eHealth Ontario
It's working for you.

ELECTRONIC HEALTH RECORD (EHR) SECURITY

Policy and Standards Compliance Webinar

for Federated or Data Contribution Organizations

Ontario
eHealth Ontario

Agenda

1. Objectives
2. Security Implementation and Adoption Process Flow
3. Security Landscape and EHR Governance Overview
4. EHR Security Policy and Standards Review
5. Security Site Assessment Process Overview
6. Next Steps
7. Questions

eHealth Ontario
It's working for you.

OBJECTIVES

Ontario
eHealth Ontario

Objectives

- Provide an overview of the steps involved in ‘Getting Connected’ to the EHR Solution
- Ensure readiness to comply with the EHR Security Policy and its Standards
- Present the governance structure for Privacy and Security
- Review the high-level obligations and processes required of the EHR Security Policy and its Standards

eHealth Ontario
It's working for you.

SECURITY IMPLEMENTATION AND ADOPTION PROCESS FLOW

Security Implementation and Adoption Process Flow

Step 1

Identify Security Contacts/Resources:

- Sites should work with their eHealth Ontario Implementation and Adoption Leads to identify their Site Security Contacts
- eHealth Ontario Implementation and Adoption Leads will communicate the Site Security Contact(s) to the ConnectingOntario Security (COS) Team

Step 2

Attend EHR Security Site Assessment Webinar:

- Security Contacts attend and participate in the security webinar (we are here)

Step 3

Download EHR Security Policy/Standards and Security Site Assessment Tool:

- Security Officers or Project Manager (PM) download EHR Security Policy and Standards, and Security Assessment Tool via EHR Security Documents

Step 4

Complete and Submit the EHR Security Site Assessment:

- Select appropriate role(s) applicable by your site and complete assessment
- If required, attend drop-in calls to answer any questions related to the Security Policy and Standards
- ***Securely*** communicate the completed security site assessment tool to the COS Team at connecting.security@ehealthontario.on.ca. See Appendices on ***How To Encrypt a Microsoft Excel 2010 Document*** and ***Creating and Communicating a Strong Password***

Security Implementation and Adoption Process Flow (cont.)

Step 5

Review and Evaluate Completed Self-Security Assessment (SSA):

- COS Team reviews, evaluates completed security site assessment, and communicates feedback to Site Security Contact

Step 6

Remediation & Exemption (if any):

- Once SSA is finalized, COS Team pre-populates the Exemption Template and sends exemption draft(s) to the Site to complete and return.
- COS Team is available to assist in Remediation Planning and completing the exemption, upon request
- COS Team scores and validates exemptions requested

Step 7

Exemption Process:

- Exemptions are presented to the eHealth Ontario Strategy Committee by a member of the COS Team
- Sites will be informed of the exemption approval status and receive a status letter upon completion
- Exemptions will be tracked ongoing by the COS team and will follow up with sites as items come due

Step 8

Security Site Assessment Status:

- The COS Team updates Site Coordinators with a general status

eHealth Ontario
It's working for you.

SECURITY LANDSCAPE AND EHR GOVERNANCE OVERVIEW

Security in the News

Massive Data Break Hits
143 Million Americans

Privacy Breach Class Action Certified against Canadian Health Provider

Hospital targeted by cyberattack

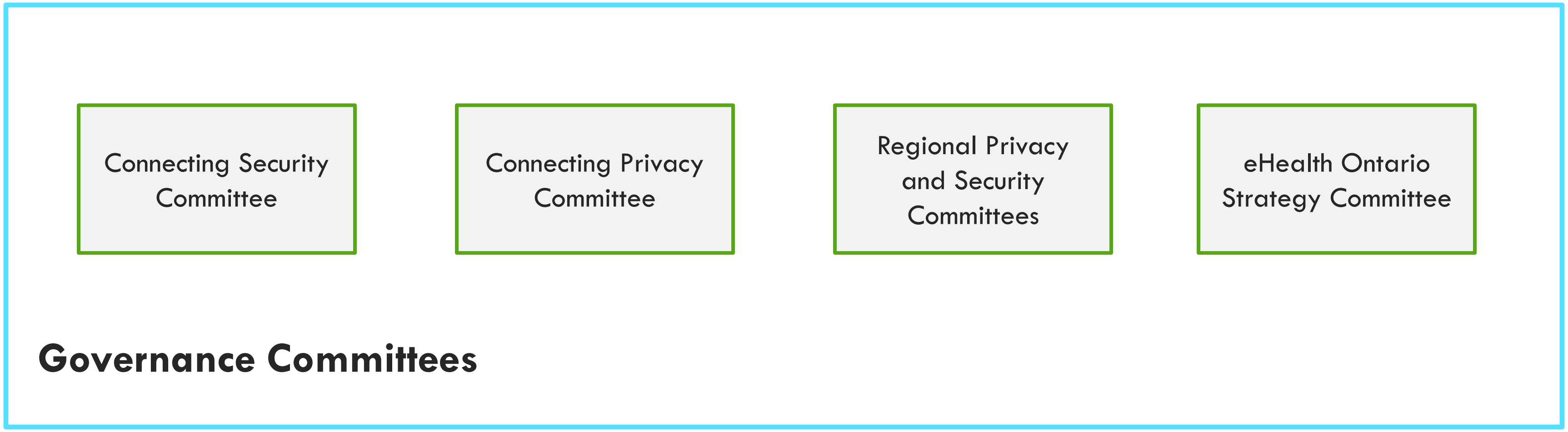
Privacy Commissioner probing missing health records

HUGE ATTACK PARALYSES HOSPITALS

U.S. hospital hit with ransomware only the latest in trend of monetizing cyberattacks

Hospital website may have infected visitors with ransomware, security firm says

What is the Privacy & Security Governance Structure?



Connecting Security Committee

Connecting Privacy Committee

Regional Privacy and Security Committees

eHealth Ontario Strategy Committee

Governance Committees

Information Security Safeguards

- PHIPA requires PHI to be protected by security safeguards
- Electronic Health Record (EHR) Security Policy and its Standards establish mandatory and recommended safeguards
- Developed by the Connecting Security Committee (CSC) with representatives from:
  - eHealth Ontario
  - ConnectingOntario Greater Toronto Area
  - ConnectingOntario Northern and Eastern Region
  - Connecting South West Ontario
  - Canada Health Infoway
- Are being standardized across regional and provincial initiatives (e.g., those funded or operated by eHealth Ontario)
- Sites are bound to the EHR Security Policy and its Standards through agreements with eHealth Ontario

EHR Security Policy/Standards List

1. Information Security Policy
2. Acceptable Use of Information and Information Technology Standard
3. Access Control and Identity Management Standard for System Level Access
4. Local Registration Authorities Practices Standard
5. Business Continuity Standard
6. Cryptography Standard
7. Electronic Service Provider Standard
8. Information and Asset Management Standard
9. Information Security Incident Management Standard
10. Network and Operations Standard
11. Security Logging and Monitoring Standard
12. System Development Lifecycle Standard
13. Physical Security Standard
14. Threat Risk Assessment Standard
15. Identity Provider Standard

Compliance with mandatory ("must"/"shall") requirements is required prior to going live

Sites are bound to EHR Security Policy and Standards through agreements with eHealth Ontario

eHealth Ontario
It's working for you.

EHR SECURITY POLICY AND STANDARDS OVERVIEW

Preparing for Compliance

Ontario
eHealth Ontario

EHR Security Policy/Standards Structure

- EHR Security Policy and its Standards are divided into two sections:
  - 1. Requirements for Health Information Custodians (HIC)s
  - 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 ConnectingOntario, and Hamilton Health Sciences for Clinical Connect)

EHR Security Policy and Standards Structure

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

EHR Security Policy and Standards Requirement Types

There are three types of requirements in the EHR Security Policy and Standards:

- **“Must/Shall” Requirements:** Used for absolute requirements (i.e., 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 security site assessment.

1. Information Security Policy

- **Principles:** High-level principles within the policy direct readers to individual standards
- **Roles and Responsibilities:** Defines the role and responsibilities of the
  - Connecting Security Committee (CSC)
  - eHealth Ontario Strategy Committee (SC)
  - EHR Privacy and Security Operations Team
  - Health Information Custodians (HICs)

Purpose: Outlines the framework for Information Security Governance

- Defines the Information Security principles to manage PHI, the EHR Solution, information systems or information technologies that connect to the EHR Solution
- Establishes the roles and responsibilities for ensuring its principles are implemented and maintained

1. Information Security Policy

Your responsibilities

- Develop, implement and maintain an Information Security policy that upholds the requirements of the EHR Security Policy/Standard
- Designate an Information Security Lead
- Ensure that all Agents and Electronic Service Providers (ESPs):
  - Are aware of their Information Security responsibilities
  - Acknowledge end-user agreement before accessing the EHR Solution
  - Are held accountable for their actions (enforce disciplinary process for non-compliances)

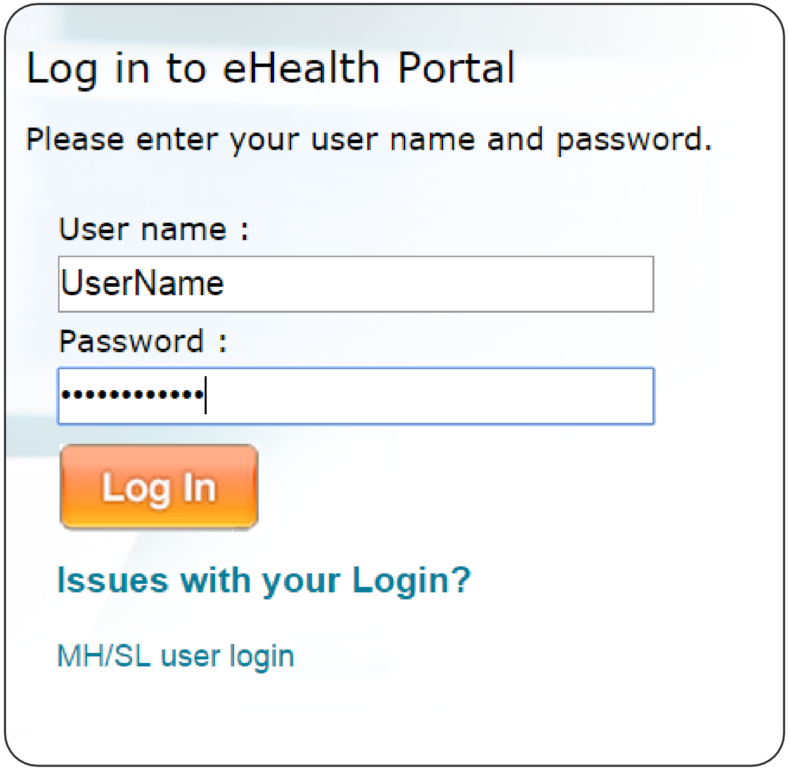
2. Acceptable Use of Information and Information Technology Standard

- **General**
  - Use only assigned credentials
  - Use only HIC-approved tools
  - Prohibits taking pictures of data
  - Lock workstations when logged in and 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 a secure e-mail system (i.e., ONE Mail)

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

2. Acceptable Use of Information and Information Technology Standard

- **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 a user feels their password has been compromised



Log in to eHealth Portal

Please enter your user name and password.

User name : UserName

Password : •••••••••••••

2. Acceptable Use of Information and Information Technology Standard

- **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

2. Acceptable Use of Information and Information Technology Standard

How to prepare

- ✓ Review your site's internal policy, awareness, education, and training programs
- ✓ Identify gaps (e.g., are there missing messages in your internal programs?)
- ✓ Consider using the EHR Privacy and Security training modules to address training gaps
- ✓ Consider using the sample EHR Information Security Policy to address any policy gaps

3. Access Control and Identity Management Standard for System Level Access

Note:

This standard applies to HIC's systems administrators at sites participating in the EHR Solution.

This standard does not address End Users accessing [the EHR Solution]. HICs acting as Identity Providers must follow the Federation Identity Provider Standard for direction and requirements when registering agents to access the EHR Solution and requirements for running IDP services.

General Access Controls

- Provisioned access based on business needs and in accordance with the principles of need-to-know and least-privilege
- Assign unique IDs and ensure that access is traceable to a single person (or information system in the case of Service IDs)
- Configure to deny access by default

Purpose: Defines the logical access control and identity management requirements for secure system level access to a site's Identity Provider (IDP) Services and Data Contribution Endpoint infrastructure that are connected to the EHR Solution

3. Access Control and Identity Management Standard for System Level Access

Administering IDs

- Require the creation/amendment of a user ID to be initiated by a written/electronic request that is approved by a Sponsor
- Maintain a list of IDs and authorization and review annually
- Suspend IDs after 180 consecutive days (or 6 months) of inactivity

Privileged IDs

- Do not name Privileged IDs in a way that provides any indication of the ID's privilege level
- Do not assign privileged entitlements to a Personal ID (e.g., the ID used for normal business activities, such as corporate email account).
- Limit Privileged IDs to minimum number of persons who are directly responsible for operational support or administration

3. Access Control and Identity Management Standard for System Level Access

Authentication

- Ensure that authentication methods that employ the criteria of "something you have" (e.g., digital certificate, SecureID token) permit the unique identification of each person and are not used concurrently by multiple users
- Communicate initial passwords securely
- Encrypt passwords in transmission

Remote Access

- Ensure that additional authentication compensating factors (e.g., two-factor authentication) are required for remote access

3. Access Control and Identity Management Standard for System Level Access

<table>
<tr><th></th><th>Personal IDs & Privileged IDs</th><th>Service IDs</th></tr>
<tr><td><b>Length</b></td><td>Be at least 8 characters.</td><td>Be at least 15 characters.</td></tr>
<tr><td><b>Complexity</b></td><td>Contain at least <b>three</b> of the following:
• At least 1 uppercase character (A through Z)
• At least 1 lowercase character (a through z)
• At least 1 numerical digit (0 through 9)
• At least 1 non-alphanumeric character (~!@#$%^&*_-+=’ |\(){}[]:;"'<>,.?/)</td><td>Contain at least <b>all</b> of the following:
• At least 1 uppercase character (A through Z)
• At least 1 lowercase character (a through z)
• At least 1 numerical digit (0 through 9)
• At least 1 non-alphanumeric character (~!@#$%^&*_-+=’ |\(){}[]:;"'<>,.?/)</td></tr>
<tr><td><b>Additional Password Attributes</b></td><td colspan="2">• Where available, software that prohibits the use of recognizable patterns must be used
• Passwords must not include all or part of the User’s first/last names or any easily obtained personal (e.g., names of family members, pets, birthdays, anniversaries, all or part of a Login ID or a commonly known nickname). See the <i>Acceptable Use of Information and Information Technology Standard</i>
• Initial or temporary passwords must be unique, not guessable, follow the password strength requirements and communicated securely following the requirements of this Standard
• Passwords must not be blank and null passwords must not be used
• Guest passwords must be disabled</td></tr>
</table>

3. Access Control and Identity Management Standard for System Level Access

	Personal IDs & Privileged IDs	Service IDs
Expiration	Up to 1 year can be set for password expiration frequency where the system is compliant with the supporting EHR Security Standard password controls. Otherwise, the password reset frequency must be set to 120 days.	Service IDs are not required to be changed on a scheduled basis however equipment must use a new password when technologies change.
Account Lockout	After ten unsuccessful consecutive attempts.	
Lockout duration	Until manually unlocked by: • An administrator, or • A self-service password reset facility – OR – • Unlocked after a minimum 30 minutes	
History	Last four passwords.	
Minimum Age	Two days.	

4. Local Registration Authorities Practices Standard

- **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
- LRAs are responsible for verifying the identity of individuals at your site who require access to the EHR Solution 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 - Registration and Enrollment aspects of the eHealth Ontario Federation Identity Provider Standard are included in the security assessment for sites to follow.

4. Local Registration Authorities Practices Standard

- Two general types of portals exist:
  - Provider Portals are those used by healthcare providers to assist in patient care
  - Site Administration Portals are those used to support backend functions such as running privacy reports or managing user accounts

Entitlement Criteria:

Provider Portals: Provide access only to those collecting PHI for the purpose of providing or assisting in the provision of healthcare. For example:

- Regulated health professionals
- Residents providing care to patients
- Administrative staff
- Ward clerks

Site Administration Portals: Provide access only to those providing support for defined and permitted functionality. Includes:

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

4. Local Registration Authorities Practices Standard

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.

5. Business Continuity Standard

Ensure that data contribution endpoints related to the EHR Solution and identity provider infrastructure standard requirements are embedded in the business continuity strategy and addresses:

- Developing a resilient technical infrastructure including disaster recovery plans
- Coordinating and maintaining business continuity plans and arrangements
- Validating business continuity plans to ensure requirements can be met

How to Prepare

- ✓ Review existing business continuity plans and identify whether or not they include plans for data contribution endpoints and identity provider infrastructure

Purpose: Defines requirements and recommendations for creating and implementing business continuity plans to help ensure that:

- Access to the EHR Solution remains available or can be restored in the event of a disruption
- The flow of PHI to the EHR Solution is not disrupted

6. Cryptography Standard

Cryptography is aimed at achieving confidentiality, integrity, authentication and non-repudiation of information

Your organization must:

- ✓ Use EHR-approved cryptographic algorithms
- ✓ Designate key custodians
- ✓ Establish appropriate key management activities for cryptographic keys related to IDP services and data contribution endpoints

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

7. Electronic Service Provider (ESP) Standard

- All new ESPs supporting your participation in [the EHR solution] must be assessed for potential information security and privacy risks, prior to entering into a contract
- Define and document all information systems and services to be provided by new ESPs or on renewal of service agreements
- ESPs must implement applicable information security and privacy controls to where they support your participation in the EHR Solution.

How to Prepare

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

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

8. Information and Asset Management Standard

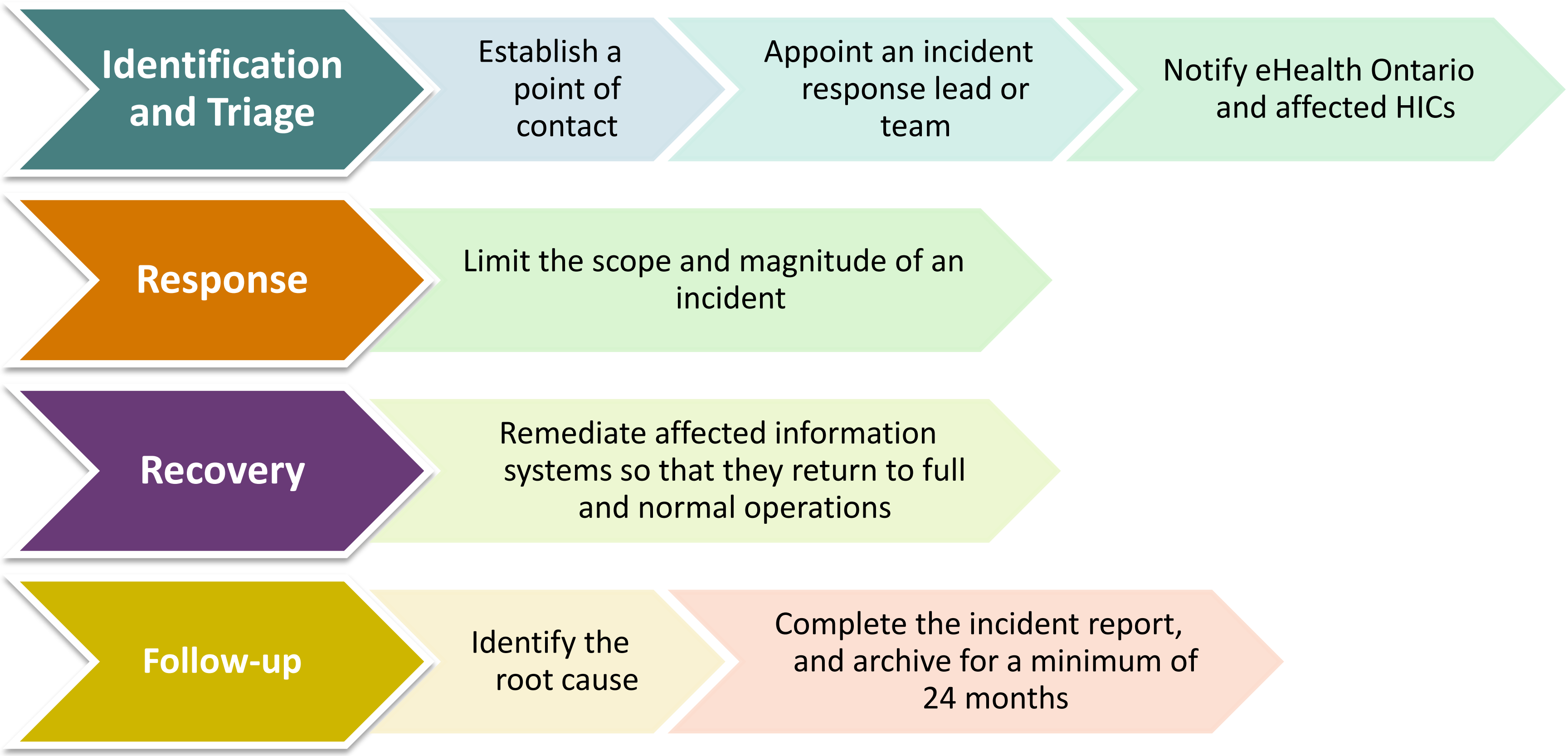
- Requires that organizations securely transmit PHI (i.e., to eHealth Ontario, the EHR Solution Program Offices, or the EHR Solution) through the use of secure email, encryption, or virtual private network tunnel

How to Prepare

✓Determine your site's secure methods of transmitting PHI

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

9. Information Security Incident Management Standard



Identification and Triage

Establish a point of contact

Appoint an incident response lead or team

Notify eHealth Ontario and affected HICs

Response

Limit the scope and magnitude of an incident

Recovery

Remediate affected information systems so that they return to full and normal operations

Follow-up

Identify the root cause

Complete the incident report, and archive for a minimum of 24 months

Purpose: Defines the requirements for creating an Information Security incident ("incident") management process

10. Network and Operations Standard

- Disable unnecessary services, protocols, and ports on IDP services and data contribution endpoints
- Implement network restrictions that secure access to data contribution endpoint services and IDP services administrative functionality to explicitly authorized services or workstations
- Harden IDP services and data contribution endpoints prior to being implemented in the production environment
- Implement malware detection and repair software or equivalent solution on their IDP service and data contribution endpoints to protect from malicious code
- Define a patch management process for patches related to IDPs services and data contribution endpoints

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

11. Security Logging and Monitoring Standard

- Enable logging by default on local IDP technology and data contribution endpoints and log system events/activities

- Implement controls to protect the confidentiality and integrity of logs both in storage and during transmission

- Have the ability to correlate logs to assist in the detection and prevention of misuse or intrusion

- Retain logs for a minimum duration indicated in the Federation Identity Provider Standard and CPC Data Retention Policy (60 days online, 24 months archived)

How to Prepare

✓ Review current logging practices related to your IDPs technology and data contribution endpoints (e.g., HL7 interface engines)

✓ Identify gaps and develop remediation plans

Purpose: Defines the security logging and monitoring requirements for system level events and activities of the EHR Solution and HIC's identity provider technology and data contribution endpoints

12. System Development Lifecycle Standard

- Perform development and testing activities on identity provider services and data contribution endpoints in non-production environments
- Test new identity provider services and data contribution endpoints prior to its promotion to the production environment

How to Prepare

✓ Verify that your site has non-production environments in which data contribution endpoints (e.g., HL7 interface engines) and IDP services can be tested

Purpose: Defines the security controls that are required to securely develop and implement information systems

13. Physical Security Standard

- Implement physical security perimeters to protect IDP services and data contribution endpoints from unauthorized physical access and environmental damage
- Ensure that facilities that house IDP services and data contribution endpoints are not accessible to the public
- Protect power supply for data contribution endpoints and IDP services
- Ensure that data contribution endpoints and IDP services are deployed in locations that meet the vendor-specified requirements for cooling, heating, humidity, and air quality
- 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.

14. Threat Risk Management Standard

- Provides guidance on performing Threat Risk Assessments (TRAs)
- Gives sites the right to request executive summaries (results) of TRAs that are completed on the EHR Solution
- Requires sites to restrict access to a TRA and handle in a secure manner

How to Prepare

- ✓ If you request a review of the TRA, apply security controls and restrict access to authorized individuals

Purpose: Defines requirements for completing Threat Risk Assessments

15. eHealth Ontario Identity Provider Standard

- Outlines requirements regarding accreditation, registration of users, authentication of end users, and service desk functionality
- Authentication must require two or more factors when accessing from the Internet or unsecured environments
- Registration procedures must follow the IDP Standard requirements to meet the assurance level necessary to access personal health information
- The Identity Management system must implement the password requirements, as outlined in the Standard

Purpose: Establishes the mandatory, minimum requirements applicable to Identity Providers. Governs the Registration and Authentication by the IDP of the End User's access to electronic health services, applications, information, and resources accessible over eHealth Ontario's Federated System.

Preparing for EHR Security Standard Compliance

- ✓ Review your site's internal policies, procedures and standards against the EHR Security Policy and its Standards. While "How to prepare for policy compliance" information exists, other items/areas to consider include:

- ▪ Ensure access control and identity management process and procedures exist to manage access provisioning and support of your identity management infrastructure and data contribution endpoints (e.g., HL7 interface engines) that will connect to the EHR Solution

- ▪ Use approved algorithms in cryptographic solutions (including remote access VPN, site-to-site VPN, disk encryption), as specified in the *Appendix of the Cryptography Standard*

- ▪ Assign key custodians and establish a key management process (i.e., secure generation, distribution, loading, storage, recovery, replacement, revocation and destruction, and the secure back-up and archive of cryptographic keys)

- ✓ Engage in Information Security Incident Management by ensuring your processes and procedures align with the EHR Security Policy and its Standards, and can be leveraged to deal with incidents related to the EHR Solution

- ✓ Establish processes for malware detection and repair software, system hardening, and patch management, to protect against malicious codes

- ✓ Identify gaps and develop remediation plans

eHealth Ontario
It's working for you.

WHAT'S INVOLVED IN THE SECURITY ASSESSMENT?

Ontario
eHealth Ontario

EHR Security Policy/Standards Assessment Overview

- The Connecting Security Committee has developed a standard assessment tool called "**EHR Security Policy/Standards Assessment Template**" to be completed by each site prior to participating in the EHR Solution
- The tool is based on Microsoft Excel and allows the site to select the roles they are undertaking with the EHR Solution. The roles as defined in next slide are:
  - Identity Provider
  - Data Contributor
  - Viewer
- Based on the role(s) selected, the applicable EHR Security Standards requirements will be displayed
- Sites are required to complete the tool and submit it

EHR Security Policy/Standards Assessment Overview

- **Data Contributors –** those organizations who send data to the Clinical Data Repository or those organizations that are being queried for data
- **Identity Providers –** those organizations who are leveraging local identities to access the EHR Solution. Typically, these sites log on locally to their HIS system and send a SAML token including Patient Context to the EHR Solution, which authenticates the transaction and sends the data back
- **Viewer –** Viewer sites are those who would typically leverage ONE ID credentials or the credentials of another Identity Provider to access the solution. These sites log on directly to the solution (e.g., Portal) and interact with it. Viewer sites do not relocate or electronically integrate the data into a local solution

Completing the Security Site Assessment Tool

Step 1

Enable Macro on the tool (if not enabled by default):

- Enable Macro after downloading the Security Assessment Tool (See slide: **How To Enable Macro In The Assessment Tool**)

Step 2

Complete Site Profile tab:

- Follow instructions to complete requested information
- Review the role definitions for Data Contributor, Identity Provider, Viewer

Step 3

Complete Control Analysis tab:

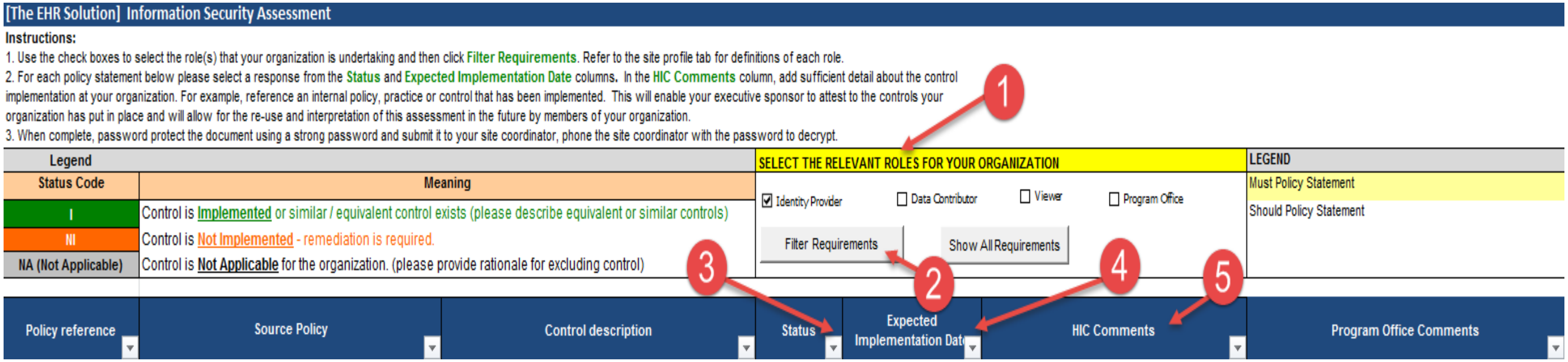
- Read through instructions on how to complete the "Control Analysis" tab
- Select the relevant roles your organization is undertaking as part of the solution and filter the results. (See slide: **EHR Security Policy/Standards Assessment Overview**)

Step 4

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 Slides: **How To Encrypt a Microsoft Excel 2010 Document** and **Creating and Communicating a Strong Password**)
- Phone the Connecting Ontario Security contact with the password to decrypt

High Level Steps to Complete the Assessment Tool



[The EHR Solution] Information Security Assessment

Instructions:

1. Use the check boxes to select the role(s) that your organization is undertaking and then click Filter Requirements. Refer to the site profile tab for definitions of each role.
2. 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 the re-use and interpretation of this assessment in the future by members of your organization.
3. When complete, password protect the document using a strong password and submit it to your site coordinator, phone the site coordinator with the password to decrypt.

Legend

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

SELECT THE RELEVANT ROLES FOR YOUR ORGANIZATION

☑ Identity Provider ☐ Data Contributor ☐ Viewer ☐ Program Office

LEGEND

Must Policy Statement

Should Policy Statement

Policy reference	Source Policy	Control description	Status	Expected Implementation Date	HIC Comments	Program Office Comments

1. Select the relevant role(s).

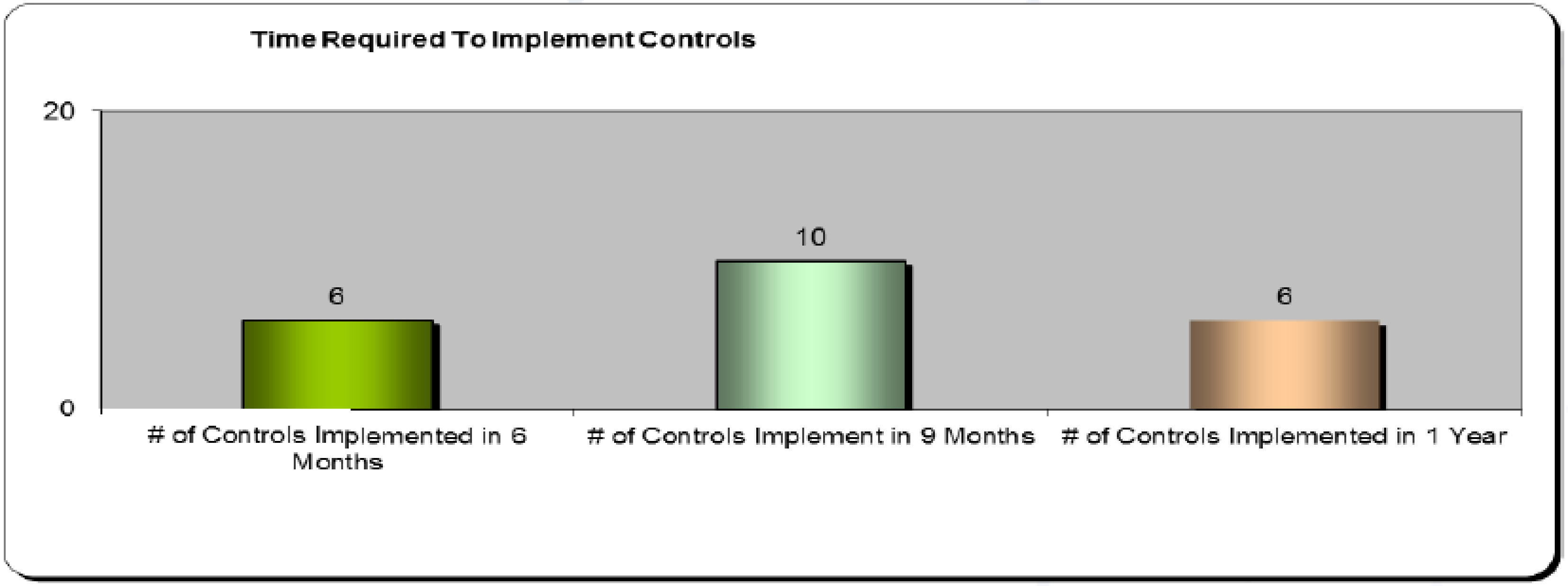
2. Click "Filter Requirements".

3. Review each control and determine if it is "**I**" (Implemented) , "**NI**" (Not Implemented) or "**NA**" (Not Applicable) based on your existing practice.

4. Where status is "**NI**", select when you plan to remediate and provide some initial details. If "**NA**" is selected, indicate what compensating controls are in place to support this answer.

5. Add additional comments if required to make notes regarding control status, remediation planning, etc.

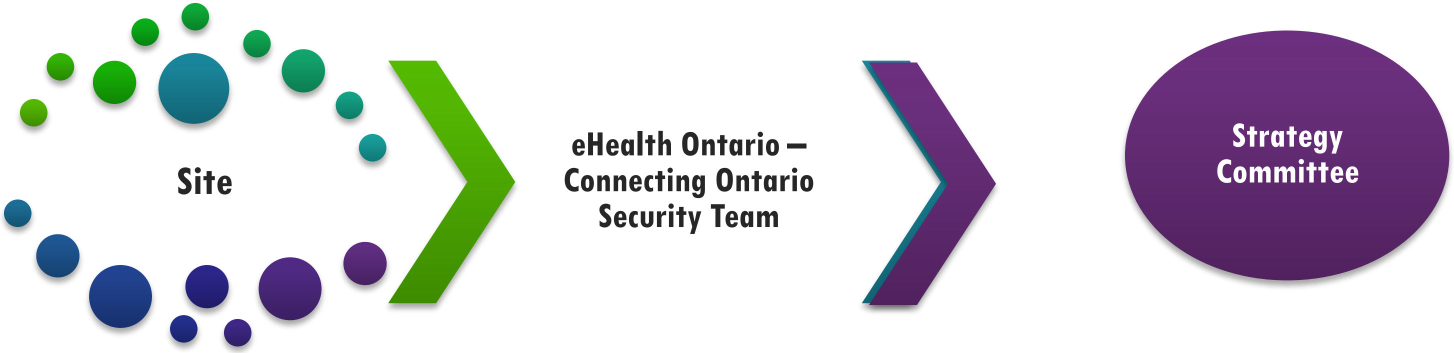
Assessment Tool - Graphical Dashboard



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, Standards, or supporting document must be approved by the Strategy Committee
- All information security exemption requests will be assessed and then reviewed by the ConnectingOntario Security Team, prior to it being sent to the Strategy Committee for approval



Site

- Completes Exemption Request Form
- Encrypts and sends the completed form to the Connecting Ontario Security team.

eHealth Ontario – Connecting Ontario Security Team

- Reviews request
- Assigns risk

Strategy Committee

- Reviews request
- Approves or denies request

Finalizing the Assessment Template

- Ideally, a site submits a single file for all roles selected
- If you cannot submit a single assessment for all roles, sending a file per role (i.e., three (3) role specific assessments) is also acceptable
- Be aware that depending on the role, there may be separate mitigations, exemptions, and approvals
- Where a site is compliant with a control for one role but not another role - this must be noted. Most often, the controls will overlap multiple roles
- Encrypt the document with a strong password and submit to ConnectingOntario Security (COS) team via connecting.security@ehealthontario.on.ca

How Will My Security Assessment Be Protected?

Who will have access to my assessment?

- The ConnectingOntario Security Team at eHealth Ontario including security analysts and leads
- Adoption Delivery Partners may be provided with status information as it related to your sites readiness to “go live”

How will it be shared?

- Encrypted, password protected, and shared with only authorized individuals

Will it be stored and for how long?

- Yes, at eHealth Ontario, with access controls applied and retained for ten years

Contact Information

Contact	At	For
ConnectingOntario Security Team	connecting.security@ehealthontario.on.ca	General inbox for the ConnectingOntario Security Team. Use this address to submit your completed assessment or to request assistance.
eHealth Ontario Privacy (General)	privacy@ehealthontario.on.ca or 1- 416-946-4767	General Ontario's Electronic Health Record privacy questions, individual to make a ConnectingOntario or DI CS Consent Directive, Access and Correction Request, Inquiry, Complaint.
eHealth Ontario Privacy Operations	privacyoperations@ehealthontario.on.ca or 1- 416-946-4767	Privacy Lead to make a ConnectingOntario or DI CS Consent Directive, Access and Correction Request, Inquiry, Complaint, Audit Report; OLIS Audit Report, Privacy Breach Report Summary.
eHealth Ontario's Service Desk	1-866-250-1554 servicedesk@ehealthontario.on.ca	Anyone to report any real or suspected Privacy Breaches, Security Incidents related to ConnectingOntario, OLIS or DI CS.

Do not email PHI (i.e. screenshots, nature of request) to eHealth Ontario
Email your contact information and eHealth Ontario will contact you

eHealth Ontario
It's working for you.

NEXT STEPS

Ontario
eHealth Ontario

Next Steps

- ✓ Review slides on **Security Implementation and Adoption Process Flow** (**Steps 1 – 8**)
  - ✓ Review the 14 EHR Security Standards and Federation Identity Provider Standard, as listed in the slide: **EHR Security Policy and Standards List** and available on the eHealth Ontario web site
  - ✓ Consider how your site can prepare to be in compliance with the EHR Security Policy and its Standards; focus on the gaps that you identified in your *Security Site Assessment*
- ✓ Remember that sites must be compliant with the **must have** requirements prior to going live, or have an Exemption Request approved
- ✓ You will need to submit exemptions about two months prior to go-live

eHealth Ontario
It's working for you.

APPENDICES

EHR Security Policy/Standards & Applicable Roles

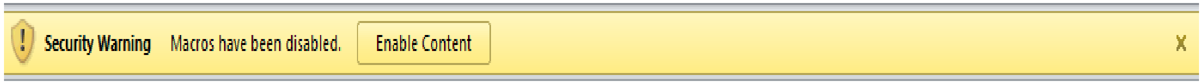
#	EHR Security Policy/Standard Name	Role* (IDP, DC, Viewer)
1	Information Security Policy	All Roles
2	Acceptable Use of Information and Information Technology Standard	All Roles
3	Access Control and Identity Management Standard for System Level Access	IDP, DC
4	Local Registration Authority Practices Standard	All Roles
5	Business Continuity Standard	IDP, DC
6	Cryptography Standard	All Roles
7	Electronic Service Provider Standard	All Roles
8	Information and Asset Management Standard	All Roles
9	Information Security Incident Management Standard	All Roles
10	Network and Operations Standard	All Roles
11	Physical Security Standard	IDP, DC
12	Security Logging and Monitoring Standard	IDP, DC
13	System Development Life Cycle Standard	IDP, DC
14	Threat Risk Management Standard	All Roles
Standard	Federation Identity Provider Standard	IDP

* [Role Legend: DC=Data Contributor; IDP=Identity Provider]

How To Enable Macro In The Assessment Tool

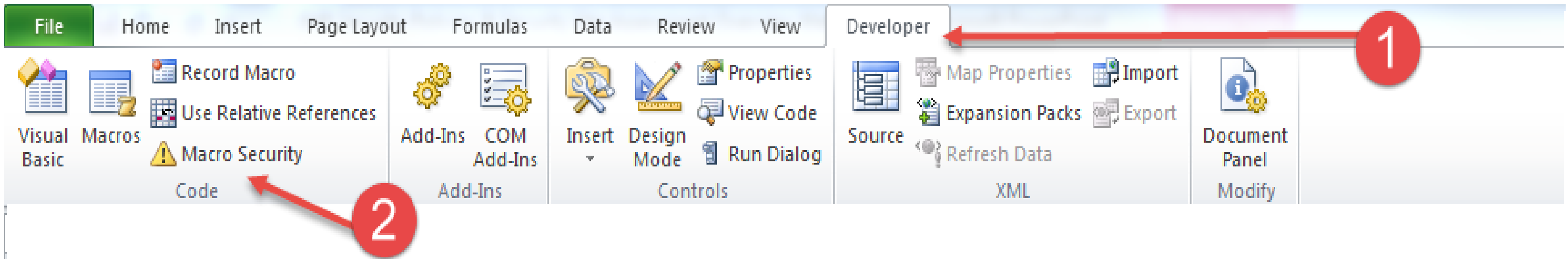
How To Enable Macro, if it’s not enabled by default

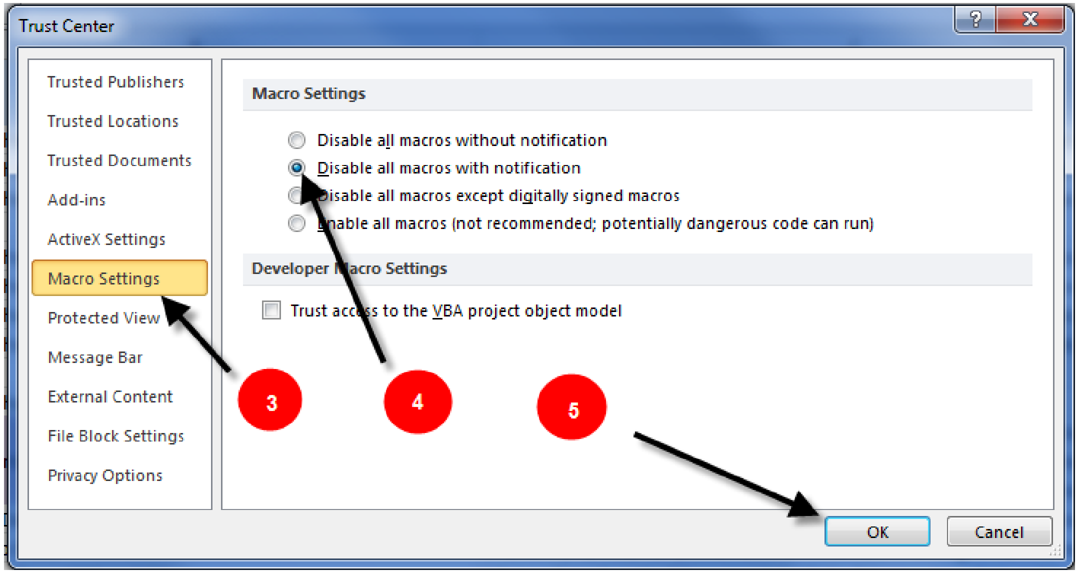
- Click on “Enable Content” button if the Security Warning pops up



Security Warning Macros have been disabled. Enable Content

- In case Security Warning does not appear, follow the steps below





Trust Center

- Trusted Publishers
- Trusted Locations
- Trusted Documents
- Add-ins
- ActiveX Settings
- Macro Settings
- Protected View
- Message Bar
- External Content
- File Block Settings
- Privacy Options

Macro Settings

○ Disable all macros without notification
● Disable all macros with notification
○ Disable all macros except digitally signed macros
○ Enable all macros (not recommended; potentially dangerous code can run)

Developer Macro Settings

□ Trust access to the VBA project object model

<u>**Note**</u>: If the **Developer** tab is not available, do the following to display it:

a. Click the **File** tab, click **Options**.

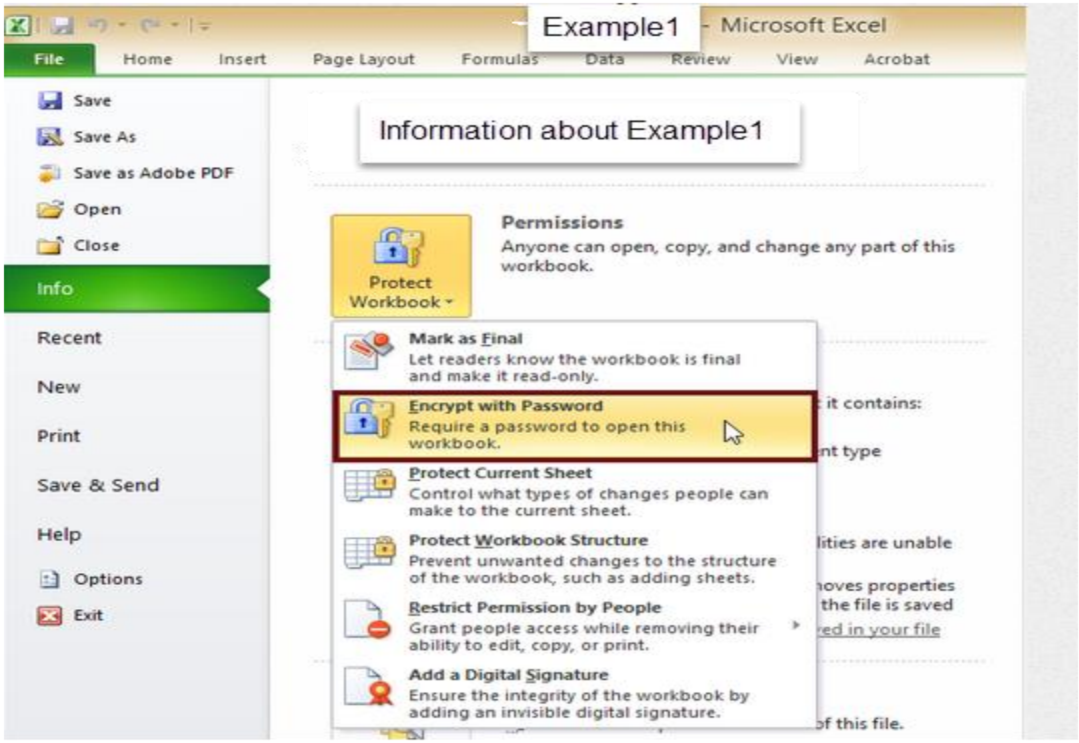
b. Click the **Customized Ribbon** category.

c. In the **Main Tabs** list, select the **Developer** check box and click **OK.**

d. Click any other tab to return to your file.

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. Re-enter password in the **Confirm Password** window.



Anyone can open, copy, and change any part of this workbook.

Let readers know the workbook is final and make it read-only.

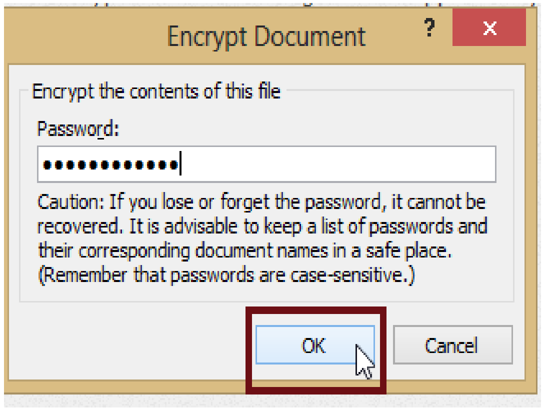
Require a password to open this workbook.

Control what types of changes people can make to the current sheet.

Prevent unwanted changes to the structure of the workbook, such as adding sheets.

Grant people access while removing their ability to edit, copy, or print.

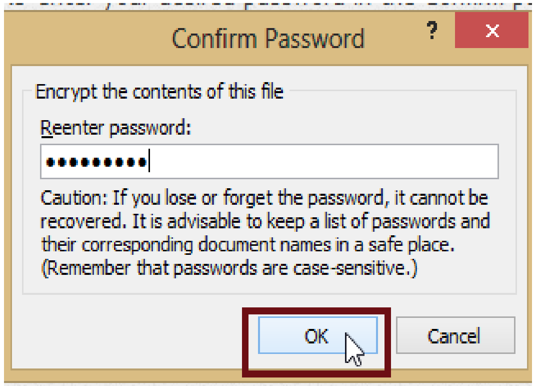
Ensure the integrity of the workbook by adding an invisible digital signature.



Encrypt the contents of this file

Password: ●●●●●●●●●●●●

Caution: If you lose or forget the password, it cannot be recovered. It is advisable to keep a list of passwords and their corresponding document names in a safe place. (Remember that passwords are case-sensitive.)



Encrypt the contents of this file

Reenter password: ●●●●●●●●●●

Caution: If you lose or forget the password, it cannot be recovered. It is advisable to keep a list of passwords and their corresponding document names in a safe place. (Remember that passwords are case-sensitive.)

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)
- Send the encrypted file to connecting.security@ehealthontario.on.ca with your contact information and a member of our Security team call you to retrieve the password

eHealth Ontario
It's working for you.

Thank you for your valuable time today. If you have any questions or need additional assistance, please do not hesitate to contact the ConnectingOntario Security Team at: connecting.security@ehealthontario.on.ca