eHealth Ontario
It's working for you.

PRIVACY OFFICER AND SECURITY OFFICER TRAINING

For Ontario's Electronic Health Record

September 2017

Ontario
eHealth Ontario

Training Outline

	Outline	Duration
1	Overview	10 minutes
2	What's involved in the Security assessment?	15 minutes
3	Privacy Officer and Security Officer Obligations	15 minutes
4	Security Obligations	25 minutes
5	Privacy Obligations	25 minutes
	Next Steps & Resources	Reference
	Contact Information	Reference
	Appendix	Reference

eHealth Ontario
It's working for you.

1. OVERVIEW

Ontario
eHealth Ontario

1. What is Ontario's Electronic Health Record?

Ontario's electronic health record (EHR) enables authorized health care providers to centrally access personal health information exclusively for the purpose of providing or assisting in the provision of health care. It includes:

- **ConnectingOntario Clinical Data Repository (CDR):** clinical reports
- ***Primary Care Clinical Data Repository (CDR):*** *clinical reports*
- **Diagnostic Imaging (DI) Common Services Repository**: diagnostic imaging reports and images
- **Ontario Laboratories Information System (OLIS)**: laboratory test orders and results
- **Digital Health Drug Repository (DHDR):** publically funded drugs and pharmacy services and monitored drugs

Keep in mind how your organization may access this information. For example:

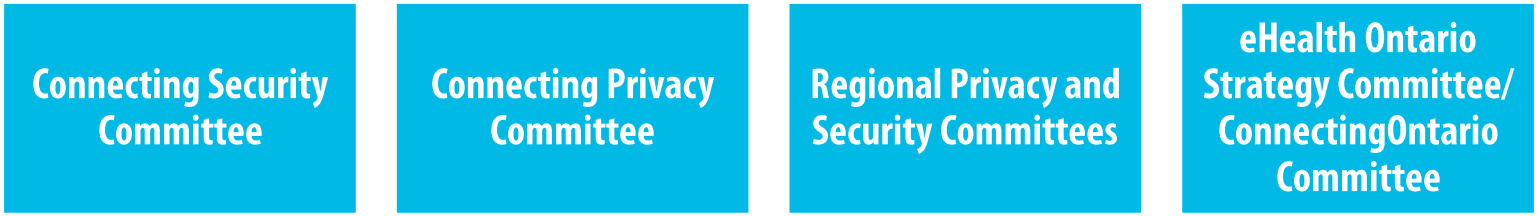
- In South West Ontario, Ontario's Electronic Health Record is accessed using ClinicalConnect™
- In the Greater Toronto Area and Northern and Eastern Region, Ontario's Electronic Health Record can be accessed using the ConnectingOntario ClinicalViewer

Information available may vary between organizations and systems.

Everything related to an individual that is viewable in Ontario's Electronic Health Record is personal health information:

- Patient Demographics
- Visit/Encounter Details
- Emergency Department Reports
- Consultation Reports
- Discharge Summaries
- Allergy Information
- Medication Profile
- Cardiovascular Reports
- Neurophysiology Reports
- Respiratory Reports
- Diagnostic Imaging Reports
- Infection Control Information
- Mental Health Reports
- LHIN (formerly CCAC) Information (e.g. Assessments, and LTCH Placement Details)
- Consent Directives and Overrides
- Laboratory Data

1. How is Privacy and Security Governed in the EHR?



The Committees recommend a consistent and sustainable approach to privacy and security in Ontario's Electronic Health Record including the development of the ***Electronic Health Record Privacy and Security Policies***.

The Electronic Health Record Policies are comprised of policies and procedures that:

- Allow for a streamlined patient experience
- Foster a common approach to safeguarding personal health information in a shared environment
- Help to mitigate privacy and security risks to an organization

To ensure the various health care organizations are represented in the decisions made by the Committees, members consult the regional Privacy and Security Working Groups.

For a list of the Electronic Health Record Privacy and Security Policies, refer to Appendix A.

1. What Are the Privacy and Security Requirements for the EHR?

PHIPA requires PHI to be protected by security safeguards. Electronic Health Record (EHR) Security Policy and its Standards establish mandatory and recommended safeguards. Please see the reference below to locate the privacy and security policy and procedure requirements for each system or repository you may participate in:

System/ Repository	Policy and Procedure Reference
ConnectingOntario Clinical Data Repository (CDR) accessed via the *ConnectingOntario Clinical Viewer* or the *ClinicalConnect Clinical Viewer*	Electronic Health Record (EHR) Policies/ Health Care Provider Guide
Diagnostic Imaging (DI) Common Services	Electronic Health Record Policies/ Health Care Provider Guide
Ontario Laboratories Information System (OLIS)*	Health Care Provider Guide
Digital Health Drug Repository (DHDR) or Publicly Funded Drugs and Pharmacy Services and Monitored Drugs*	Health Care Provider Guide

Updates to requirements are provided to the Authorized Representative at your organization (as per the agreements) and via the Privacy and Security Working Groups.

Note: HICs in the SWO that contribute personal health information to the ConnectingOntario CDR are bound by two sets of EHR privacy policies and two 'Program Offices' i.e., eHealth Ontario and ClinicalConnect

Client Support:

- Electronic Health Record Policies
- Health Care Provider Guide
- eHealth Ontario Electronic Health Record (EHR) Contributor Agreement
- eHealth Ontario EHR Contributor Agreement Amendment Schedule B

*MOHLTC is the Health Information Custodian.

1. What Are the Privacy and Security Prerequisites for Getting Connected?

Before answering assessment questions:

1. Familiarize yourself with the EHR program
2. Review EHR Policies and resources available in Privacy Toolkit
3. Complete Privacy Officer and Security Officer training

Client Support:

- Electronic Health Record Policies
- Health Care Provider Guide
- Security Quick Start Guide: Securely Connecting to EHR
- Summary of Security Obligations
- EHR Privacy Toolkit

Refer to Appendix B for instructions on how to complete the Privacy Readiness Assessment Tool.

eHealth Ontario
It's working for you.

2. WHAT'S INVOLVED IN THE SECURITY ASSESSMENT?

2. 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.

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***

2. 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
- 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

10

2. 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:
  - **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

2. 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

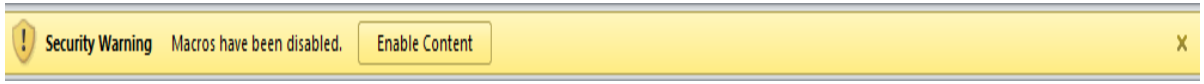
Submit Complete Assessment:

- 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

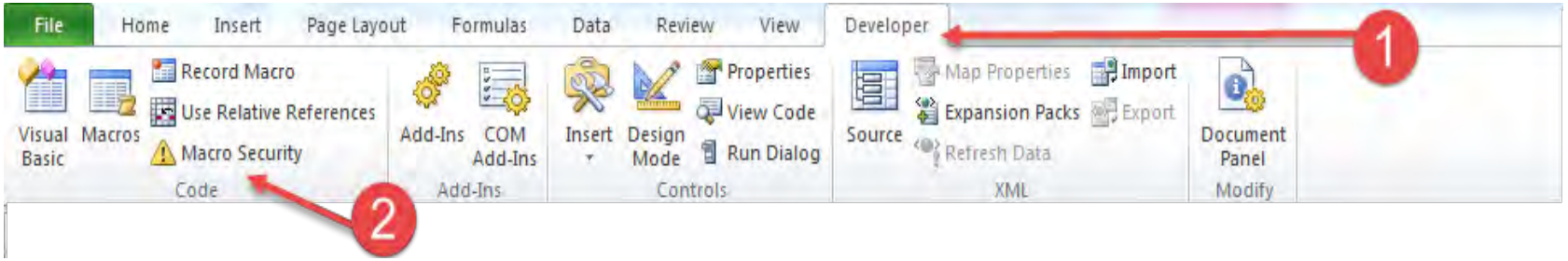
2. How To Enable Macro In The Assessment Tool

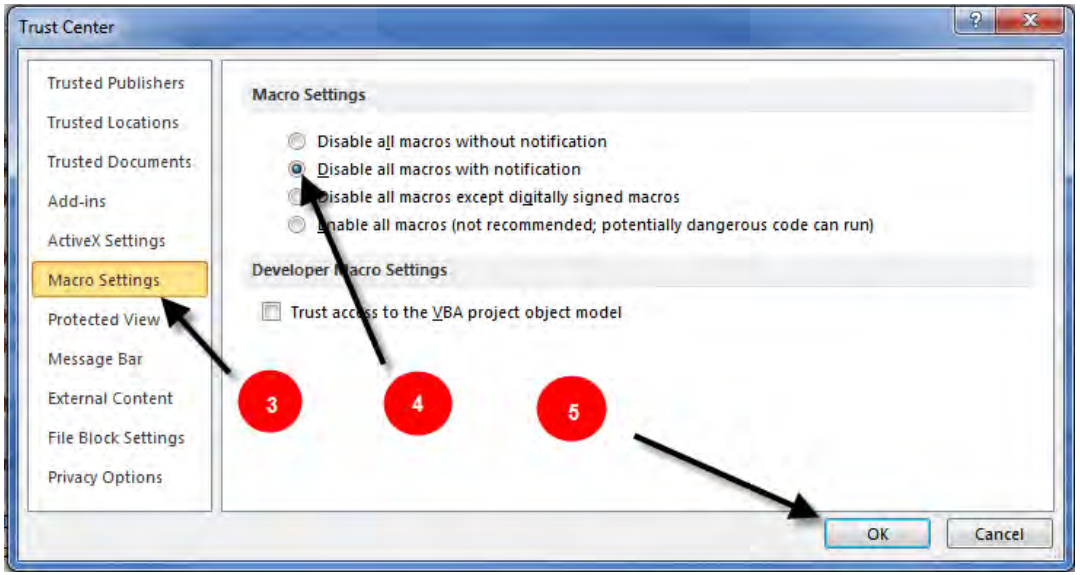
How To Enable Macro, if it's not enabled by default

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



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

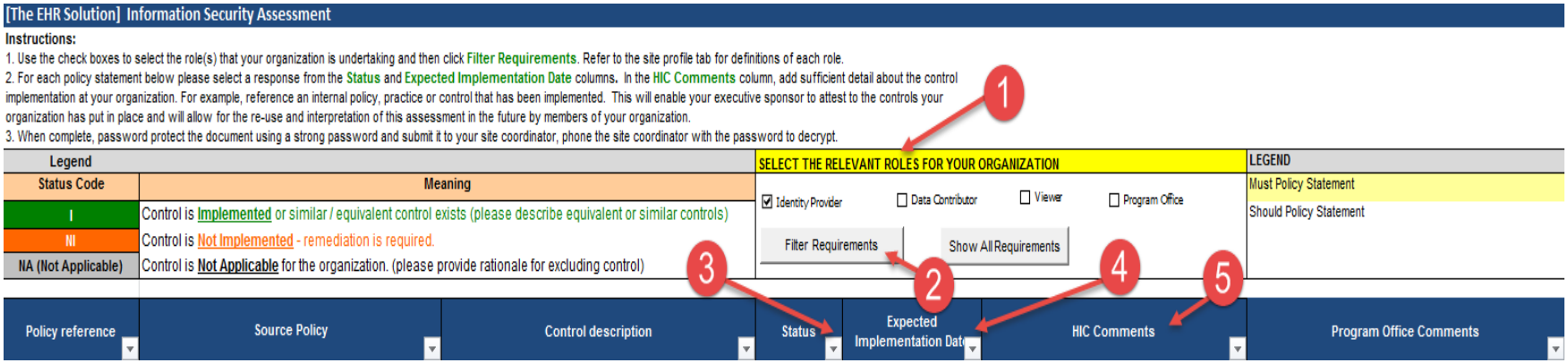




Note: If the **Developer** tab is not available, do the following to display it:

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.

2. High Level Steps to Complete the Assessment Tool



1. Select the relevant role(s).

2. Click "Filter Requirements".

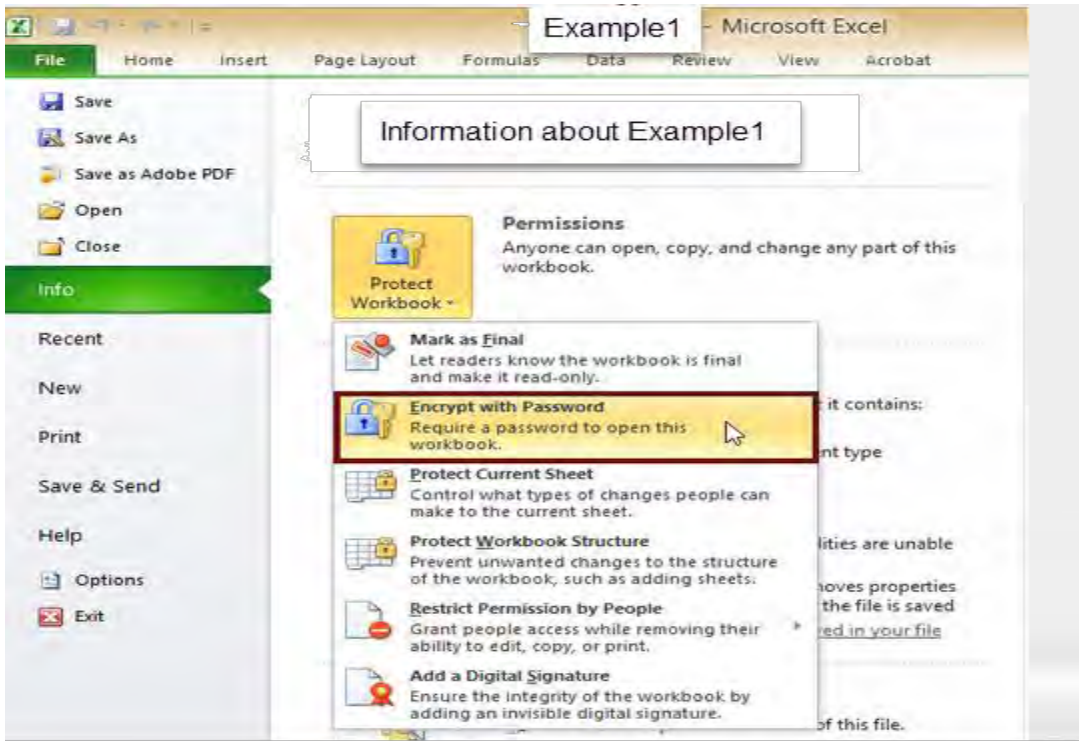
3. Review each control and determine if it is "**I**" (Implemented) , "**NI**" (Not Implemented) or **"NA"** (Not Applicable) based on your existing practice.

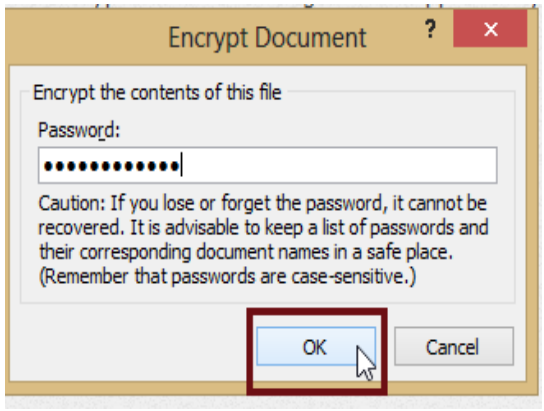
4. Where status is "**NI**", select when you plan to remediate and provide some initial details. If **"NA"** is selected, indicate what compensating controls are in place to support this answer.

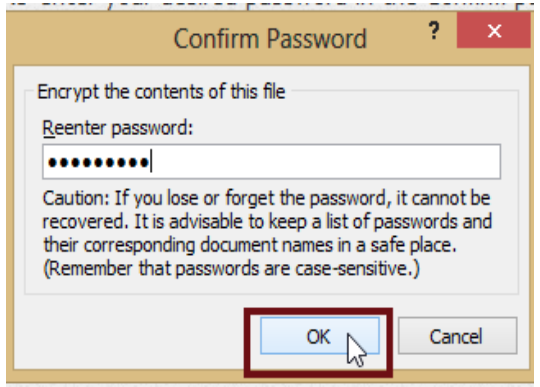
5. Add additional comments if required to make notes regarding control status, remediation planning, etc.

2. How To Encrypt a Microsoft Excel 2010

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.







2. 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

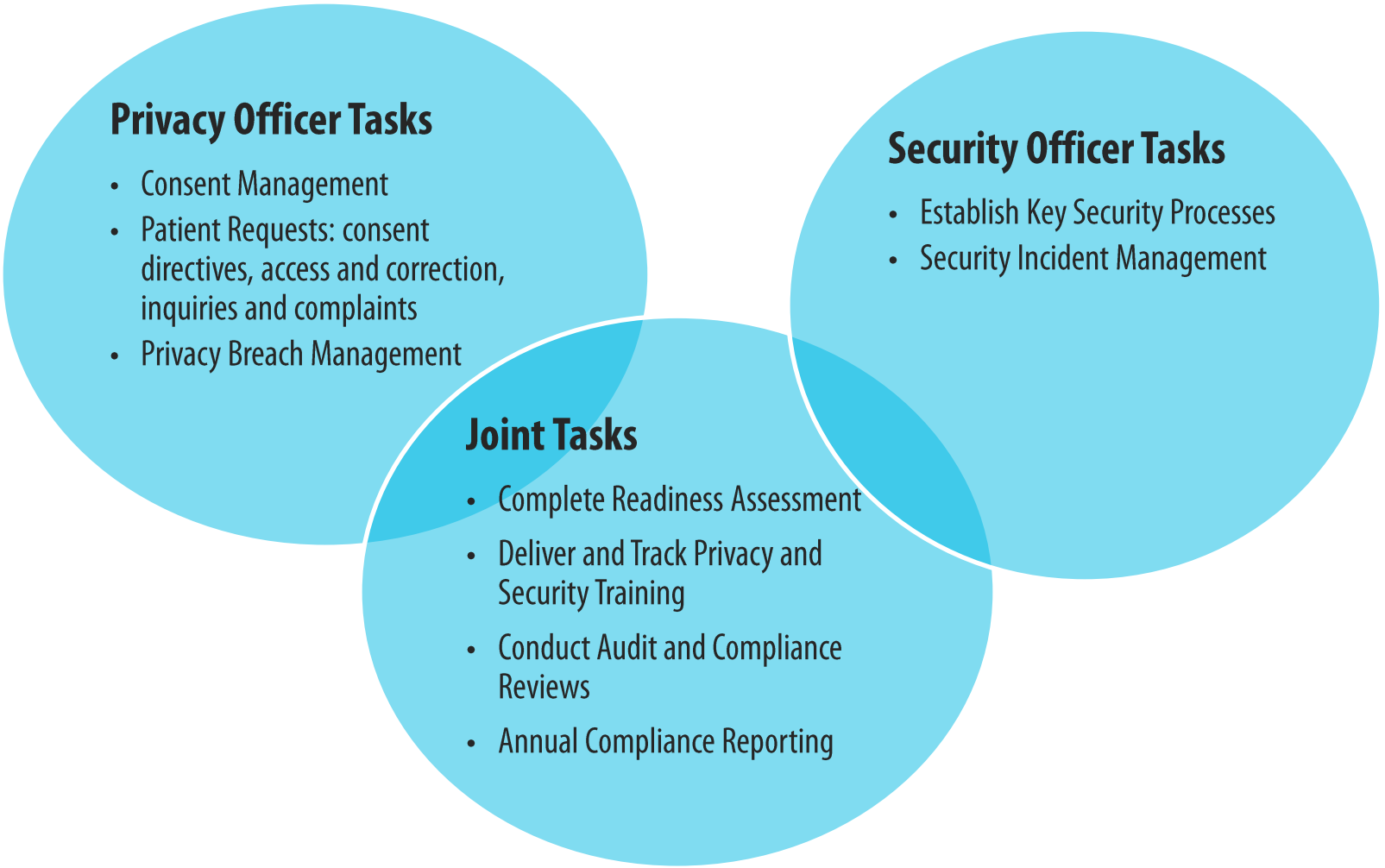
eHealth Ontario
It's working for you.

3. PRIVACY OFFICER AND SECURITY OFFICER OBLIGATIONS

Ontario
eHealth Ontario

3. What does a Privacy Officer and Security Officer Do When Participating in the EHR?

The Privacy Officer and Security Officer is responsible for managing the privacy and security programs at your organization. Many assurance tasks carried out in respect of the EHR are managed jointly:



3. What Is Assurance And What Am I Required To Do?

Assurance ensures your organization and its agents and ESPs are compliant with the EHR policies and procedures. This enables trust amongst participating organizations that each has a comparable level of personal health information protection and safeguards implemented.

	Ensure Agents and ESPs Are Compliant	Report Compliance
Prior to go-live	✓ Deliver and Track Privacy and Security Role-Based Training	✓ Identify "Readiness" to Connect to the EHR
Participating in the EHR	✓ Request and Review Privacy Audit Reports ✓ Investigate Consent Directive Overrides and Security Alerts ✓ Deliver and Track Annual Privacy and Security Role-Based Training	✓ Annually Attest Compliance

3. How Do I Report Compliance?

Privacy Readiness Assessment and Security Readiness Assessment

Complete the assessments provided by eHealth Ontario prior to contributing/collecting

- Review your organization's existing policies, procedures and standards against the EHR Policies and 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)
- Identify risks to compliance
- Develop mitigation plan to address gaps in your existing Privacy and Security Program
  - ✓ 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

3. How Do I Report Compliance?

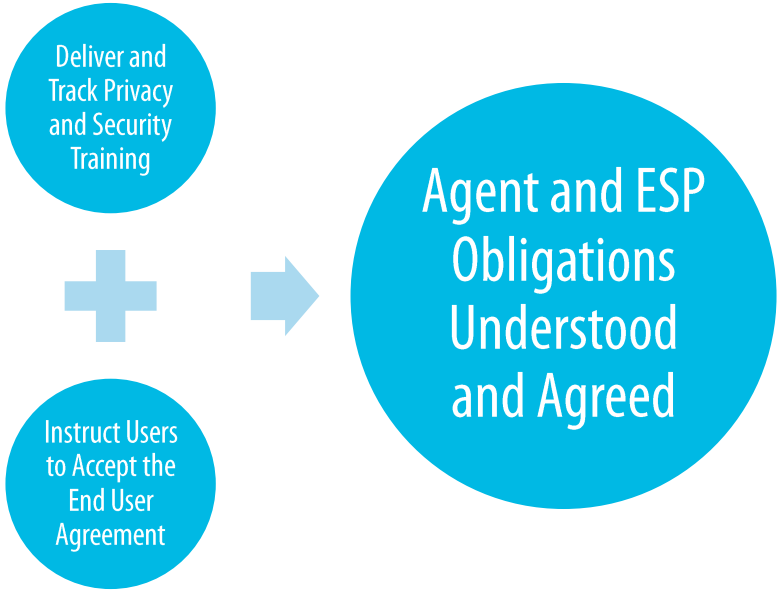
Annual Self-Attestation

Annually attest to compliance with the EHR Policies

1. eHealth Ontario to issue request to complete Self- Attestation to Authorized Contact, Privacy Officer and Security Officer
    - Request issued by EHR Program Office April (Q1)
2. Instructional session and privacy officer refresh training (optional)
    - Scope: how to complete letter; refresher of privacy requirements; reminder of policy changes
3. Site to review privacy and security requirements outlined in previously completed privacy and security readiness assessment
    - Report Status of Risks (Closed, Open, New) and Mitigation Plan
4. Site to submit signed letter to eHealth Ontario by end of Quarter (Q1)
    - Response required June (Q1)
5. Mitigation Plan to be reviewed and approved by EHR governing bodies

3. What Do I Need to Tell My Staff and Vendors?

Privacy Officer and Security Officer must:



- Before a user is granted access to the EHR, these tasks must be completed and on an annual basis.
- Ensure only authorized users are granted access to the EHR (to provide or assist in the provision of health care).
  Note: If your organization performs research, include a check in the approvals process that Ontario's EHR systems may not be used for this purpose.

Note: Users accessing the ConnectingOntario ClinicalViewer and ClinicalConnect ClinicalViewer will accept the End User Agreement when logging in to the system for the first time. Administrative staff must physically sign a copy of the Electronic Health Record Portal User Agreements, available on the eHealth Ontario website.

3. How Do I Deliver and Track Training?

Your organization must train and track completion of agents and ESPs accessing the EHR from your organization of their duties prior to accessing the system and annually thereafter.

There is a standard EHR privacy and security training available for the following roles:

- Clinicians
- Newly on-boarded local registration agents (who register users on the EHR)
- Technical Staff (i.e. testers, Help Desk, staff that maintain the connection to the EHR)

Training Courses with the mandatory messaging are available for you to leverage as is or you can incorporate this messaging into your existing privacy and security training program.

Review the **EHR Strategy** to:

1. Classify your organization's training profile
2. Understand the menu of delivery options available- the courses are available in various outputs for flexibility., timelines in which training must be delivered and tracking methods available

3.What Auditing and Monitoring Activities Am I Required to Perform?

Your organization must perform auditing and monitoring activities to identify suspicious activities, risks or areas of non-compliance.

- ❑ Establish an auditing and monitoring process at your organization leveraging the *Auditing and Monitoring Guide*
- ❑ Reports should be reviewed:
  - ✓ On a regularly-scheduled basis according to agreement requirements and the frequency established at your organization
    - Organizations viewing the EHR: an audit must be performed at a minimum of a quarterly basis
  - ✓ If you If you suspect that PHI was inappropriately collected, used, or disclosed
  - ✓ When the EHR Program Office provides you with a Consent Directive Override Report or Security Alert*
- ❑ Request reports from the EHR Program Office (refer to EHR Contact Matrix)
- ❑ Review reports and investigate
- ❑ Report actual or suspected breaches to EHR

Privacy Toolkit:
- **Audit and Monitoring Guide**
- **Audit Report Request Form (coming soon)**
- **Audit Report Output Sample (coming soon)**

Reminder: the EHR Program Office will only intake reports or email reports to the designated Privacy Lead for investigation (unless a delegate is noted otherwise).

*Investigating these reports can be counted toward meeting the quarterly audit requirement.

3. Incident and Breaches 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

3. What Should I Have in Place to Be Prepared for A Privacy Breach?

Your organization should have in place the following to be prepared to handle a privacy breach:

- ❑ Point of contact for reporting actual or suspected Privacy Breaches.
- ❑ Disciplinary procedures for Individuals responsible for a Breach.

Consequences of Breach

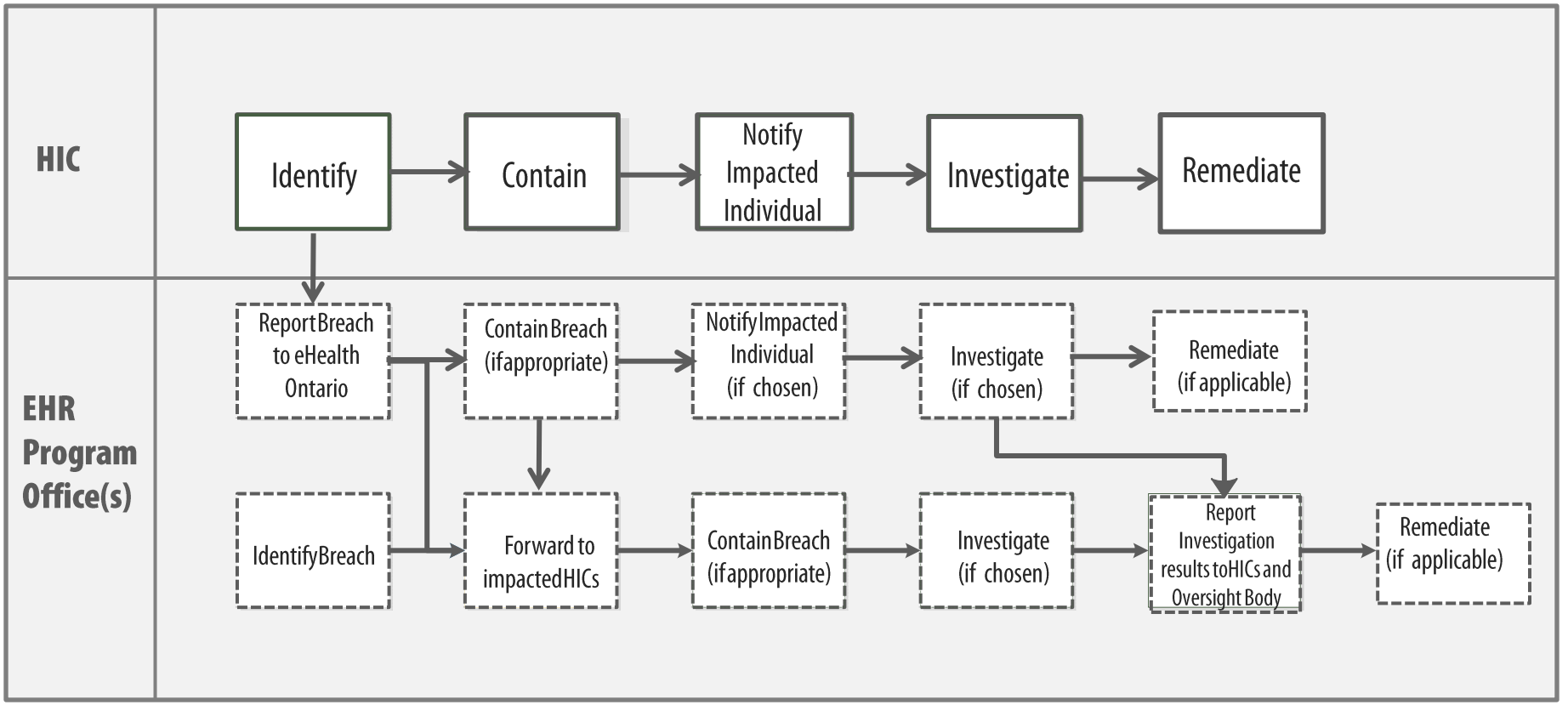
- Be aware that the Oversight Body reviews breaches and may require containment, remediation, and prevention activities from your organization (as per the agreements signed)
  - A Privacy Breach may result in a user's access being terminated
  - Person responsible for the breach may be subject to increased monitoring and auditing- you may need to support these activities
  - Your organization may be subject to an investigation by the Information and Privacy Commissioner of Ontario

In the event you become aware of an actual or suspected privacy breach, the steps you follow depend on:

1. Who caused the breach
2. Who contributed the personal health information subject to the breach

Privacy Toolkit:
- **Privacy Breach Log**
- **Privacy Breach Report**

3. Privacy Breach Management



Legend

Existing Step	New Step

3. What Do I Do Once I Become Aware of A Privacy Breach ?

Where Only Your Organization Contributed the Personal Health Information

Step 1 – Report *Any* Breaches

- ❑ Users will report suspected or actual privacy breach to Privacy Lead
- ❑ Report any *confirmed* breaches, or where there is a reasonable suspicion that a Privacy Breach has occurred involving Ontario's Electronic Health Record, inform the the EHR Program Office a soon as possible but no later than the end of the next business day.

Step 2 – Contain, Investigate, Notify, and Remediate

- ❑ Contain, investigate, notify, and remediate according to your internal policies and procedures

Step 3 – Summary of the Investigation Results

- ❑ Provide a summary of the investigation results to EHR Program Office and the individuals to whom the personal health information relates

Privacy Toolkit:
- **Privacy Breach Log**
- **Privacy Breach Report**

3. What Do I Do Once I Become Aware of A Privacy Breach ?

Where Other Organizations Contributed the PHI

Step 1 – Report *All* Breaches

- ❑ Users will report suspected or actual privacy breach to Privacy Lead
- ❑ Report all confirmed breaches, or where there is a reasonable suspicion that a Privacy Breach has occurred, involving Ontario's Electronic Health Record to EHR Program Office as soon as possible but no later than the end of the next business day after the Privacy Lead becomes aware of the issue
  - Use the *Notification Report to eHealth Ontario Template*

Step 2 – Contain the Breach

- ❑ Containment must begin as soon as possible to prevent a small Breach turning into a big one!
- ❑ If multiple health information custodians (or their agents or ESPs) caused the Breach, the health information custodians may choose an appropriate health information custodian to contain the Breach – this will be coordinated by EHR Program Office

Privacy Toolkit:
- **Notification Report to eHealth Ontario Template**
- **Privacy Breach Log**

3. What Do I Do Once I Become Aware of A Privacy Breach ?

Step 3 – Notify Individuals impacted by the Breach

- Notification must happen as soon as reasonably possible if personal health information is "stolen, lost, or accessed by unauthorized persons"; *PHIPA, s12 (2)*
- ❑ The health information custodians (HIC) impacted by the Breach will choose the most appropriate HIC to notify
- ❑ Notification is provided to the Individual following the organization's existing processes

Who Notifies?

The HICs impacted by the Breach will identify a HIC to notify based on:

- The HIC where the Individual typically receives care
- The HIC that caused the Breach
- The HIC where the Individual most recently received care

Step 4 – Investigate the Breach and identify remediation steps

- ❑ Identify Investigation Lead
- ❑ Investigation to begin within 7 days
- ❑ Report to be written within 7 days of completing the investigation
- ❑ Impacted health information custodians have 7 days to comment on the report

Who Investigates?

Investigator can be:

- HICs that were impacted by the Breach, and
- HIC(s) or eHealth Ontario that caused the breach

Step 5– Summary of the Investigation Results

- ❑ Provide a summary of the investigation results to EHR Program Office and the individuals to whom the personal health information relates

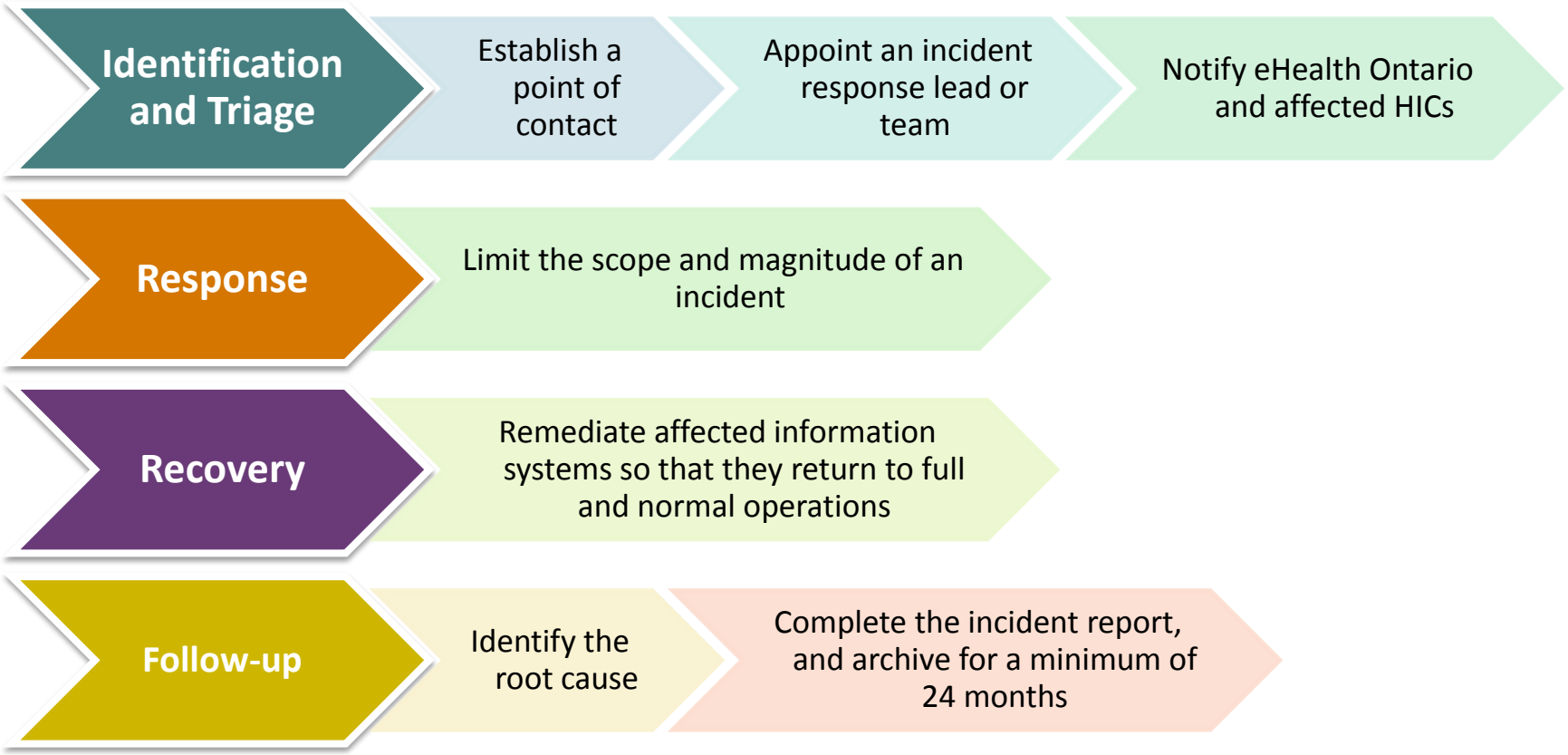
Step 6 – Remediating a Breach

- ❑ Conduct the remediation steps requested by the Oversight Body
- ❑ Status updates to be emailed to eHealth Ontario Service Desk every 30 days until mitigated

Privacy Toolkit:

- Privacy Breach Log
- Privacy Breach Report

9. Information Security Incident Management Standard



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

eHealth Ontario
It's working for you.

4. SECURITY OBLIGATIONS

Ontario
eHealth Ontario

4. 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 Connecting Ontario, and Hamilton Health Sciences for Clinical Connect)

4. 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

4. 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.

4. 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

4. 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)

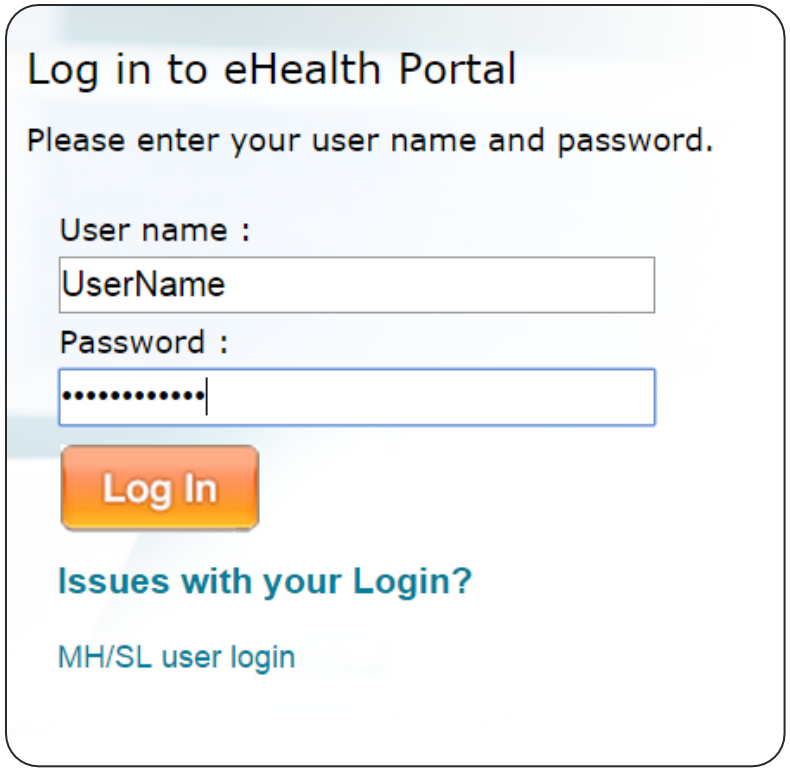
4. 2 - Acceptable Use of Information and Information Technology Standard

- **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

4. 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



4. 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

4. 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

4. 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

4. 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

4. 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

4. 3 - Access Control and Identity Management Standard for System Level Access

	Personal IDs & Privileged IDs	Service IDs
Length	Be at least 8 characters.	Be at least 15 characters.
Complexity	Contain at least **three** 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 (~!@#$%^&*_-+=′|\(){}[]:;"'<>,.?/)	Contain at least **all** 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 (~!@#$%^&*_-+=′|\(){}[]:;"'<>,.?/)
Additional Password Attributes	• 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 *Acceptable Use of Information and Information Technology Standard* • 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	

4. 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. 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. 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. 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.

4. 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

4. 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

4. 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)

4. 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

4. 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

4. 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

4. 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

4. 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.

4. 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

4. 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.

eHealth Ontario
It's working for you.

5. PRIVACY OBLIGATIONS

Ontario
eHealth Ontario

5. What Should My Privacy Program Have?

1. **Privacy Officer contact** - lead for privacy at your organization, responsible for compliance with the EHR Privacy Policies. eHealth Ontario identifies this individual from the *Client Information Form* signed by the Authorized Representative at your organization.
   Privacy Office Delegates – send a written confirmation to privacy.operations@ehealthontario.on.ca of individuals authorized to request and/or receive reports with PHI.
   Privacy Officer replacement – send a written update to agreements@ehealthontario.on.ca or complete the *eHealth Ontario Client Information Form*.

2. **Internal privacy policy and procedures** - enables you to address privacy requests and activities required in the EHR Privacy Policies.

   Privacy Toolkit:
   - Sample Policy Guide – Privacy Policy and Operating Practices Manual

3. **Secure method of transmitting PHI to eHealth Ontario** – ONE Mail is a secure transmission (additional protections not required) or password protect and encrypt forms and reports to eHealth Ontario (i.e. WinZip). Please note, all emails to the eHealth Ontario Service Desk must be encrypted.
   - eHealth Ontario will always encrypt files when circulated externally.

4. **Document classification** - ensure you retain documents related to the EHR in accordance with the EHR Retention Policy (see Appendix C).

5. What Privacy Activities Am I Responsible For?

As the Privacy Officer, your privacy program is responsible for handling the following:

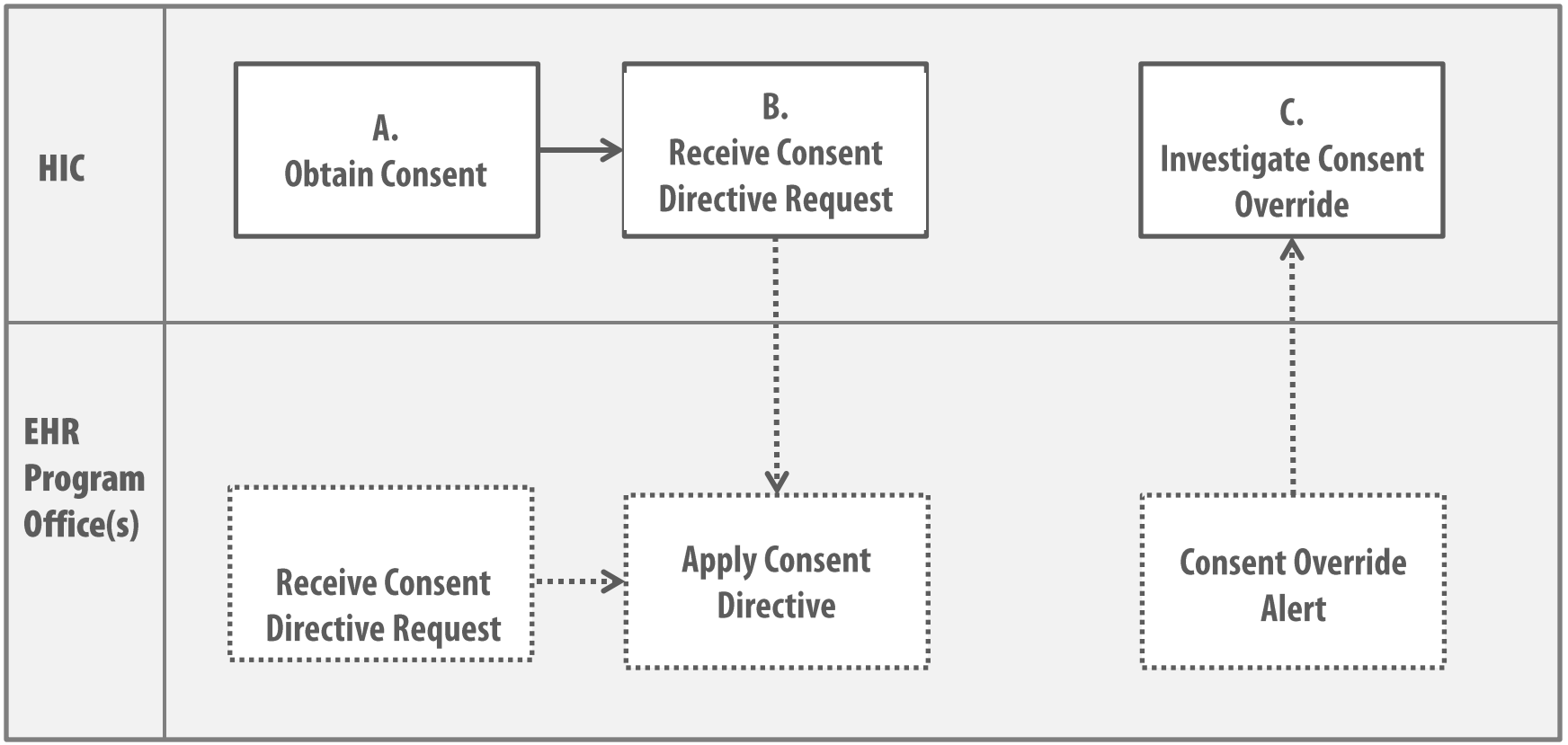
- Consent Management
- Access and Correction
- Inquiries and Complaints

Clinical and Technical Support staff are trained to direct patients to you in the event there are questions or requests related to privacy.

The **EHR Program Office** will provide support for certain tasks. Refer to the *eHealth Ontario Privacy Office* as the point of contact for EHR Program Office for CDR and DI CS. The *ClinicalConnect Program Office* should be contacted for all requests related to the ClinicalConnect Clinical Viewer.

5. Consent Management

The following outlines the existing steps performed at your organization and new steps that will be carried out to support consent management in respect of the EHR.



Legend

Existing Step

New Step

A. How do I Receive Consent at my Organization?

Participating organizations may collect, use and disclose personal health information in Ontario's Electronic Health Record for health care purposes with the individual's consent.

The individual's consent may be express or implied, according to your organization's practices. Reflect your participation to ensure an individual is knowledgeable by:

1. Updating your existing notices, brochures, website, and other communication channels to ensure it includes the following:
   - ❑ General description of the PHI
   - ❑ Administrative, technical and physical safeguards and practices to protect PHI
   - ❑ Persons and organizations that may view PHI
   - ❑ Purposes for which PHI is viewed
   - ❑ Individual's right to manage consent
   - ❑ Contact information for the Privacy Officer or equivalent to handle privacy-related requests
   - ❑ Contact information for the Information and Privacy Commissioner to make a privacy-related complaint

2. Making available the notices pertaining to each system you participate*:
   - ❑ ConnectingOntario ClinicalViewer/ClinicalConnect Patient Notice
   - ❑ ConnectingOntario ClinicalViewer/ClinicalConnect Patient Brochure
   - ❑ OLIS Patient Information Sheet
   - ❑ DI CS Patient Notice

3. Using a layered approach- make brochures and posters available, have a conversation with the individual then refer them to the eHealth Ontario (and ClinicalConnect's) website.

*Contact your Change Management and Adoption Delivery Partner for more information on the patient notices.

A. What Can Be Done if the Individual Does Not Want to Share Their PHI?

Individuals may manage access to their personal health information by asking for a block or **consent directive** to be added to their record.

- A consent directive gives individuals - or their substitute decision makers - the option to restrict access to personal health information in the electronic health record. This means that when a clinician tries to access the record, a notice pops up indicating the record is blocked.
- Just because access is restricted does not mean that the record will be out of date – new information will continue to be added throughout an individual's health care journey. The individual can always unblock the record at any time. Once applied or removed, the individual will a receive confirmation that the consent directive is in place or has been lifted.

B. How Can an Individual Block Access to Their PHI (Request a Consent Directive)?

Where an Individual or substitute decision-maker makes a Request will vary on the scope of the request:

1. **Contact Privacy Officer (You)**
   This method is ideal where the individual would like to place a consent directive for the organization's health information system, other shared systems as well as Ontario's Electronic Health Record.

2. **eHealth Ontario Privacy Office**
   This method is ideal where the individual would like to place a consent directive only in Ontario's Electronic Health Record.
   1. Mail or Fax a completed copy of the Patient Consent Directive Request Form
   2. Call (or provide an email with contact information)the eHealth Ontario Privacy Office

   Contact:
   eHealth Ontario Privacy Office
   P.O. Box 148, Toronto Ontario M5G 2C8
   T. 1-866-250-1554
   F: 1-866-831-0107 or 416- 586- 4397
   privacy@ehealthontario.on.ca

For Patients and Families:
- Patient Consent Directive Request Form

Privacy Toolkit:
- EHR Contact Matrix

4. **Service Ontario**
   The individual would like to place a consent directive for the Publicly Funded Drugs and Pharmacy Services and Monitored Drugs (DHDR) or the Ontario Laboratory Information System.
   1. Call: T. 1-800-291-1405 (TTY: 1-800-387-5559)

5. **ClinicalConnect**
   The individual would like to place a consent directive for the ClinicalConnect Clinical Viewer.
   1. Call: T. 905-870-8270 ext. 9

B. How Do I Respond to a Consent Directive Request?

1. Discuss with the individual:
   - ❑ Access concerns
     - Does the individual have a concern with their information being shared across the province?
     - Is there a concern with a particular health care provider or user that may have access to the individual's record? Is the concern with a particular data type (in which a block should only be requested for a specific repository).
   - ❑ What type of consent directive may be applied to address the concern (detailed on the next slide),
   - ❑ Advise of the implications of applying a consent directive as information will not be accessible unless a temporary override is performed,
   - ❑ Inform the individual of the instances in which the record may be temporarily accessed (overridden) and that they will be notified of this activity (refer to the eHealth Ontario Contact Matrix), and
   - ❑ Advise the individual they may always unblock or modify the type of block at any time.

2. Complete the HIC Consent Directive Request Form*:
   - ❑ Verify the identity of the individual or SDM following your existing practices,
   - ❑ Inform the individual to contact other organizations , if applicable depending on their concern- i.e. ServiceOntario INFOLine for OLIS and Publicly Funded Drugs and Pharmacy Services and Monitored Drugs (DHDR), ClinicalConnect Program Office for ClinicalConnect data
   - ❑ Confirm preferred method for confirmation and notification in the future- you may provide written or verbal communication.
   - ❑ Log receipt of the request in the Privacy Log, and
   - ❑ Submit request as directed on the form as soon as possible- this block must be applied within 7 calendar days .

3. Provide notice to Individual using the Notification of Consent Directive Template (if providing a verbal confirmation, refer to Appendix D).
   - ❑ Complete the template using the confirmation provided by EHR Program Office and
   - ❑ Log that the notice was provided in the Privacy Log or retain a copy.

Privacy Toolkit:
- HIC Consent Directive Request Form
- ClinicalConnect Consent Directive Form
- Notification of Consent Directive Template
- eHealth Ontario Contact Matrix
- Privacy Log

*Note: Privacy Officers in SWO must also complete the *ClinicalConnect Consent Directive Form*.

B. What Do I Do with Consent Directive Forms for MOHLTC Assets?

Consent directive forms from MOHLTC are not for the Privacy Officer to complete. Where a patient makes a request for consent directive in OLIS or DHDR to a Privacy Officer or equivalent, the patient must be directed to contact ServiceOntario.

1. OLIS

A **Laboratory Specimen Collection Centre** may receive the *MOHLTC Restricting Access to Information in the Ontario Laboratories Information System (OLIS) Withdrawal of Consent Form* from a patient **with** a laboratory requisition form.

Where the form indicates the patient wishes to "restrict access to ALL lab test information that has been entered into OLIS", the **lab** must fax or mail this form to eHealth Ontario. The lab must not apply this consent directive.

Where the form indicates the patient wishes to "restrict access to the SPECIFIC test identified", the lab may apply the consent directive directly. Test-level consent directives may not be applied retroactively and must be applied at the time the requisition is received.

2. DHDR

The *MOHLTC Blocking Access to Your Drug and Pharmacy Service Information Form* is provided from a patient to ServiceOntario.

B. What Type of Block(s) Can Be Applied to an Individual's Record?

The following are levels of detail at which a consent directive may be applied:

- In some instances, combinations can be used to meet a patient's request (i.e. block all users except for one family physician). For more information, refer to Appendix D.
- The consent directive will be applied to all historical and future data.
- A block is applied only to those systems requested.

Applicable Repositories	Action	Example	Policy Term
CDR, ClinicalConnect	Block all users from using or sharing personal health information	Jennifer does not want any personal health information shared in ConnectingOntario.	Global
ClinicalConnect, DHDR, DI CS, OLIS	All personal health information in a particular repository or system.	Jennifer wants to block all of lab results from being viewed.	Domain
CDR, DI CS	Block/allow all users from the organization(s) listed from using or sharing personal health information	Jennifer does not want anyone from Neverland Hospital in Toronto to view any of her records.	HIC-Agents
CDR, ClinicalConnect, DI CS	Block/allow all users from using or sharing personal health information from the organization(s) listed	Jennifer does not want any personal health information collected and used by Narnia Hospital to go outside of the site	HIC-Records
CDR	Block/allow particular user(s) from using or sharing personal health information	Jennifer does not want Dr. Pan to view any of her records	Agent
ClinicalConnect, DI CS	Block/ allow the use or sharing of a particular record of personal health information.	Jennifer does not want an ultrasound completed last Tuesday to be viewed.	Record

B. How Are Existing Consent Directives in My Organization Applied to the EHR?

Before your organization begins to contribute data to the CDR, patient-requested consent directives within your organization should be applied.

Your Privacy On-boarding Lead will provide you with the Consent Directive batch spreadsheet to enter your existing consent directives in the spreadsheet:

1. Ensure all PHI is captured on the spreadsheet – including MRNs, DOB, and HCN. Complete each patient's profile to ensure they can be accurately identified.

2. Translate the request you received from the patient to apply to the types of consent directives available in the CDR:
    - For agent level CDs, ensure that CPSO No., registered college No. or an HIS ID is included for each agent.
    - Indicate what type of CD to apply for each patient (Global, HIC Record, HIC Agent etc.)
        - Global consent directives in your HIS will translate to a HIC-Record block.
    - The following combinations may be applied: Global + HIC Agent, Global + Agent, Global + HIC Record, etc. For more information on how the system processes the consent directive levels, refer to Appendix D.
3. Review the log to ensure it is accurate and all information has been captured then submit to privacy.operations@ehealthontario.on.ca.

4. eHealth Ontario will apply the consent directives and provide you with a summary report to verify accuracy and approve.

If you have questions or require assistance with translating your organization's consent directives to the provincial consent directives, please speak to your Delivery Partner.

C. What is a Consent Directive Override?

A consent directive override is temporary access to personal health information that is blocked by a consent directive.

- An override can be applied to the record by selecting the "Override Consent" button to enable a clinical end user to view blocked personal health information in Ontario's electronic health record.
- There are 3 circumstances* in which information can be temporarily accessed by a user:
    1. Express consent by individual or substitute decision-maker
    2. Foreseeable risk of significant bodily harm to the individual and it is not reasonable to get consent in a timely manner
    3. Foreseeable risk of significant bodily harm to another individual or group

*The circumstances may vary depending on the type of information and the system functionality.

C. How is an Override with Express Consent Applied- ConnectingOntario ClinicalViewer?

In the ConnectingOntario Clinical Viewer, where the user receives **express consent** from an individual or SDM, the following steps must be followed:

1. Before a user performs an override on any portlet, the user must confirm if a block is placed on the Dispensed Medications tab by locating the Consent Override button.

2. User must inform the individual or substitute decision maker (SDM):
   - the reason for overriding consent and that personal health information can only be viewed for the reason the consent directive was overridden.
   - the override will apply to any other information or portlet where a block has been applied
   - Individual or SDM may refuse to permit the override
   - Information will be displayed according to the chart below

Data Source	Duration and Users Who May Access
CDR	Up to 11:59pm on the day that the override was initiated to the user that requested the override.
OLIS, DHDR	Available for 4 hours to all users at the organization or practice where the override occurred.

3. User clicks "Override Consent" to complete the consent override dialogue box,
   - If Dispensed Medications is blocked: user prints the hard-copy consent form and obtain signature from the individual or SDM; If Dispensed Medications is not blocked user obtains verbal or written consent. Written consent should be retained as part of the patient's chart.
   - User select the Circumstance fill out SDM information accordingly
   - Click Override Consent and View Patient Record

A disclaimer remains when the information is displayed.

These instructions are included in the Clinical End User Privacy and Security Training and the ConnectingOntario Clinical Viewer Privacy and Security Tip Sheet.

B. How is an Override for Significant Risk of Bodily Harm Applied?

In the ConnectingOntario Clinical Viewer, where the user performs an override for **significant risk of bodily harm**, the following steps must be followed:

1. User clicks "Override Consent" to complete the consent override dialogue box
2. Select radio button with Significant Risk of Bodily Harm
3. Click Override Consent and View Patient Record

A disclaimer remains when the information is displayed.

Note: An override for this reason will not display OLIS or DHDR results (therefore does not require the DHDR consent form to be completed).

C. How is an Override with Express Consent Applied- ClinicalConnect ClinicalViewer?

In the ClinicalConnect Clinical Viewer, where a physician receives express consent from an individual or SDM to access DHDR records, the following steps must be followed:

1. Click the Unblock Access button (only appears for physicians).
2. Print the Consent **Form** (Temporary Unblocking of Access) from the links provided in ClinicalConnect.
3. Complete the consent information. If selecting the Substitute Decision Maker (SDM), enter the name of the SDM and select the relationship to the patient.
4. Advise the patient or SDM that once the consent reinstatement is activated (**access is unblocked**), that all ClinicalConnect users from your organization (physician's organization/practice) may access the patient's information from DHDR for a period of four hours.
5. Obtain the consent of the patient or SDM by way of a wet signature.

Currently the MOHLTC does not permit a consent override without patient or SDM consent. A consent override for the purpose of eliminating or reducing a significant risk of serious bodily harm to the patient is not permitted.

Only physicians can currently override a consent directive in the ClinicalConnect system and only in certain source systems (see cSWO EHR Reference Guide for more information)- an override may not be performed for ConnectingOntario Clinical Data Repository, DI CS and OLIS.

C. What am I Required to do in the Event of an Override?

If an override occurs for **CDR, DI CS or DHDR** the following steps must be followed:

1. Receive an audit report via email from eHealth Ontario.
2. Investigate to confirm the override was appropriate. Until your investigation is complete, this should be treated as a potential privacy breach.
   - ❑ If the investigation is confirmed to be a privacy breach, follow the privacy breach process and report to eHealth Ontario as soon as possible, but no later than the end of the next business day of becoming aware.
   - ❑ If the override was performed for the purpose of eliminating or reducing a significant risk of serious bodily harm to a person other than the individual to whom the PHI relates or to a group of persons, you must inform the Information and Privacy Commissioner immediately after investigation by completing the Notification of Consent Override to IPC Template.
3. If the investigation confirmed the access was appropriate, provide notice to Individual using the Notification of Consent Override Template (if providing a verbal confirmation, refer to Appendix E):
   - ❑ Complete the template using the results of your investigation and
   - ❑ Log that the notice was provided in the Privacy Log or retain a copy.

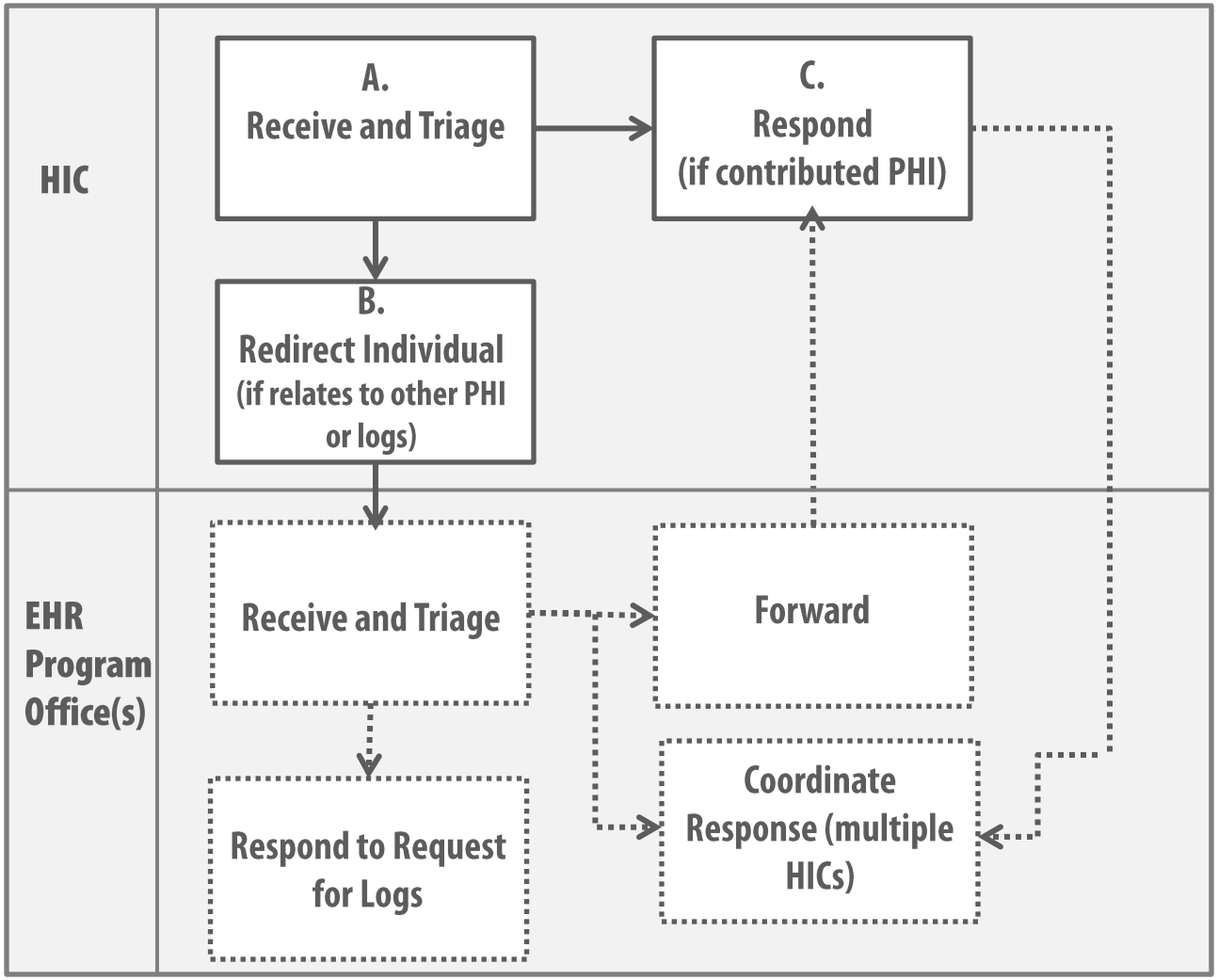
   Note: You do not need to perform this step for DHDR- MOHLTC will provide the individual with a letter.

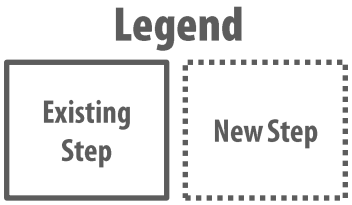
If an override occurs for **OLIS**, MOHLTC will provide the individual with a letter. This individual may contact you to investigate if they believe override was appropriate (express consent was not provided).

Privacy Toolkit:
- **Notification of Consent Directive Override Letter to Individual**
- **Notification of Consent Directive Override Letter to the IPC**
- **Consent Directives Log**

5. Access Requests

The following outlines the existing steps performed at your organization and new steps that will be carried out to support requests to access personal health information or reports of access to personal health information in respect of the EHR.





A. What Information May Be Requested?

An individual may request the following under an access request:

- Copies of the Individual's personal health information in Ontario's and/or regional EHR
- Report of who has viewed the Individual's personal health information
- Report of history of Consent Directives applied and removed
- Report of Consent Directive overrides

B. How Can an Individual Make an Access Request?

Where an Individual or substitute decision-maker makes a Request will vary on the scope of the request:

1. **Contact Privacy Officer (You)**
   The individual would like a copy of personal health information that only your organization contributed or for a report that you may generate with respect to Ontario's Electronic Health Record.

2. **eHealth Ontario Privacy Office**
   The individual would like a copy of personal health information contributed by another custodian or an audit report for ConnectingOntario or Diagnostic Imaging.
   1. Mail or Fax a completed copy of the Access and Correction Request Form
   2. Call (or provide an email with contact information)the eHealth Ontario Privacy Office

   Contact:
   eHealth Ontario Privacy Office
   P.O. Box 148, Toronto Ontario M5G 2C8
   1-866-250-1554, F: 1-866-831-0107 or 416- 586- 4397
   privacy@ehealthontario.on.ca

For Patients and Families:
- Access and Correction Request Form

Privacy Toolkit
- eHealth Ontario Contact Matrix

3. **MOHLTC**
   The individual would like a copy of personal health information or for a report of who has accessed their record in the Ontario Laboratory Information System.
   1. 1. 416-327-7040

4. **Service Ontario**
   The individual would like a copy of personal health information or for all reports for the Digital Health Drug Repository and for consent management-related reports for the Ontario Laboratory Information System.
   1. Call: T. 1-800-291-1405 (TTY: 1-800-387-5559)

5. **ClinicalConnect**
   The individual would like a copy of personal health information or for all reports for ClinicalConnect Clinical Viewer.
   1. Call: T. 905-870-8270 ext. 9
   2. Email (contact information only): privacy@clinicalconnect.ca

Note: a Clinician may allow a patient to view the screen at the time of receiving care if the clinician collected the PHI (formal request not required).

C. How Do I Respond to an Access Request?

From an Individual

Discuss with the individual what information the individual wishes to see .

- Does the individual want a copy of a certain type of data?
- What report is the individual looking for?
- Should this request be considered the first step in a potential breach investigation?

A. Where the request is for your organization only

- ❑ Follow your internal policies and procedures.

B. Where the request is for information from another or multiple organizations or a report you cannot generate

Within 4 calendar days of receiving the request

- ❑ Inform the individual to contact other organizations , if applicable depending on their concern- i.e. ServiceOntario INFOLine for OLIS Consent and Publicly Funded Drugs and Pharmacy Services and Monitored Drugs, MOHLTC for OLIS PHI and Access Reports, ClinicalConnect Program Office for ClinicalConnect data, eHealth Ontario for ConnectingOntario or Diagnostic Imaging.
- ❑ Log receipt of the request and that you redirected the individual.

Forwarded from EHR Program Office

A. Where the request is for your organization only

- ❑ Follow your internal policies and procedures
- ❑ Log that a response was made or keep a copy of the response

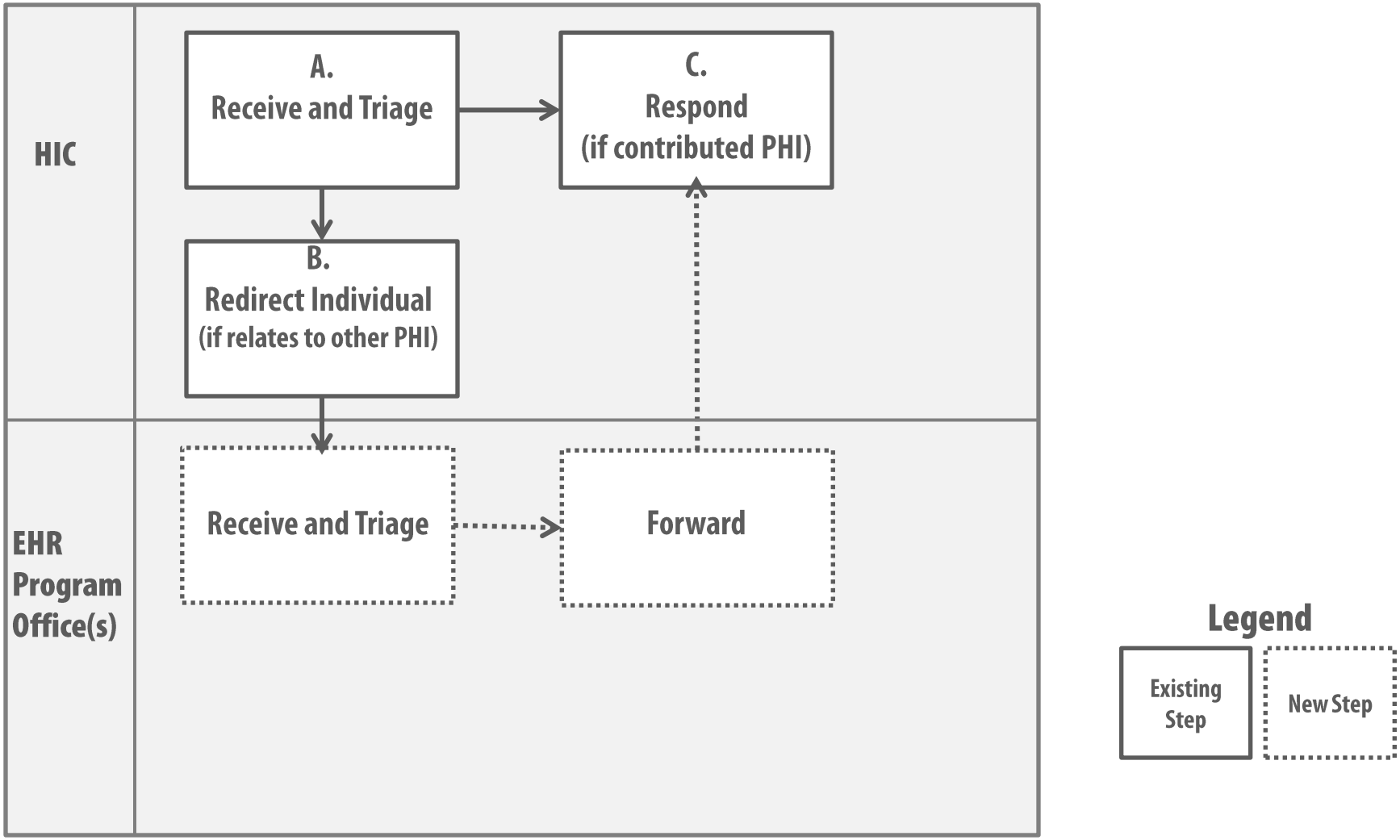
B. Where the request is for information from another or multiple organizations or a report you cannot generate

- Within 21 calendar days of receiving the request, advise the Program Office of
  - ❑ Fee estimate- you may charge a fee if your organization retrieves the responsive records – See Appendix E
  - ❑ Decision on whether to grant the request or apply exceptions
  - ❑ An extension request (if needed)
- Complete all template letters provided and securely return.
- EHR Program Office will provide a response to the individual- if you do not respond within 21 days, the EHR Program Office will inform the individual and advise the individual to contact your organization directly or make a complaint to the Information and Privacy Commissioner.

Privacy Toolkit:
- Access Request Log

5. Correction Requests

The following outlines the existing steps performed at your organization and new steps that will be carried out to support requests for correction to personal health information in the EHR.



A. How Are Correction Requests Handled?

- Your organization may grant or refuse a correction request in accordance with section 55) of PHIPA.
- Corrections in your local HIS are automatically uploaded into the provincial and regional EHR systems

B. How Can an Individual Make an Correction Request?

Where an Individual or substitute decision-maker makes a Request will vary on the scope of the request:

1. **Contact Privacy Officer (You)**
   The individual would like to correct personal health information that your organization contributed to Ontario's Electronic Health Record.

2. **eHealth Ontario Privacy Office**
   The individual would like to correct personal health information contributed by another custodian or multiple custodians to ConnectingOntario or Diagnostic Imaging.
   1. Mail or Fax a completed copy of the Access and Correction Request Form
   2. Call (or provide an email with contact information)the eHealth Ontario Privacy Office

   Contact:
   eHealth Ontario Privacy Office
   P.O. Box 148, Toronto Ontario M5G 2C8
   1-866-250-1554, F: 1-866-831-0107 or 416- 586- 4397
   privacy@ehealthontario.on.ca

For Patients and Families:
- Access and Correction Request Form

Privacy Toolkit
- eHealth Ontario Contact Matrix

3. **Health Information Custodian that Requested a Lab Result in OLIS**
   The individual would like to correct personal health information contributed in the Ontario Laboratory Information System.
   1. 1. 416-327-7040

4. **Service Ontario**
   The individual would like to correct personal health information contributed to the Digital Health Drug Repository.
   1. Call: T. 1-800-291-1405 (TTY: 1-800-387-5559)

5. **ClinicalConnect**
   The individual would like to correct personal health information contributed by another custodian or multiple custodians to the ClinicalConnect Clinical Viewer.
   1. Call: T. 905-870-8270 ext. 9
   2. Email (contact information only): privacy@clinicalconnect.ca

C. How Do I Respond to a Correction Request?

From an Individual

A. Where the request is for your organization only

- ❑ Follow your internal policies and procedures.
- ❑ Make the correction (or attach a notice of disagreement) in the source system
- ❑ Notify other organizations* that collected the personal health information (where the individual requests and if medically relevant).
- ❑ Log or keep a copy of the notice that the correction was made or notice of disagreement

B. Where the request is for a correction for another or multiple organizations

As soon as possible

- ❑ Inform the individual to contact other organizations , if applicable depending on their concern- i.e. ServiceOntario INFOLine for Publicly Funded Drugs and Pharmacy Services and Monitored Drugs, HIC that ordered the lab for OLIS, ClinicalConnect Program Office for ClinicalConnect data, eHealth Ontario for ConnectingOntario or Diagnostic Imaging.

Forwarded from EHR Program Office

- ❑ Follow your internal policies and procedures.
- ❑ Make the correction (or attach a notice of disagreement) in the source system
- ❑ Notify other organizations that collected the data (where the individual requests and if medically relevant).
- ❑ Log or keep a copy of the notice that the correction was made or notice of disagreement

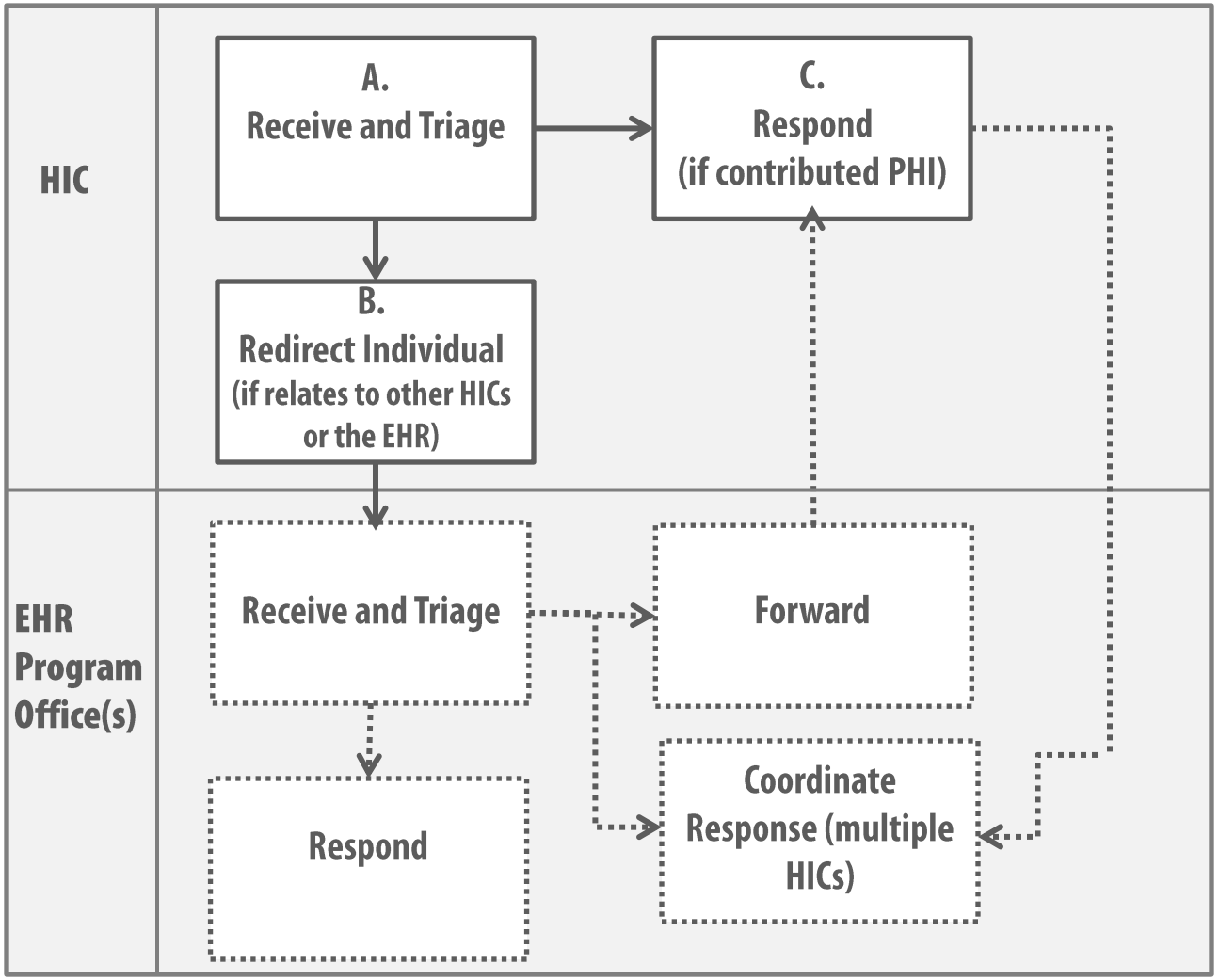
Privacy Toolkit:

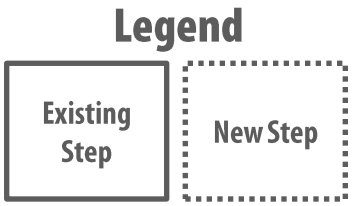
- Correction Request Log

*If you require assistance in identifying organizations that collected the personal health information, contact the EHR Program Office for assistance. You will be provided with the list and contact information for each applicable organization.

5. Inquiries

The following outlines the existing steps performed at your organization and new steps that will be carried out to support questions received in respect of the EHR.





A. What Is Classified as an Inquiry?

A privacy-related inquiry can be classified as a question raised in respect of:

- When, how and the purposes for which PHI in the EHR is collected, used or disclosed or viewed, handled or otherwise dealt with;
- The administrative, technical and physical safeguards and practices maintained in respect of PHI in the EHR;
- The policies, procedures and practices implemented in respect of the EHR; and
- Compliance with PHIPA, applicable agreements and the policies, procedures and practices implemented in respect of the EHR.

What is the EHR?	How is my information protected?	Who has access to the EHR and when can it be accessed?	What are my rights as a patient?

B. Who Can an Individual Contact for Questions?

Where an Individual or substitute decision-maker contacts to ask a question will vary on the scope of the request:

1. **Contact Privacy Officer (You)**
   The individual would like to know more information about your organization's privacy and information practices .

2. **eHealth Ontario Privacy Office**
   The individual would to know more about eHealth Ontario's privacy, information practices or has questions related to ConnectingOntario or Diagnostic Imaging.
   1. Mail or Fax a completed copy of the Inquiries and Complaints Request Form
   2. Call (or provide an email with contact information)the eHealth Ontario Privacy Office

   Contact:
   eHealth Ontario Privacy Office
   P.O. Box 148, Toronto Ontario M5G 2C8
   1-866-250-1554, F: 1-866-831-0107 or 416- 586- 4397
   privacy@ehealthontario.on.ca

For Patients and Families:
- Inquiries and Complaints Request Form

Privacy Toolkit
- eHealth Ontario Contact Matrix

3. **MOHLTC**
   The individual would like to know more about the Ontario Laboratory Information System.
   1. 1. 416-327-7040

4. **Service Ontario**
   The individual would like to know more about the Digital Health Drug Repository.
   1. Call: T. 1-800-291-1405 (TTY: 1-800-387-5559)

5. **ClinicalConnect**
   The individual would like to know more about the ClinicalConnect Clinical Viewer.
   1. Call: T. 905-870-8270 ext. 9
   2. Email (contact information only): privacy@clinicalconnect.ca

C. How Do I Respond to a Question?

From an Individual

Ask the individual what information they are looking for.

- Can this information be addressed via the Patient Notice or the Privacy Officer scripting?
- Is the question related to another request (i.e. Consent Directive or Access and Correction)?

A. Where the request is for your organization only

- ❑ Follow your internal policies and procedures.

B. Where the request is for information from another or multiple organizations or a report you cannot generate

Within 4 calendar days of receiving the request

- ❑ Inform the individual to contact other organizations , if applicable depending on their concern- i.e. ServiceOntario INFOLine for Publicly Funded Drugs and Pharmacy Services and Monitored Drugs, MOHLTC for OLIS, ClinicalConnect Program Office for ClinicalConnect data, eHealth Ontario for ConnectingOntario or Diagnostic Imaging.
- ❑ Log receipt of the request and that you redirected the individual.

Forwarded from EHR Program Office

A. Where the request is for your organization only

- ❑ Follow your internal policies and procedures
- ❑ Log that a response was made or keep a copy of the response

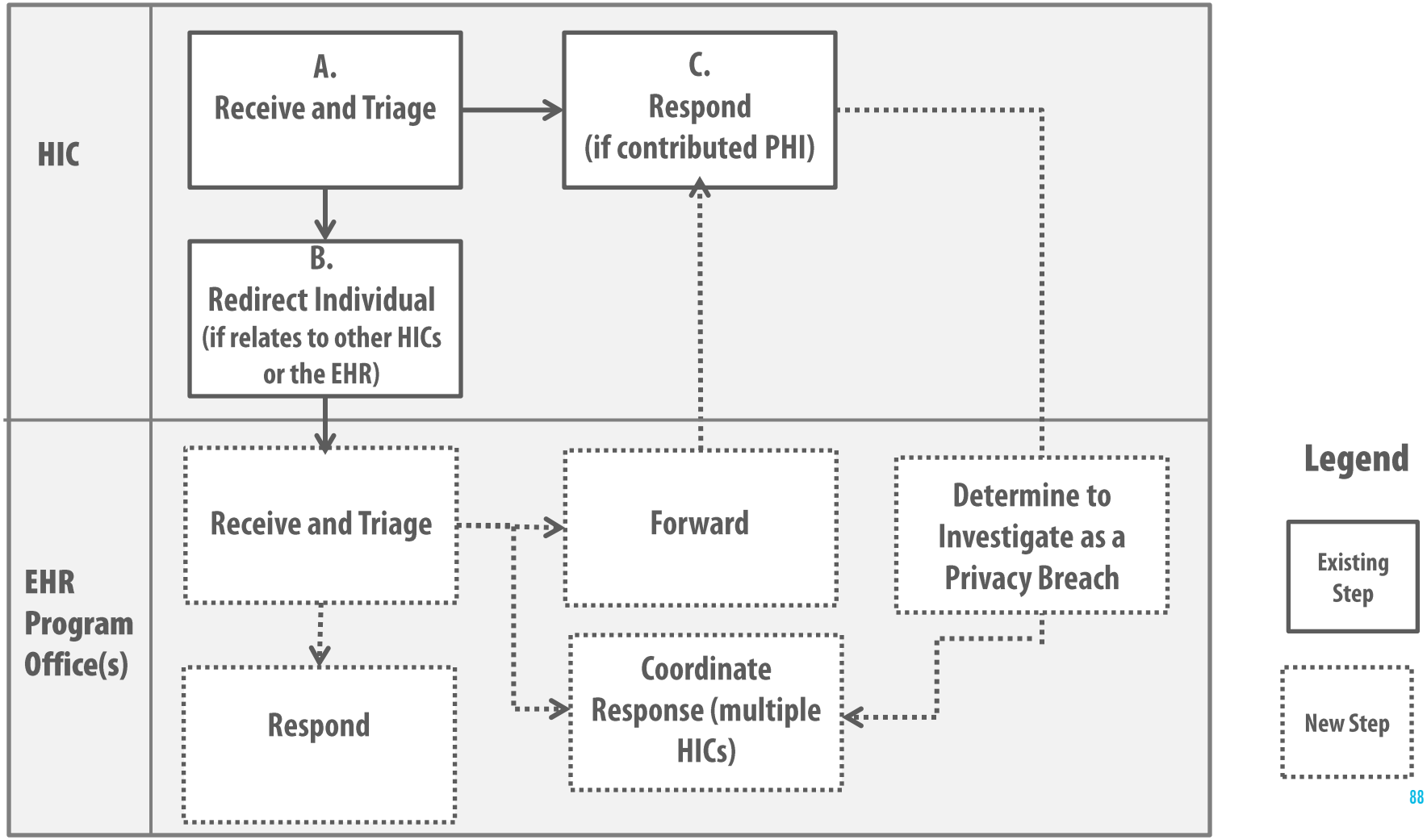
B. Where the request is for information from another or multiple organizations or a report you cannot generate

- ❑ Within 14 calendar days of receiving the request, provide the Program Office with information necessary for Program Office to draft a response.
- ❑ Within 4 days of receiving the draft response provide Program Office with comments.
- ■ Complete all template letters provided and securely return.
- ■ EHR Program Office will provide a response to the individual- if you do not respond within 14 days, the EHR Program Office will inform the individual and advise the individual to contact your organization directly or make a complaint to the Information and Privacy Commissioner.

Privacy Toolkit:
- Inquiries Log

5. Complaints

The following outlines the existing steps performed at your organization and new steps that will be carried out to respond to concerns received in respect of the EHR.



A. What Is Classified as a Complaint?

A privacy-related complaint can be classified as a concern raised in respect of compliance with PHIPA, applicable agreements and the policies, procedures and practices implemented in respect of the EHR.

- Someone has accessed my record inappropriately
- I was refused access to my personal health information
- I have not received a written consent directive confirmation
- I do not believe my personal health information is adequately protected

B. Who Can an Individual Contact for Complaints?

Where an Individual or substitute decision-maker contacts to ask a question will vary on the scope of the request:

1. **Contact Privacy Officer (You)**
   The individual would like to raise a concern about your organization's privacy and information practices .

2. **eHealth Ontario Privacy Office**
   The individual would to raise a concern about eHealth Ontario's privacy, information practices or has questions related to ConnectingOntario or Diagnostic Imaging.
   1. Mail or Fax a completed copy of the Inquiries and Complaints Request Form
   2. Call (or provide an email with contact information)the eHealth Ontario Privacy Office

   Contact:
   eHealth Ontario Privacy Office
   P.O. Box 148, Toronto Ontario M5G 2C8
   1-866-250-1554, F: 1-866-831-0107 or 416- 586- 4397
   privacy@ehealthontario.on.ca

For Patients and Families:
- Inquiries and Complaints Request Form

Privacy Toolkit
- eHealth Ontario Contact Matrix

3. **MOHLTC**
   The individual would like to raise a concern about the Ontario Laboratory Information System.
   1. 1. 416-327-7040

4. **Service Ontario**
   The individual would like to raise a concern about the Digital Health Drug Repository.
   1. Call: T. 1-800-291-1405 (TTY: 1-800-387-5559)

5. **ClinicalConnect**
   The individual would like to raise a concern about the ClinicalConnect Clinical Viewer.
   1. Call: T. 905-870-8270 ext. 9
   2. Email (contact information only): privacy@clinicalconnect.ca

C. How Do I Respond to a Complaint?

From an Individual

Ask the individual what information they are looking for.

- Can this information be addressed via the Patient Notice, Privacy Officer scripting or reference to the policy?
- Is the question related to another request (i.e. Consent Directive or Access and Correction)?
- Should you investigate this concern?

A. Where the request is for your organization only

- ❑ Follow your internal policies and procedures.

B. Where the request is for information from another or multiple organizations or a report you cannot generate

Within 4 calendar days of receiving the request

- ❑ Inform the individual to contact other organizations , if applicable depending on their concern- i.e. ServiceOntario INFOLine for Publicly Funded Drugs and Pharmacy Services and Monitored Drugs, MOHLTC for OLIS, ClinicalConnect Program Office for ClinicalConnect data, eHealth Ontario for ConnectingOntario or Diagnostic Imaging.
- ❑ Log receipt of the request and that you redirected the individual.

Forwarded from EHR Program Office

A. Where the request is for your organization only

- ❑ Follow your internal policies and procedures
- ❑ Log that a response was made or keep a copy of the response

B. Where the request is for information from another or multiple organizations or a report you cannot generate

- ❑ Within 14 calendar days of receiving the request, provide the Program Office with information necessary for Program Office to draft a response.
- ❑ The Program Office may decide to investigate as a privacy breach- be prepared to assist.
- ❑ Within 4 days of receiving the draft response provide Program Office with comments.
- ■ Complete all template letters provided and securely return.
- ■ EHR Program Office will provide a response to the individual- if you do not respond within 14 days, the EHR Program Office will inform the individual and advise the individual to contact your organization directly or make a complaint to the Information and Privacy Commissioner.

Privacy Toolkit:
- Complaints Log

5. Acceptable Use Practices for Privacy Officers

Privacy Officers or delegates come in to contact with personal health information and must adhere to the acceptable use practices and safeguards in place

Limit Access to Personal Health Information

- Adhere to the principles of need-to-know and least-privilege for the personal health information you come into contact with
- Keep personal health information and patient's concerns and breach investigation information confidential- do not discuss this information in public places where others may hear or see.

Protect Personal Health Information

- Do not take pictures or screenshots of information displayed.
- When sharing personal health information via email ensure it is encrypted, verify the recipient of the message and transmit securely.

Use a Strong Password

- Create a strong and hard-to-guess password by following conventional guidelines and keep your password a secret.
  - Always change an initial or temporary password provided to you on first use.

Retain Personal Health Information Securely

- Securely store personal health information and follow the EHR Security Policies for the appropriate disposal methods of personal health information

Use Approved Devices

- Only use approved and encrypted devices to store personal health information

eHealth Ontario
It's working for you.

NEXT STEPS & RESOURCES

Ontario
eHealth Ontario

Next Steps

1. Complete the Privacy Readiness Assessment and Security Readiness Assessment. If you haven't already attended the Security Policy and Assessment Webinar, make arrangements through your SDP to attend that session so that you can complete the Security Readiness Assessment
2. Submit the Privacy Readiness Assessment to your Service Delivery Partner and the Security Readiness Assessment to eHealth Ontario
3. Identify gaps and develop remediation plan
   - **Privacy Requirements:** gaps in the requirements in the EHR Privacy Policies must be mitigated prior to contribution/collection
   - **Security Requirements:** exceptions to gaps may be permitted; consult with Ontario's Electronic Health Record Security to complete an Exception Request Form for any deviations from a mandatory requirement in an EHR Security Policy
4. Utilize the tools provided by eHealth Ontario to develop your Privacy and Security Program

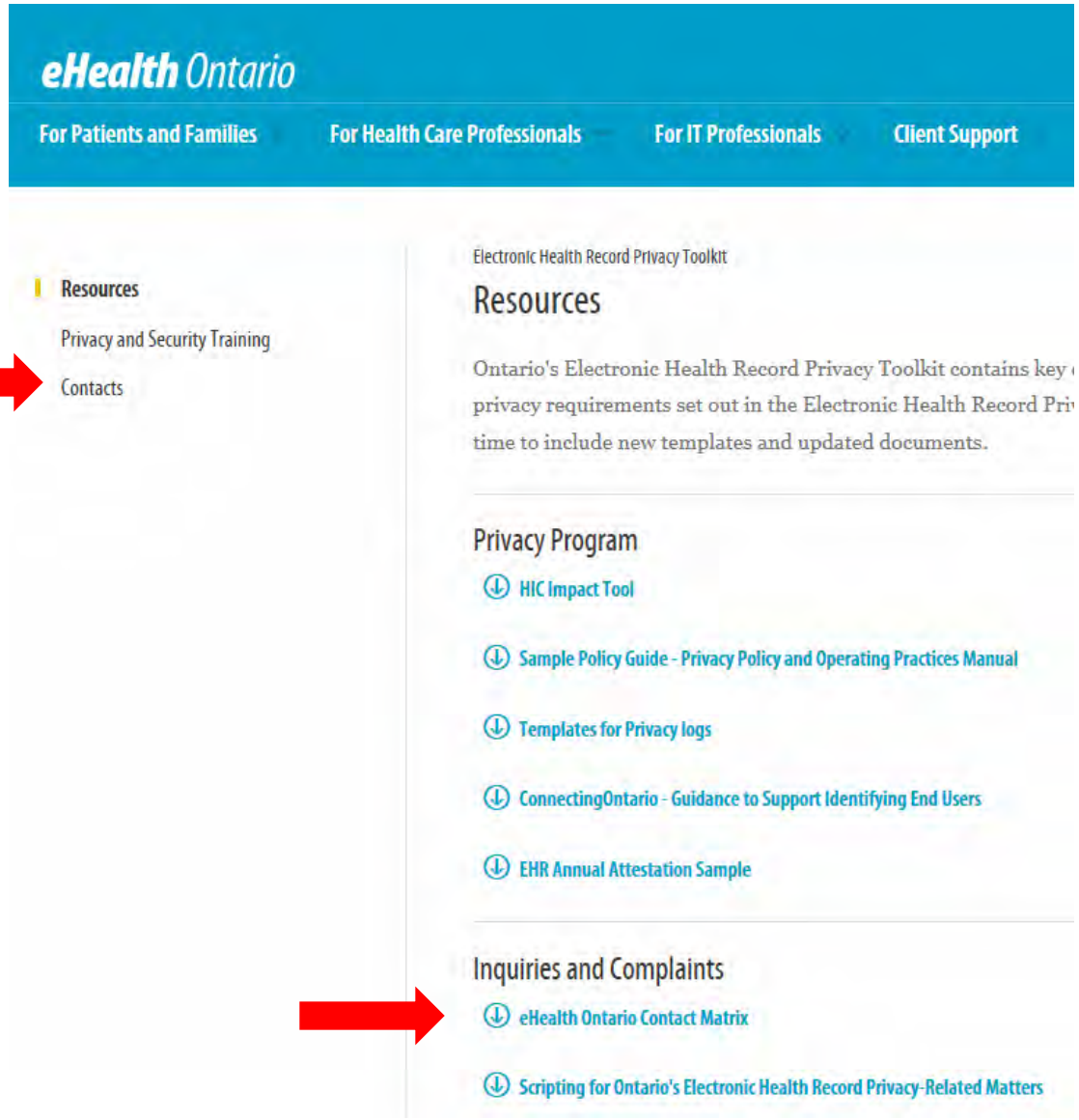
Security Contact Information

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's Service Desk	1-866-250-1554 servicedesk@ehealthontario.on.ca	Anyone to report Security Incidents related to ConnectingOntario, OLIS or DI CS.
ConnectingOntario Help Desk	1-888-802-1967 support@connectinggta.ca	First level support for ConnectingOntario technical issues.

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

Privacy Contact Information

Refer to the **eHealth Ontario Contact Matrix** or the **EHR Privacy Toolkit Page** on the eHealth Ontario Website: www.ehealthontario.on.ca



eHealth Ontario
It's working for you.

APPENDIX

Appendix A: Electronic Health Record Policies

The following are the **Electronic Health Record Privacy and Security Policies**:

EHR Security Policies/ 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. eHealth Ontario Federation Identity Provider Standard

Privacy Policies (5)

- Access and Correction
- Consent Management
- Inquiries and Complaints Policy
- Logging and Auditing
- Privacy Breach Management

Privacy and Security Policies (3)

- Assurance
- Privacy and Security Training
- Retention

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

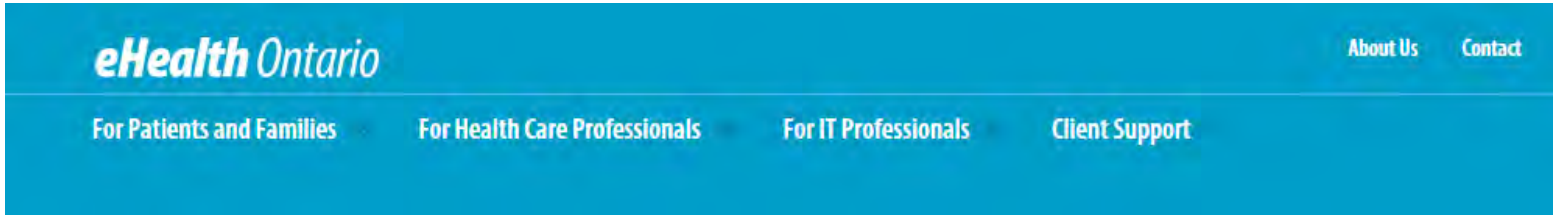
Appendix A: EHR Security Policy/Standards & Applicable Roles

#	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]

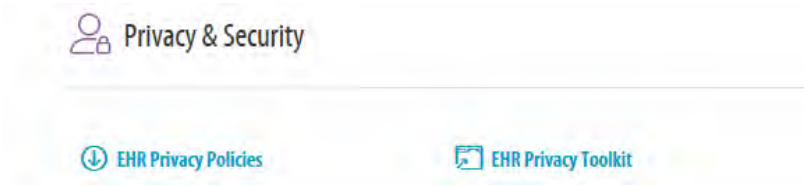
Appendix A: Locating the EHR Privacy Toolkit

1. Go to ehealthontario.on.ca

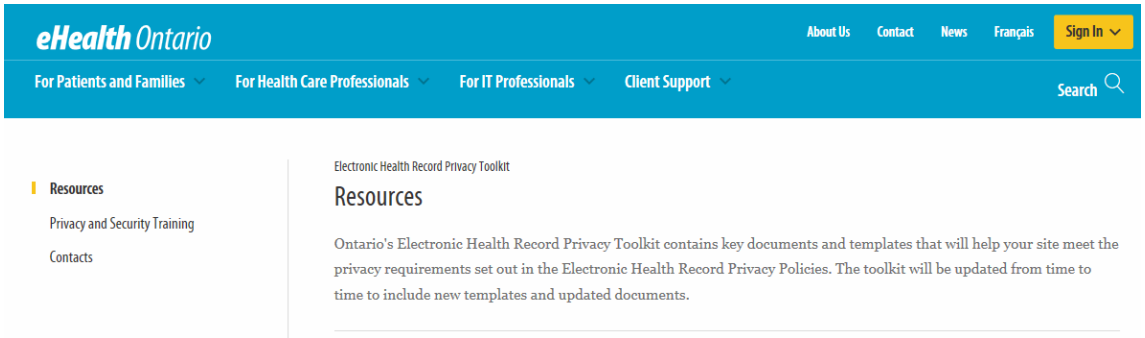


2. Click on "Client Support" and Select the relevant initiative

3. Scroll to Privacy & Security



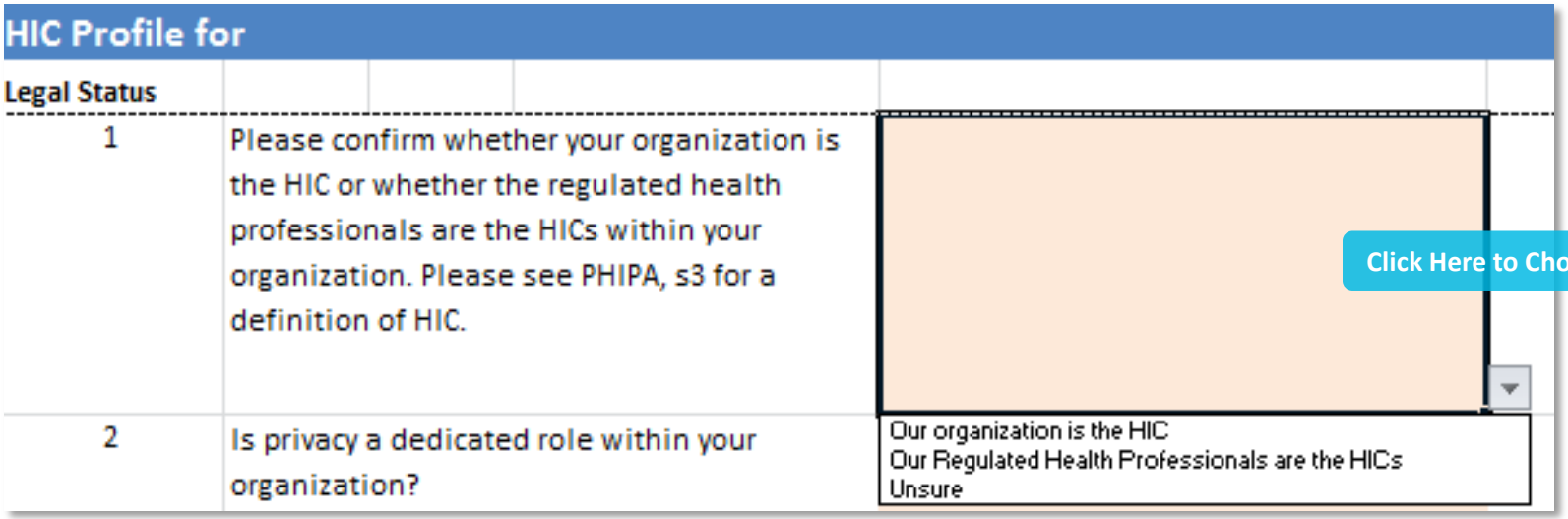
4. Click EHR Privacy Toolkit



Appendix B: EHR Privacy Readiness Assessment Instructions

Responding to Questions

Most questions have **drop down answer bars** as identified below:

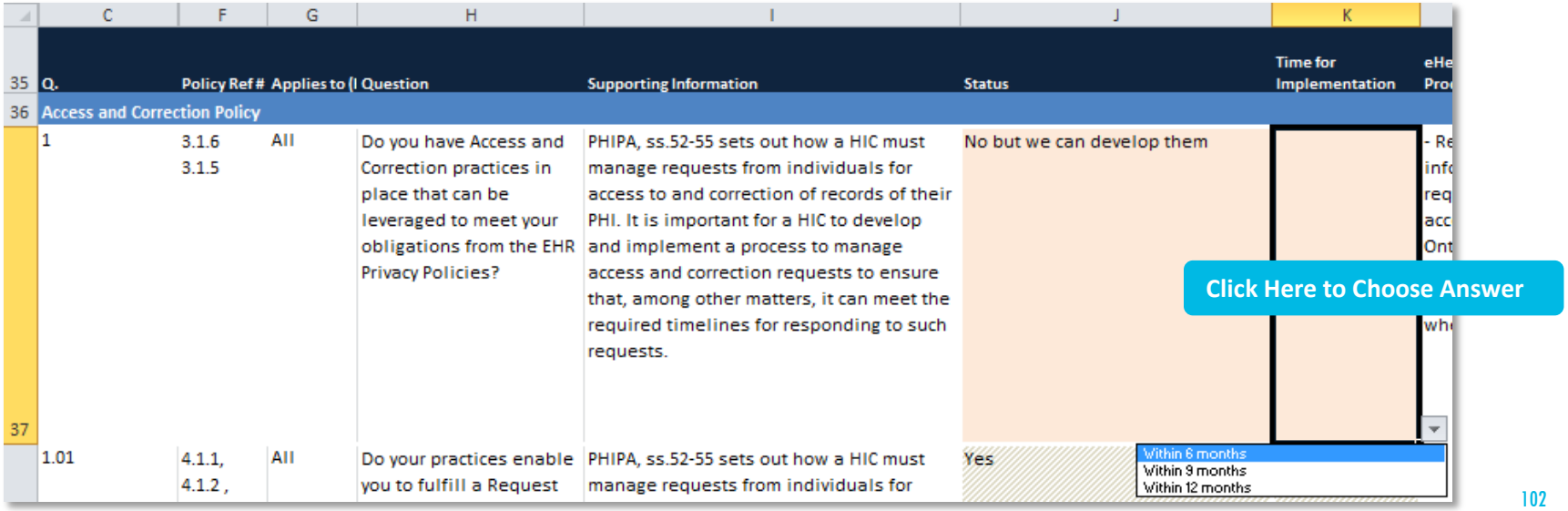


Appendix B: EHR Privacy Readiness Assessment Instructions

Responding to Questions

Completing the timeline drop down bar:

- If your status response indicates that you have practices in place, there is no need to complete the timeline or other supports required from eHealth Ontario fields.
- If your status response indicates that you do not have practices in place, you will need to complete the timeline and other supports required from eHealth Ontario fields.



Appendix B: EHR Privacy Readiness Assessment Instructions

Responding to Questions

You only need to complete the questions highlighted in **light orange** colour.

- This being said, it is highly recommended to complete the entire assessment so that you are prepared for discussions with eHealth Ontario regarding your choice of answers.

Q.	Policy Ref #	Applies to	Question	Supporting Information	Status	Time for Implementation	eHealth Ontario Technical or Process Supports	What other supports could eHealth Ontario provide to help you meet this
Access and Correction Policy								
1	3.1.6	All	Do you have Access and Correction practices in place that can be leveraged to meet your obligations from the EHR Privacy Policies?	PHIPA, ss.52-55 sets out how a HIC must manage requests from individuals for access to and correction of records of their PHI. It is important for a HIC to develop and implement a process to manage access and correction requests to ensure that, among other matters, it can meet the required timelines for responding to such requests. HICs that contribute PHI need to respond to both Requests for Access and Correction, and their existing process will need to accommodate addressing these. HICs that are view-only still must be able to respond to Requests for Access involving audit reports, and therefore must also ensure that their existing practice is able to accommodate addressing requests related to the EHR.	No but we can develop them		- Reporting Tool in EHR (provides information required to fulfill requests). If the HIC does not have access to the reporting tool, eHealth Ontario will provide the HIC with the reports. - eHealth Ontario coordinates where multiple HICs are involved	
1.01	4.1.1, 4.1.2, 4.1.8, 4.1.14, 4.1.17	All	Do your practices enable you to fulfill a Request for Access related to the PHI your organization contributes to or collects from the EHR?	PHIPA, ss.52-55 sets out how a HIC must manage requests from individuals for access to and correction of records of their PHI. It is important for a HIC to develop and implement a process to manage Requests for Access to ensure that, among other matters, it can meet the required timelines for responding to such requests.			- Reporting Tool in EHR (provides information required to fulfill requests). If the HIC does not have access to the reporting tool, eHealth Ontario will provide the HIC with the reports.	

A "No" response at the beginning of this section...

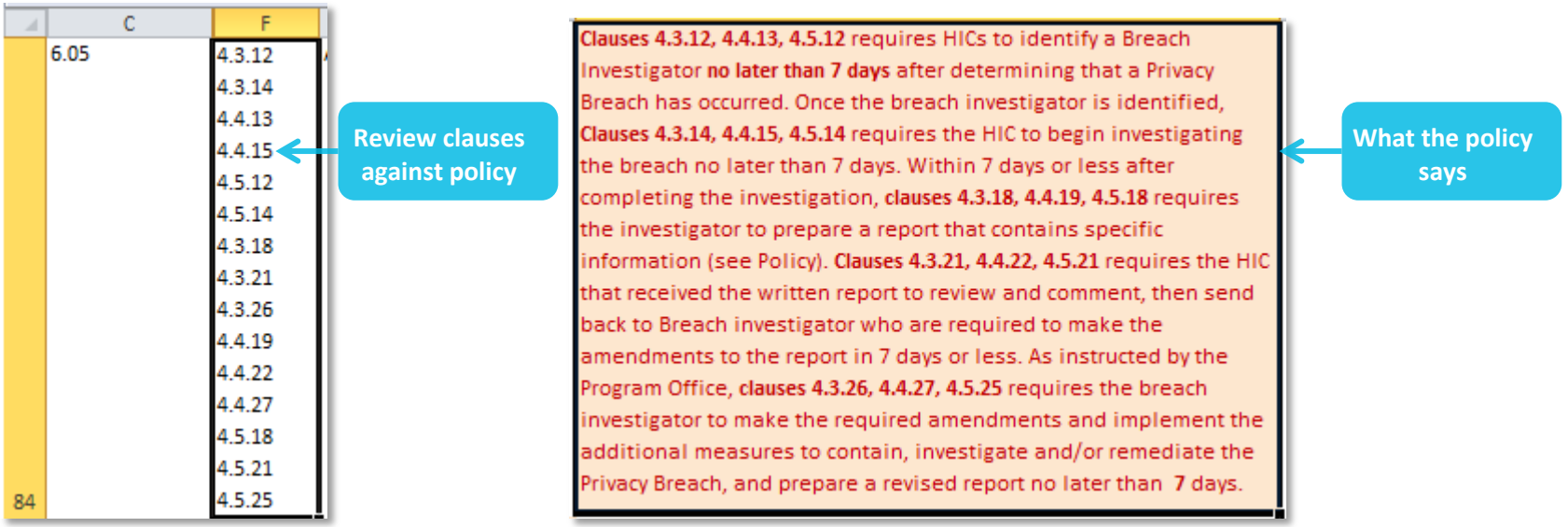
Results in the rest of the questions being grayed out.

Appendix B: EHR Privacy Readiness Assessment Instructions

Responding to Questions

It is **highly recommended** that you reference the associated clause(s) in the tool to the appropriate Electronic Health Record Privacy Policy.

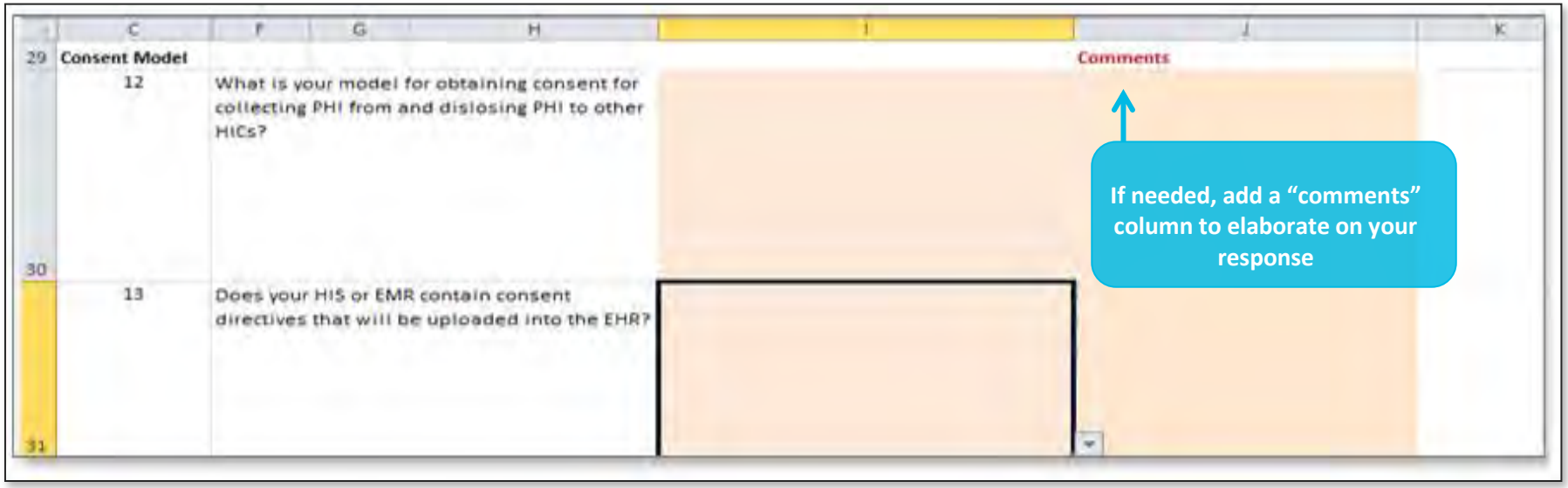
- **(e.g.)** Question 6.05 (row 84) of the Assessment lists a number of considerations to ensure compliance (see below). You must review the associated clauses against the appropriate policy. In this case, that would be the *Privacy Breach Management Policy.*



Appendix B: EHR Privacy Readiness Assessment Instructions

Responding to Questions

As long as existing rows and columns remain intact, additional columns and rows can be inserted at the side or bottom of the file.



Appendix B: EHR Privacy Readiness Assessment Instructions

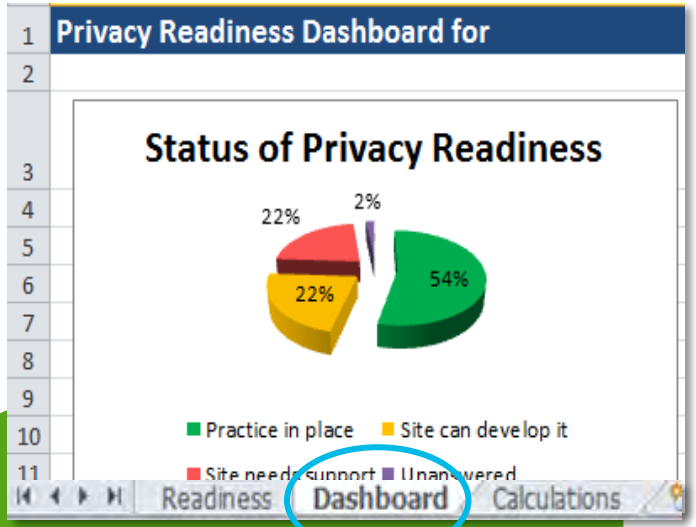
Finalizing the Assessment

1	**Current Status**		
2			Practice in place
3	Access	Access / Correction	
4	Obtaining	Consent Mgmt	
5	ConsentD	Consent Directive Mgmt	
6	Logging	Logging and Auditing	
7	Inquiries	Inquiries / Complaints	
8	Breach	Privacy Breach	
9	Training	Privacy Training	
10	Assurance	Assurance	
11			
12	Total		
13			
14			
15			
16			

Readiness | Dashboard | Calculations

1. Ensure the calculations and dashboard spreadsheets **reflect your actual responses** in the readiness spreadsheet.

If a number does not match, **simply override** the incorrect number in the appropriate row and column within the "calculations" spreadsheet. Doing so will automatically update the "dashboard" spreadsheet as well.



2. Review the "readiness" spreadsheet and **add up** the number of practices in place / site can develop / and site needs support. Then cross-reference it to the "calculations" spreadsheet.

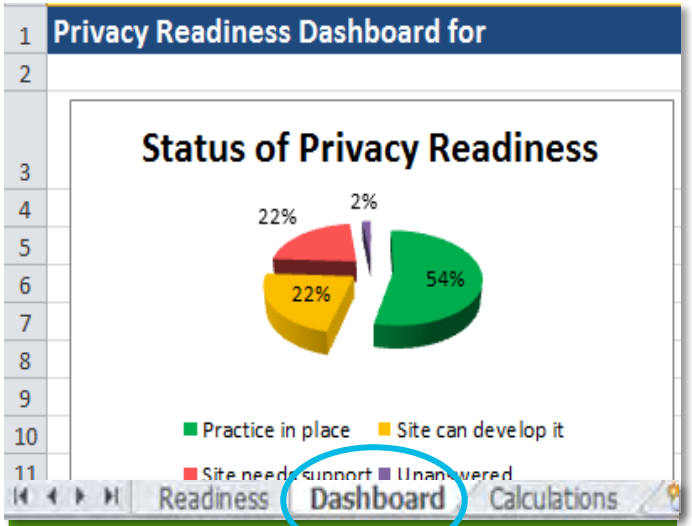
Appendix B: EHR Privacy Readiness Assessment Instructions

Finalizing the Assessment

1. Ensure the calculations and dashboard spreadsheets **reflect your actual responses** in the readiness spreadsheet.

1	**Current Status**		
2			Practice in place
3	Access	Access / Correction	
4	Obtaining	Consent Mgmt	
5	ConsentD	Consent Directive Mgmt	
6	Logging	Logging and Auditing	
7	Inquiries	Inquiries / Complaints	
8	Breach	Privacy Breach	
9	Training	Privacy Training	
10	Assurance	Assurance	
11			
12	Total		
13			
14			
15			
16			

Readiness | Dashboard | **Calculations**



2. Review the "readiness" spreadsheet and **add up** the number of practices in place / site can develop / and site needs support. Then cross-reference it to the "calculations" spreadsheet.

If a number does not match, **override** the incorrect number in the appropriate row and column within the "calculations" spreadsheet. Doing so will automatically update the "dashboard" spreadsheet as well.

Appendix B: EHR Privacy Readiness Assessment Instructions

Submitting the Privacy Assessment

Submit your completed Privacy Readiness Assessment to:

SWO

cSWO Program Office (cSWO Program Office will notify your Change Management & Adoption Delivery Partner Lead of your submission):
cswoprivacysecurity@lhsc.on.ca

GTA

GTA Privacy Service Delivery Partner:

NER

Privacy Readiness Assessment Delivery Partner Lead:

Appendix C: Retention Requirements

Retention

Health information custodians are required to securely retain the following information related to Ontario's Electronic Health Record:

Information Type		Retention Period
Reports that contain PHI	• Auditing and Monitoring Reports	30 years or when PHI is removed from the system (longest of)
Privacy Operations	• Log of all requests, including request forms, notices, and responses in respect of Requests for Access or Correction, Consent Directives, Inquiries or Complaints under PHIPA (where the HIC is accountable for producing the record)	2 years after the request has been closed • Complaint: 2 years after closed by the HIC, eHealth Ontario or IPC (longest of)
Privacy Breach/Security Incident	• Log s of Privacy Breach/ Security Incident • Privacy breach Management Remediation Report and status of the remediation report • Information created about an individual as part of a Privacy Breach/ Security Incident investigation	2 years after the investigation has been closed by the HIC, eHealth Ontario or IPC (longest of)
Registration Information	• Information used for IDP registration that contains PHI	7 years after last use
System-level logs	• Log of all access by the HIC and their agents and ESPs to Ontario's Electronic Health Record • Log all information system events on their identity provider services and data contribution endpoints • Log of all activities of administrators and operators on their identity provider services and their data contribution endpoints • List of all agents or ESPs who have authorized access to IDP technology and data contribution endpoints logs • Logs of any instance in which keys, key components or related materials for ISP services and data contribution endpoints are generated, removed from storage or loaded to a cryptographic device • Logs of all requests for user IDs that they administer and will have access to the IDP services and data contribution end point infrastructure connected to Ontario's Electronic Health Record	A minimum of 2 years
Assurance-related documents	• Privacy and Security Readiness Self- Assessment and associated decisions and directions • Privacy and Security Operational Self- Attestation and associated decisions and directions • Remediation Attestation • Non-compliance Reports and associated recommendations • Compliance Monitoring Reports • Audit Reports and associated recommendations, decisions and directions • Business continuity plan	10 years

Appendix D: Consent Granularity Enforcement Rules

The following are examples of multiple consent directive levels applied to meet a patient's request:

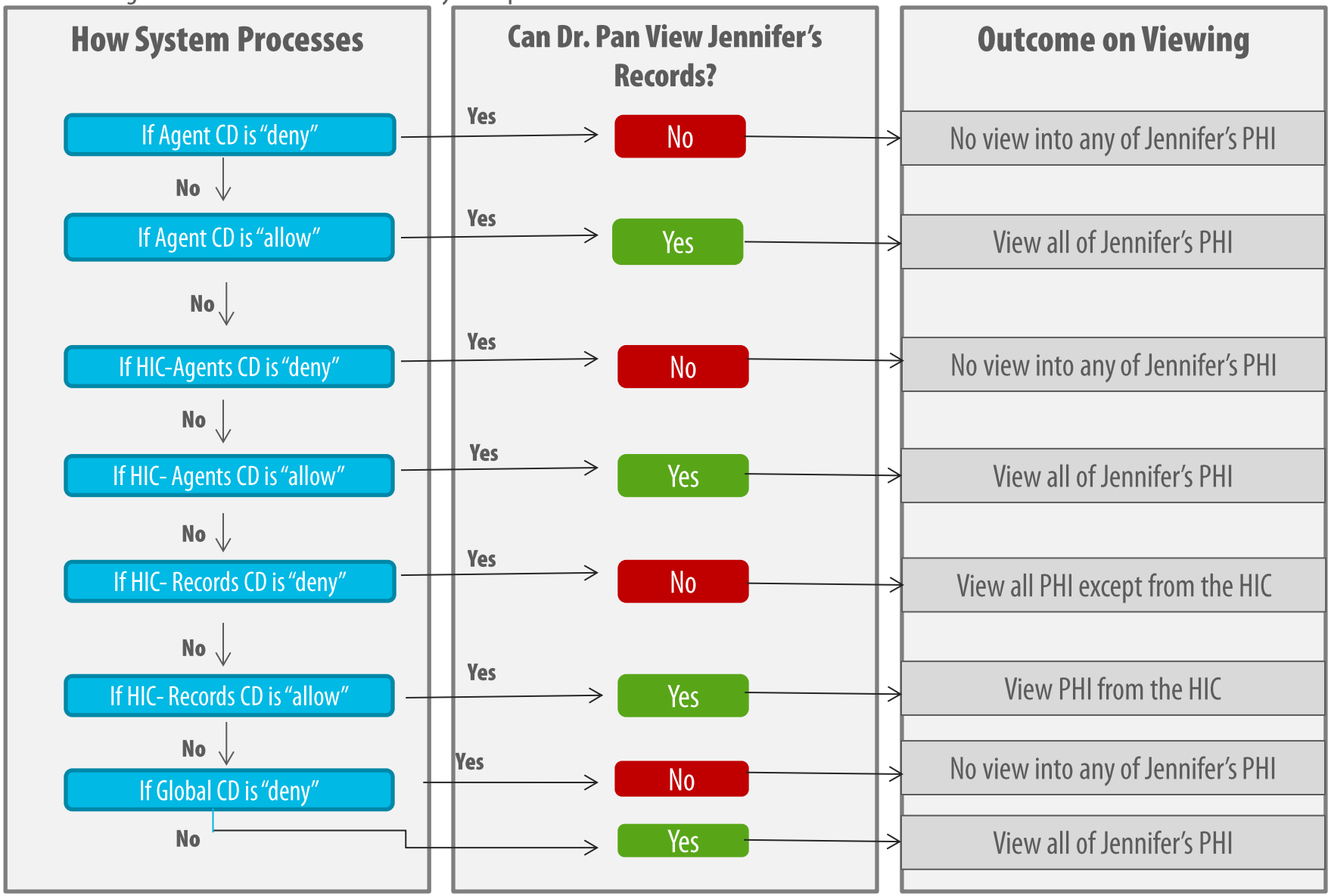
Jennifer does not want anyone except the users of Narnia Hospital to view her records in ConnectingOntario:
Global Consent Directive to block all users and create an exception with a HIC-Agent Consent Directive to allow Narnia Hospital.

Jennifer does not want anyone except Dr. Pan to view her records in ConnectingOntario:
Global Consent Directive to block all users and create an exception with an Agent Consent Directive to allow Dr. Pan in ConnectingOntario.

Refer to the next slide for more information on the system logic for reading a consent directive.

Appendix D: Consent Granularity Enforcement Rules

The diagram below describes how the system processes the consent level enforcement rules in the EHR.



Appendix D: Confirmation of a Consent Directive Notification

(EHR Consent Management Policy, version 1.3, section 4.4.1)

The following must be communicated when providing a verbal confirmation that a consent directive request has been implemented:

1. Describe to Individual:
   - ❑ The request received
   - ❑ The request applied/removed and confirm the date applied/removed
   - ❑ The impact of the consent directive applied/removed- information will not be accessible unless a temporary override is performed
   - ❑ Where a consent directive was applied, describe the circumstances under which it may be temporarily accessed (i.e., consent, significant risk of bodily harm to self or others) and be temporarily accessed that they will be notified of this activity,
2. Advise the individual they may always unblock or modify the type of block at any time.
3. Provide contact information for the person to whom individuals may direct inquiries or complaints related to the consent directive.
4. Ensure you document that the confirmation was provided in the Privacy Log.

Appendix D: Consent Directive Override Notification

(EHR Consent Management Policy, version 1.3, section 4.6.9)

The following must be communicated when providing a verbal confirmation that a consent directive override investigation is completed and confirmed it was appropriate:

1. Describe to Individual:
   - ❑ Name of the clinician and health information custodian who overrode the Consent Directive
   - ❑ Date and time of the override
   - ❑ Type of PHI collected and the name of the health information custodian that contributed the PHI
   - ❑ Reason for the override (i.e., reason that the clinician chose in the viewer)
2. Provide contact information for the person to whom individuals may direct inquiries or complaints related to the consent directive.
3. Ensure you document that the notification was provided in the Privacy Log.

Appendix E: Charging Fees for an Access Request

You may charge fees to fulfill access requests associated with EHR systems where your organization is required to provide a copy of the record

- Fees must:
  - Be communicated to the Individual prior to charging them
  - Not exceed the amount of reasonable cost recovery
  - Be consistent with applicable orders of the Information and Privacy Commissioner of Ontario (Refer to Order HO-009)

- If eHealth Ontario or ClinicalConnect coordinates the response
  - Communicate the fee estimate to Program Office
  - Program Office will collect the fee from the Individual and forward it to your organization

- Individuals with concerns about the fee estimate will be asked to contact the health information custodian(s) charging the fee directly