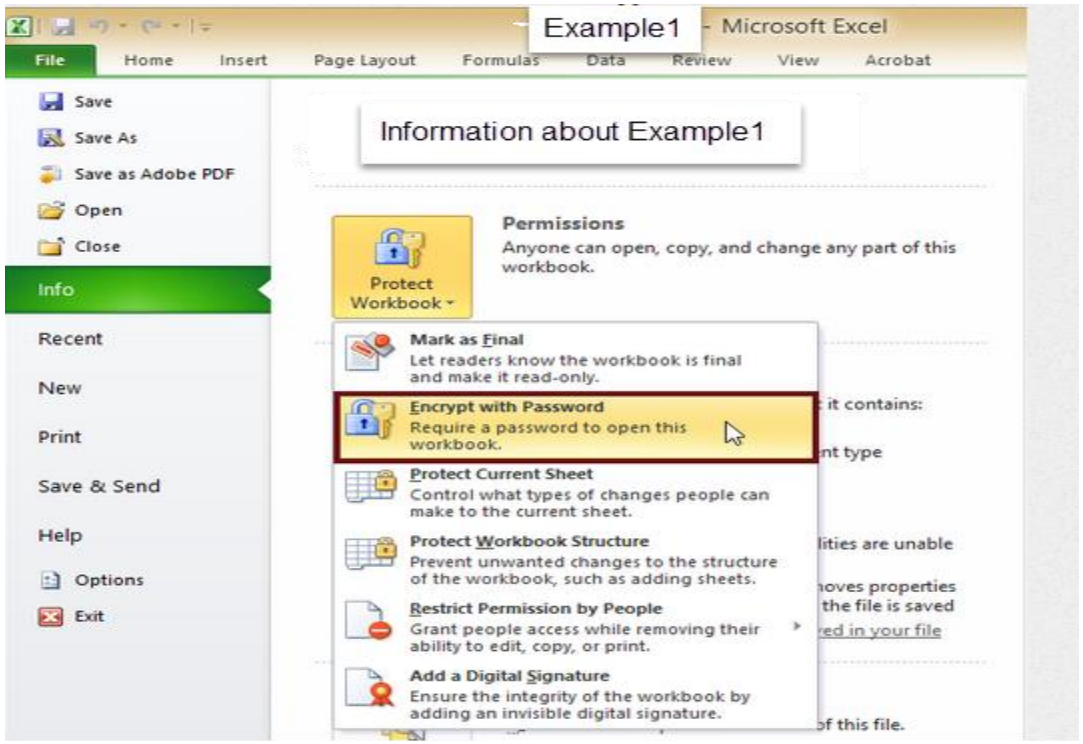
Connecting Ontario
POWERED BY EHEALTH ONTARIO

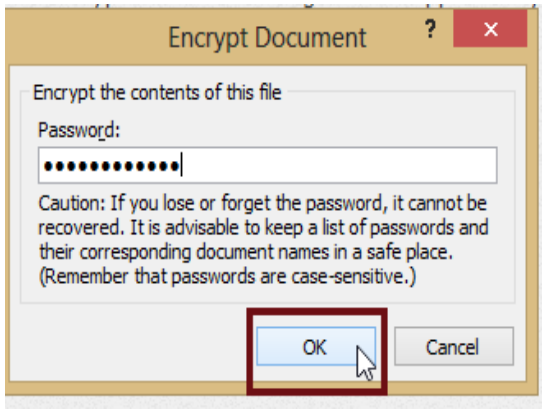
APPENDIX

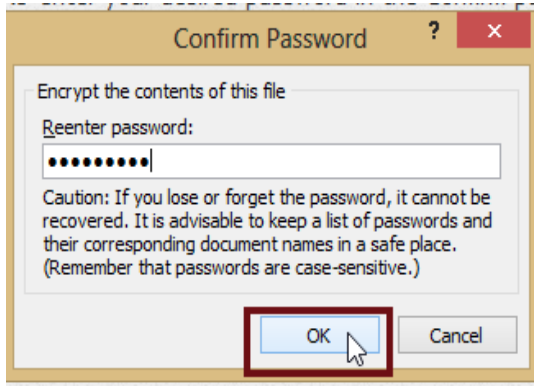
Ontario
eHealth Ontario

How To Encrypt a Microsoft Excel 2010 Document

1. Open the document
2. Click on the **File** tab, then click on **Info**
3. Select **Protect Workbook**, and choose **Encrypt with Password** from the pull down menu
4. Enter a strong password in the **Encrypt Document** window (See slide on **Creating and Communicating a Strong Password**)
5. Reenter password in the **Confirm Password** window







Creating and Communicating a Strong Password

It is important to create a **strong** password with which to protect encrypted files.

- Create and use a different password for each different encrypted document
- Use 8 characters or more
- Passwords must contain characters from three of the following four categories: uppercase characters (A-Z); lowercase characters (a-z); numeric (0-9); and special characters (e.g. !, $, #, _, ~, %, ^)
- Example of a bad password is 1234Password!
- Example of a good password is iT_iS_A_warM_daY22

Communicating the Password

- Once the file has been encrypted, the password **must** be communicated to the file recipient by using an "out of band" method to the designated contact (e.g. if emailing document, send password by phone, fax or mail)
- Designated contact: **Ola Edidi (416-324-0838)** or **Razi Farooqui (416-586-4018)**
- Password **must not** be sent through the same channel as the encrypted file