Privacy and Security Training for Local Registration Authorities and Sponsors Ontario's Electronic Health Record

Version 1.0

Welcome to the Privacy and Security Training for Local Registration Authority and Sponsor

Hi my Name is Anne. What is yours?

Please enter the following information in the fields below:

- Enter your first and last name
- Enter your Job Title and Organization
- Enter your email address

Error Page

Sorry, you may not continue until you have entered the required information for your certificate.

Getting Started

Before you Begin

- This course consists of 1 module with 20 slides and 5 quiz questions and will take a minimum of 15 minutes to complete.
- You must achieve 100% on the quiz. A completion certificate will be available to print for your records.
- Provide a copy to the person responsible for tracking training at your organization or practice.

Click here to review the instructions on how to navigate this module: (Table with instructions).

Buttons	**Navigation**
Top Right Menu Bar	
Slide Progress Bar	
Play	play audio
Pause	pause audio
Previous	navigate to the previous slide
Next	navigate to the next slide
Submit	submit quiz
Review Quiz	review test feedback
Volume	controls the audio volume for each slide. Test it now!
Exit	close the course

Icon	**Supplementary Information**
Interactions	opens a link
Example	navigates to examples illustrating the content
Case Study	navigates to a real experience illustrating the content
Learn More	displays additional information on the content

Course Objective

By the end of this training, you will understand your privacy and security obligations as a Local Registration Agent or Sponsor of Ontario's Electronic Health Record by learning:

1. What is Ontario's Electronic Health Record?
2. Why do I need to Complete This Training?
3. As a Local Registration Agent or Sponsor of Ontario's Electronic Health Record, what is expected of me?

What is Ontario's Electronic Health Record?

It enables authorized health care providers to centrally access personal health information. It includes:

- **ConnectingOntario**: clinical reports
- **Diagnostic Imaging Common Services (DI CS) Repository**: diagnostic imaging reports
- **Ontario Laboratory Information System (OLIS)**: laboratory test orders and results
- **Digital Health Drug Repository (DHDR):** dispensed drug history

- 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 Clinical Viewer.

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

Learn More: What is personal health information?

Personal Health Information (PHI) is defined in section 4 of the *Personal Health Information Protection Act, 2004* (PHIPA).

Means identifying information about an individual in oral or recorded form, if the information,

- (a) relates to the physical or mental health of the individual, including information that consists of the health history of the individual's family,
- (b) relates to the providing of health care to the individual, including the identification of a person as a provider of health care to the individual,
- (c) is a plan of service within the meaning of the *Home Care and Community Services Act, 1994* for the individual,
- (d) relates to payments or eligibility for health care, or eligibility for coverage for health care, in respect of the individual,
- (e) relates to the donation by the individual of any body part or bodily substance of the individual or is derived from the testing or examination of any such body part or bodily substance,
- (f) is the individual's health number, or
- (g) identifies an individual's substitute decision-maker.

Examples

Examples of personal health information:

- Provider name;
- Individual's address and telephone number;
- Electronic medical charts;
- Discharge summaries;
- Lab specimens;
- X-ray results;
- Drug information; and
- Health card number and medical record number.

Why do I need to complete this training?

Why do I need to complete this training?

- You are authorized by your organization's Legally Responsible Person to manage the enrollment process of health care providers.
  - Your organization or practice is a Health Information Custodian and a participant in Ontario's Electronic Health Record and has legal obligations to other health information custodians and individuals that they are required to meet.
    - Your organization or practice is a Federated Identity Provider Site; or a ONE ID Site leveraging eHealth Ontario's ONE ID Service.
- You have access to personal information to approve and/or register and enroll users (agents and Electronic Service Providers) to Ontario's Electronic Health Record.
  - You need to understand what activities are acceptable when registering users of Ontario's Electronic Health Record and what constitutes a privacy breach or security incident.

What are my obligations in Ontario's Electronic Health Record?

- You must understand the privacy and security activities you may be required to perform in your role in Ontario's Electronic Health Record.

Where are these obligations from?

- *Electronic Health Record Information Security Policies*
- *Electronic Health Record Local Registration Authority Practices*
- *eHealth Ontario Federation Identity Provider Standard*

What if I do not comply with my obligations?

- You may be subject to consequences established by law, your organization or your practice and/or Electronic Health Record oversight body.

Potential consequences of non-compliance

- Re-training on privacy and security requirements.
- Loss of access to one or more systems.
- Being reported to your professional college, loss of professional standing, college sanctions.
- Termination or loss of privileges at your organization or practice.
- Orders of the Information and Privacy Commissioner of Ontario.
- Legal action or regulatory fines against your organization or practice or you personally (up to $100,000).
- Significant financial losses for your organization or practice to correct the situation.

Learn More: Personal Health Information Protection Act, 2004

What is the Personal Health Information Protection Act, 2004?

- Is the law for protecting the privacy of an individual and the confidentiality of an individual's personal health information.
- Sets rules for the collection, use and disclosure of personal health information and provides individuals with the right to access and to request a correction of their personal health information.

In this training, "view, handle or otherwise deal with" will be referenced to activities you perform such as viewing personal health information.

How does Personal Health Information Protection Act, 2004 apply to me?

When providing health care, each person and organization or practice has a role :

- The organization or practice in which you work is either
  - A Health Information Custodian (HIC) and a participant in Ontario's Electronic Health Record as such is accountable for the personal health information in Ontario's Electronic Health Record that it creates and contributes or collects, uses and discloses;
  - A Health Information Network Provider (HINP) , that enables the electronic sharing of personal health information between two health information custodians and is accountable for personal health information or that it views, handles or otherwise deals with; or
  - An Electronic Service Provider (ESP), that provided services to support the electronic sharing of personal health information and is accountable for personal health information or that it views, handles or otherwise deals with.
- You are an Agent of a Health Information Custodian, Health Information Network Provider or Electronic Service Provider when providing technical or operational support
  - You are accountable to your organization or practice for your actions.

Examples

Examples of activities logged and audited:

- Login/logout
- Viewing personal health information
- Consent directive overrides
- System activity (starting-stopping services)

As a Local Registration Authority or Sponsor of Ontario's Electronic Health Record, what is expected of me?

- Understand the expectations for your organization or practice
- Know how to register users of Ontario's Electronic Health Record
- Know the entitlement criteria for the provider portal and administration portal
- Know how to revoke or suspend user access
- Maintain a record of enrolled users
- Report privacy breaches and security incidents
- Adhere to privacy and security do's and don'ts
- Be aware of the privacy and security safeguards

To fulfil your expectations within Ontario's Electronic Health Record, identify the Privacy Officer for your organization or practice. If you are unaware of or do not have a Privacy Officer, refer to eHealth Ontario.

Understand the expectations for your organization or practice

What does my organization or practice do to ensure I meet my privacy and security obligations?

1. Your organization or practice establishes controls to manage all access to Ontario's Electronic Health Record.
    - These controls ensure that only authorized persons are granted access and that personal accountability is assured.
2. Your organization or practice establishes a process to verify the identities of all persons requesting access to Ontario's Electronic Health Record.

The Legally Responsible Person for your organization or practice delegate s authority to the Sponsor (a manager, group, legally responsible person or another individual with approval authority), to verify that these entitlement requirements were followed and approve a user's access for defined and permitted functionality within a user's role .

The Legally Responsible Person for your organization or practice delegate s authority to the Local Registration Agent to review requests for completeness, ensure a user's identity has been verified.

- Your organization may leverage internal HR processes or other processes to satisfy the identity verification requirements. It is important that you understand those processes established by your organization and follow them.
- Organizations using ONE ID must leverage ONE ID processes

Registering and Enrolling Users

What are my obligations when registering and enrolling a user to Ontario's Electronic Health Record?

1. Ensure that each user requesting access to Ontario's Electronic Health Record has had their identity verified in accordance with the Assurance Level 2 (AL2) processes established by your organization in alignment with the Local Registration Authority Practices Policy and eHealth Ontario Federation Identity Provider Standard
2. Ensure that all requests for access to Ontario's Electronic Health Record have been approved by a Sponsor authorized by your Legally Responsible Person.
3. Ensure that a copy of all requests to enroll a user with access to Ontario's Electronic Health Record is retained including Sponsor approval.
    - Registration and enrollment documentation must be retained permanently.

Enrolling a User (1/4)

Below are sample steps taken from the Local Registration Authority Practice Policy, your organization may have established electronic workflows to facilitate these processes or may be leveraging electronic tools provided by your Identity Provider such as ONE ID.

Note: The *End User Enrollment Forms* are templates provided in the LRA Practices Policy (Appendix E & F) to assist in the registration and enrolment process. Your organization may use its own forms, processes, and/or electronic tools in place of these forms, so long as the requisite information is captured.

Sample 1: Provider Portal - Identity Verification previously completed

1. User submits request to Sponsor. Request should contain:
    a) Full Name;
    b) Role/Job Title;
    c) User ID; and
    d) Reason for Access.
2. Sponsor reviews request.
    a) Sponsor reviews and approves request and forwards approval and request to Local Registration Authority.
    b) Sponsor denies request and informs the requestor of the reason for denying request.
3. Local Registration Authority reviews the request to ensure user has been authorized and processes the request.
    a. Approvals have been received:
        i. Files request
        ii. Enables Access
    b. Approvals have not been received:
        i. Denies request and informs the requestor and Sponsor of the reason for denying the request.

Enrolling a User (2/4)

Below are sample steps taken from the Local Registration Authority Practice Policy, your organization may have established electronic workflows to facilitate these processes or may be leveraging electronic tools provided by your Identity Provider such as ONE ID.

Note: The *End User Enrollment Forms* are templates provided in the LRA Practices Policy (Appendix E & F) to assist in the registration and enrolment process. Your organization may use its own forms, processes, and/or electronic tools in place of these forms, so long as the requisite information is captured.

Sample 2: Provider Portal - Identity Verification Required (first time enrollment)

1. User submits request to access the Portal. Request should contain:
    a) Full Name;
    b) Role/Job Title; and
    c) Reason for Access.
2. Sponsor reviews request.
    a) Sponsor reviews and approves request and forwards approval and request to Local Registration Authority.
    b) Sponsor denies request and informs the requestor of the reason for denying request.
3. Local Registration Authority reviews the request to ensure user has been authorized.
    a. Approvals have been received:
        i. Refers the user to their Local Identity Provider and/or ONE ID LRA for identity validation
        ii. Confirms that user has been issued an AL2 credential and adds credential information to request record
        iii. Files request record
        iv. Enables Access
    b. Approvals have not been received:
        i. Denies request and informs the requestor and Sponsor of the reason for denying the request.

Enrolling a User (3/4)

Below are sample steps taken from the Local Registration Authority Practice Policy, your organization may have established electronic workflows to facilitate these processes or may be leveraging electronic tools provided by your Identity Provider such as ONE ID.

Note: The *End User Enrollment Forms* are templates provided in the LRA Practices Policy (Appendix E & F) to assist in the registration and enrolment process. Your organization may use its own forms, processes, and/or electronic tools in place of these forms, so long as the requisite information is captured.

Sample 3: Administration Portals- ***Identity Verification previously completed***

1. User submits request to access the Portal. Request should contain:
    a) Full Name;
    b) Role/Job Title;
    c) User ID;
    d) Reason for Access; and
    e) Signed End User Agreement
2. Sponsor reviews request.
    a) Sponsor reviews and approves request and forwards approval and request to Local Registration Authority.
    b) Sponsor denies request and informs the requestor of the reason for denying request.
3. Local Registration Authority reviews the request to ensure user has been authorized and End User Agreement has been signed.
    a. Approvals have been received and Agreement has been signed:
        i. Local Registration Agent forwards request to eHealth Ontario's Service Desk.
    b. Approvals have not been received or Agreement has not been signed:
        i. Denies request and informs the requestor and Sponsor of the reason for denying the request.
4. Program Office reviews request and enables access.

Enrolling a User (4/4)

Below are sample steps taken from the Local Registration Authority Practice Policy, your organization may have established electronic workflows to facilitate these processes or may be leveraging electronic tools provided by your Identity Provider such as ONE ID.

Note: The *End User Enrollment Forms* are templates provided in the LRA Practices Policy (Appendix E & F) to assist in the registration and enrolment process. Your organization may use its own forms, processes, and/or electronic tools in place of these forms, so long as the requisite information is captured.

Sample 4: Administration Portals- – Identity Verification Required (first time enrollment)

1. User submits request to access the Portal. Request should contain:
    a) Full Name;
    b) Role/Job Title;
    c) User ID;
    d) Reason for Access; and
    e) Signed End User Agreement
2. Sponsor reviews request.
    a) Sponsor reviews and approves request and forwards approval and request to Local Registration Authority.
    b) Sponsor denies request and informs the requestor of the reason for denying request.
3. Local Registration Authority reviews the request to ensure user has been authorized and End User Agreement has been signed.
    a. Approvals have been received and Agreement has been signed:
        i. Refers the user to their Local Identity Provider and/or ONE ID LRA for identity validation
        ii. Confirms that user has been issued an AL2 credential and adds credential information to request record
        iii. Local Registration Agent forwards request to eHealth Ontario's Service Desk.
    b. Approvals have not been received or Agreement has not been signed:
        i. Denies request and informs the requestor and Sponsor of the reason for denying the request.
4. Program Office reviews request and enables access.

Assurance Level 2 (AL2) Requirements

AL2 represents the minimum criteria (i.e. Registration or Authentication) to access Personal Health Information. For AL2 Registrations, the process requires the person to supply verifiable identification:

- At least one identity document from the primary identity document list found in Appendix G of the Local Registration Authority Practice Policy and
- The other identity document being from either the primary identity document list or secondary identity document list found in Appendix G of the Local Registration Authority Practice Policy.

At least one of the identity documents must include a photo of the person and

Both must show the name of the person.

The identity validation processes of ONE ID and other authorized Identity Providers meet these requirements.

Examples

Acceptable Identity Documents

The following are examples of acceptable identity documents to meet Assurance Level 2 Requirements for Registration or Authentication:

Primary Identity Documents

- Driver's License
- Canadian Passport
- Canadian Permanent Resident Card
- Certificate of Canadian Citizenship
- Ontario Photo Card

Secondary Identity Documents

- Canadian Employment Authorization
- Certificate issued by a government ministry or agency, e.g. Marriage, Divorce, Adoption
- Current Professional Association License/Membership Card
- Current Employee Card from a Sponsoring Organization
- Current Registration Document from the College of a Health Profession under the Regulated Health Professions Act, 1991.

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

Entitlement Criteria for the Portals (1/3)

As the Local Registration Authority, you must review requests for completeness. As a Sponsor, you must verify that these entitlement requirements were followed when approving access.

The Sponsor must only approve and provide access to the Provider Portals or Administration Portals to provide support for defined and permitted functionality within the roles as identified below.

Portal	Role	Purpose	Example
Provider Portal	Clinical End User Role	To view personal health information for providing or assisting in the provision of health care.	• Regulated health professional who see patients; • Resident physicians providing care to patients; • Administrative staff who pull charts for physicians; and • Ward clerks who review test results for physicians to flag abnormal results for patients.
Provider Portal (Back End)	Site Support Role	To technically support Clinical End Users who have access to the Provider Portal.	• Help Desk personnel.
Administration Portal	Site Identity Manager Administrator	To manage role access for other types of site administrators. Works with other site administrators to delegate role access/history.	• Individual such as a Local Registration Authority at a site who will manage enrollments to the Administrator Portal
Administration Portal	Site Dead Letter Queue – Error Queue Administrator	To manage site message conformance and errors. Works with eHealth Ontario to investigate message and solution errors. Works with Site Terminology Administrators to investigate site conformance errors.	• System Administrator Individual who will manage inbound messages for data contributors.
Administration Portal	Site Terminology Administrator	To manage site local terminology codes and conformance issues. Works with eHealth Ontario Operations to adhere to the Electronic Health Record terminology repository.	• System Administrator Individual who will manage inbound messages for data contributors.
Administration Portal	Site Privacy Officer	To manage privacy operations processes. Works with Site Privacy Reporting Administrators and eHealth Ontario Privacy Officer during privacy investigations.	• Privacy Officer
Administration Portal	Site Privacy Reporting Administrator	Generates site privacy reports.	• Privacy Officer
Administration Portal	Site Operational Reporting Administrator	Generates site operational, business and adoption and ad-hoc reports.	• System Administrator Individual who will manage inbound messages for data contributors. • Business Analyst

Entitlement Criteria for the Portals (2/3)

Portal	Role	Purpose	Example
Administration Portal	Site Identity Manager Administrator	To manage role access for other types of site administrators. Works with other site administrators to delegate role access/history.	• Individual such as a Local Registration Authority at a site who will manage enrollments to the Administrator Portal
Administration Portal	Site Dead Letter Queue – Error Queue Administrator	To manage site message conformance and errors. Works with eHealth Ontario to investigate message and solution errors. Works with Site Terminology Administrators to investigate site conformance errors.	• System Administrator Individual who will manage inbound messages for data contributors.
Administration Portal	Site Terminology Administrator	To manage site local terminology codes and conformance issues. Works with eHealth Ontario Operations to adhere to the Electronic Health Record terminology repository.	• System Administrator Individual who will manage inbound messages for data contributors.
Administration Portal	Site Privacy Officer	To manage privacy operations processes. Works with Site Privacy Reporting Administrators and eHealth Ontario Privacy Officer during privacy investigations.	• Privacy Officer
Administration Portal	Site Privacy Reporting Administrator	Generates site privacy reports.	• Privacy Officer
Administration Portal	Site Operational Reporting Administrator	Generates site operational, business and adoption and ad-hoc reports.	• System Administrator Individual who will manage inbound messages for data contributors. • Business Analyst

Entitlement Criteria for the Portals (3/3)

What roles or purposes are not permitted access to the Provider Portal?

Sponsors must not approve and provide access to the Provider Portal for other purposes including:

- Program planning, evaluation or monitoring;
- Improving the quality of care, programs and services;
- Research; and
- Education and training (unless the access is required to provide care).

What if a Clinical End User has multiple roles?

- If a Clinical End User has multiple roles, the Sponsor may approve that person's access in order to collect personal health information for the purposes of providing or assisting in the provision of healthcare but must ensure that the Clinical End User understands his or her responsibilities or obligations.

Revoking/Suspending Access

When is user access revoked or suspended?

- As the Local Registration Authority, where you are notified or identify inappropriate access, you must ensure that access privileges are modified, suspended or revoked and follow the incident management protocols to report the situation.

- Once access has been revoked, persons must formally re-enroll in order to have their access reinstated.

Maintaining a Record of Enrolled Users

What do I need to know about maintaining a record of enrolled users?

- You are responsible for ensuring a record is maintained of all users at your organization or practice that have access to Ontario's Electronic Health Record.
  - Another group (i.e. Active Directory) may maintain this list on your behalf.
- You may be required to provide this list to eHealth Ontario upon request.
- The list must include:
  1. First Name
  2. Last Name
  3. Middle Name (if applicable)
  4. Practitioner License Number (if applicable)
  5. Username
  6. Contact details (where available)
  7. Approving Sponsor

How long do I need to keep enrollment and registration information?

- Information collected for provider identification or registration that contains personal information must be kept for at least 7 years after last use.
- Identity providers must keep End User Credential Information permanently.

What are a privacy breach and a security incident?

What are a privacy breach and a security incident?

Be aware that a privacy breach or security incident can be:

- Actual or suspected.
- Intentional or unintentional.

Privacy Breach

A privacy breach in Ontario's Electronic Health Record includes circumstances where:

- A contravention of (or about to be):
  - A provision of the Personal Health Information Protection Act, 2004 or its regulations;
  - Applicable agreements' privacy provisions;
  - Privacy policies, procedures and practices implemented;
- Personal health information is lost or stolen or has been or is about to be accessed for unauthorized purposes; or
- Records of personal health information have been or are about to be copied, modified or disposed of in an unauthorized manner.

Information Security Incident

An information security incident in Ontario's Electronic Health Record is any:

- Violation or imminent threat of violation of information security policies, standards, procedures or practices; or

Learn More

Reminder:

Only access information you require to perform your role.

As part of an organization or practice, you are an agent of that health information custodian and are accountable for adhering to the privacy and security requirements when using Ontario's Electronic Health Record including policies and procedures.

Examples

The following are examples of a privacy breach or security incident:

- **Enrolling a user without Sponsorship.**
- **Changing a user's access privileges without Sponsorship.**
- **Inappropriate access.**
  - Accessing user's identification documents for purposes other than registration.
- **Misdirected email.**
  - Personal health information is sent to members of the public where the wrong email address was used.
  - Sharing of login and password information.
- **Lost enrollment forms.**
- **Compromising the security of Ontario's Electronic Health Record.**
- **Emailing unencrypted personal information or personal health information to eHealth Ontario.**

Case Scenario

- Sam, a Local Registration Authority realizes that he accidently enabled access to the wrong individual (i.e. not the original requestor). What should Sam do?

- Sam should revoke the user's access and contact his Privacy Officer to report the incident. The Privacy Officer will investigate and contact Sam for additional information and support. If Sam is unaware of or does not have a Privacy Officer, Sam should contact eHealth Ontario.

My Role in a Privacy Breach or a Security Incident

What is my role in a privacy breach or a security incident in Ontario's Electronic Health Record?

- **Identify:** If you suspect a privacy breach or security incident has occurred don't second guess yourself - report it.
- **Report:** Report the suspected privacy breach or security incident **immediately** to your Privacy Officer or Security Officer.
  - If you are asked to send personal health information by email to eHealth Ontario for an investigation, encrypt and use a strong password or a secure email system approved by your health information custodian.
- **Contain**: Take reasonable and safe measures to contain the privacy breach or security incident.
  - Do not destroy evidence. It is required for the investigation and may be needed to contact individuals.
- **Participate**: Be prepared to participate in an investigation as required.

Individuals will be informed if their personal health information has been lost, stolen or accessed for unauthorized purposes. This may include the name of the individual that caused the privacy breach or security incident.

If you caused a privacy breach or security incident, you may be subject to consequences established by law, your organization or your practice and/or Electronic Health Record oversight body.

If you are unaware of or do not have a Privacy Officer, refer to eHealth Ontario.

Learn More

- Immediate reporting and action helps prevent a privacy breach or security incident from becoming a big one.
- Your organization or practice has legal obligations to other health information custodians and individuals that they are required to meet.

Privacy and Security Do's and Don'ts (1/3)

Access Personal Information as Authorized or Required to Perform your Role

Do:

- Access personal information as authorized or required to perform your role in enrolling users of Ontario's Electronic Health Record.
- Abide by the terms and conditions of access.

Don't:

- Allow "shoulder surfing"- allowing an unauthorized person to look over your shoulder when entering/accessing sensitive information.
- Discuss or access personal information in public places where others may hear or see the information.
- Take a picture of data displayed on Ontario's Electronic Health Record.

Securely Sharing Personal Health Information for Ontario's Electronic Health Record

Do:

- Communicate with other staff via corporate email.
  - Only email personal health information as required and use ONE Mail or an approved secure file transfer solution.
- Email identifying information to eHealth Ontario only when requested.

Don't:

- Send unencrypted personal information to eHealth Ontario's Service Desk servicedesk@ehealthontario.on.ca.
- Share personal information with anyone except as authorized and required for your job.
- Send from or to any unsecure email accounts, such as Hotmail and Gmail, including your own.

Privacy and Security Do's and Don'ts (2/3)

Using a Unique and Strong Password for Ontario's Electronic Health Record

Do:

- Create a strong and hard-to-guess password by following conventional guidelines and keep your password a secret.
- Use only your own ID and password and protect it- You are accountable for any actions tracked to your account!
- Change your password if you suspect it may have been compromised and notify your Privacy Officer, Security Officer or eHealth Ontario as applicable.
- Always change an initial or temporary password provided to you on first use.

Don't:

- Share your credentials with another person.
- Include your user name or password in any automated single sign-on process unless approved by eHealth Ontario.

Logging in to Approved Devices for Ontario's Electronic Health Record

Do:

- Only use approved devices or processes to access either remotely or locally.
- Only use your own login and protect it. You are accountable for any actions tracked to your login account.
- Log off your account when no longer in use.

Don't:

- Leave your login open and unattended.

Privacy and Security Do's and Don'ts (3/3)

Privacy Breaches and Security Incidents in Ontario's Electronic Health Record

Do:

- Immediately report all suspected or actual privacy breaches or security incidents following your organization's or practice's policies and procedures.
- Support your Privacy Officer or eHealth Ontario when they conduct an audit of access to personal health information.

Don't:

- Change or delete information.

Using Electronic Devices for Ontario's Electronic Health Record

Do:

- Use encrypted devices.
- Only store the minimum amount of personal information necessary (if your organization or practice permits downloads to a portable device).

Don't:

- Leave a computing device in public places or in your car in plain view. Take it with you or lock it in your trunk.
- Disable, bypass or override any information security controls including virus protection.
- Attempt to exploit a real or suspected security weakness.
- Do anything that will interfere with the system's normal operations or the integrity of the information processed by the system.

Password Requirements

- Must contain 8 characters- include at least 3 of the following 1 number, 1 uppercase letter, 1 lowercase letter, 1 special character.
- Never create a password that includes your ID, 3 consecutive letters, an easily recognized pattern or easily obtained personal information about yourself.
- Create a unique password (different from your email or bank account).
- Commit your password to memory- only record it if it can be stored securely.
- Use phases when creating your password (ILOv2EatPizza).

Service ID Password Notes

- *Service IDs are IDs used by an automated information system process to perform specific pre-determined activities (e.g. program start-up, file transfer, backup)*
- *Service IDs must be at least 15 characters in length*
- *Service IDs do not need to be changed on a scheduled basis however equipment must use a new password when technologies change.*

Ontario's Electronic Health Record Privacy and Security Safeguards

In addition to do's and don'ts, what is being done to protect personal health information in Ontario's Electronic Health Record?

Privacy and security are taken very seriously. There are strong protections built into the systems and processes to protect personal health information. The following safeguards have been implemented in respect of Ontario's Electronic Health Record:

Administrative Safeguards:	Physical Safeguards:	Technical Safeguards:
• Appointed Privacy and Security Leads • Privacy and Security Committee to oversee operational activities • Public communications regarding Ontario's Electronic Health Record • Privacy and security training • Agreements with agents and electronic service providers • Privacy and Security policies • Privacy and Security operating procedures and practices • Privacy Impact Assessments and Threat Risk Assessments	• Physically controlled access to servers and networking equipment • Personal health information stored in a secure and redundant data centre • Formalized processes and procedures for the disposal and replacement of hardware	• Login and logouts (logical access controls) • Consent directives (blocked personal health information) • Logging and auditing of user activity • Search controls- open-ended searches are not allowed • Additional authentication mechanisms for system administrators • Headers and footers in printouts • Users who work for more than one organization required to select the appropriate organization when logging in • Protection against anti-virus and malware • Operational monitoring of services for performance and integrity