Privacy and Security Training for Clinical End Users of Ontario's Electronic Health Record

Version 1.3

Welcome to the Privacy and Security Training for Clinical End Users

Hi my name is Pam. What is yours?

User Information

- Please enter the following information in the fields below:
  - Enter your first and last name
  - Enter your job title and organization
  - Enter your license number if applicable and
  - Enter your email address.

Getting Started

- Before you begin - This course consists of 1 module with 18 slides and 5 quiz questions. It will take approximately 15 to 25 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.

Course Objective

By the end of this training, the following questions will be answered and you will understand your privacy and security obligations as a user of Ontario's Electronic Health Record:

1. What is Ontario's Electronic Health Record?
2. Why do I need to complete this training?
3. What are my privacy and security requirements as a user of Ontario's Electronic Health Record?

What is Ontario's Electronic Health Record?

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

- **ConnectingOntario Clinical Data Repository**: clinical reports
- **Diagnostic Imaging Common Services (DI CS) Repository**: diagnostic imaging reports
- **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 you may access. For example:

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

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

When you go into Ontario's Electronic Health Record you may **view** an individual's record of personal health information.

View means that you have collected and/or used the 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; or
- Health card number and medical record number.

Why do I need to complete this training?

Why do I need to complete this training?

- You have a legal obligation to protect individual's privacy with respect to personal health information.
- You must understand acceptable use activities and what constitutes a privacy breach or security incident.
  - Your activities in Ontario's Electronic Health Record are logged and audited.

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

- Protect individuals' privacy by adhering to privacy and security requirements.
- Help individuals exercise their rights in respect of personal health information.
- Facilitate timely responses to individuals' inquiries, requests, concerns or complaints.

Where are these obligations from?

- *Personal Health Information Protection Act, 2004*;
- Your organization's or your practice's privacy and security policies and procedures;
- Electronic Health Record Privacy and Security Policies; and
- Your professional obligations.

The *End User Agreement* binds you to the obligations covered in this training. You will acknowledge the terms during your first login to Ontario's Electronic Health Record and annually thereafter.

What if I do not comply with my obligations?

- You may be subject to consequences established by law, your organization or practice, professional regulatory colleges or bodies and/or the 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?

- It is the law for protecting the privacy of an individual and the confidentiality of an individual's personal health information.
- It 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, "collection, use and disclosure" 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 a health information custodian and a participant in Ontario's Electronic Health Record.
  - A health information custodian is accountable for the personal health information it creates and contributes or collects, uses and discloses.
- As a user you are an agent of a health information custodian.
  - 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
- Adding individuals to your patient list

As a user of Ontario's Electronic Health Record, what is expected of me?

You must understand your expectations with respect to:

- Viewing Personal Health Information
- Understanding Individual Consent
- Consent Directives
- Overriding Consent Directives
- Understanding Access and Correction
- How to Deal with Questions and/or Complaints
- Understanding Privacy Breaches and Security Incidents
- My Role in a Privacy Breach or Security Incident
- Privacy and Security Do's and Don'ts
- 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 or the ClinicalConnect Program Office as applicable.

Rules on Viewing Personal Health Information

When can I view personal health information?

- **All systems:** When providing or assisting in the provision of health care to an individual to whom the personal health information relates.
- **ConnectingOntario Clinical Data Repository and ClinicalConnect:** When eliminating or reducing significant risk of serious bodily harm to an individual or group of individuals where the health care provider believes on reasonable grounds that viewing is necessary. Note: OLIS, DI CS and DHDR cannot be viewed for this purpose.

When you view personal health information, this is logged, monitored and reviewed to ensure that your actions are appropriate.

Learn More

Viewing personal health information found in Ontario's Electronic Health Record for other purposes is not allowed and is a privacy breach; even with the individual's verbal or written consent.

Examples

Examples of privacy breaches in Ontario's Electronic Health Record:

- Snooping in personal health information of family, friends, former patients or known individuals to whom you are not providing care.
- Viewing personal health information for research, training or education.
- Viewing personal health information for billing purposes.
- Viewing personal health information when you are no longer in an individual's circle of care.

Understanding Individual Consent

What do I need to know about individual consent?

1. Be familiar with and follow your organization's or practice's policies and procedures for obtaining consent.
2. If the information in Ontario's Electronic Health Record is not blocked, you may use it to provide care.
3. If an individual or a substitute decision maker asks for more information on consent, refer the individual to your Privacy Officer.

Learn More

Notices and brochures are made available to individuals, either in waiting rooms or other high traffic areas to inform:

- Purposes for which personal health information is viewed; and
- Circumstances to withhold or withdraw consent and how to do so.

Implied or express consent may be used to view personal health information to provide individuals with care. Consent is implied from the individual's behavior, such as attending an appointment at a clinic.

- Only rely on implied consent if an individual understands why you are viewing their personal health information and that they may give or withhold consent.

Examples

Below is an example of a patient brochure that may be used as a notice to patients regarding Ontario's Electronic Health Record.

Ontario's Electronic Health Record Patient Notice.

Case Scenario

It has been 7 years since Dr. Smith saw her patient Jim for his Periodic Health Assessment. Jim has not requested an appointment and had originally requested his personal health information be transferred to another physician.

Should Dr. Smith view Jim's information in Ontario's Electronic Health Record to check on him?

No, Dr. Smith is not currently providing or assisting in the provision of health care to Jim.

Consent Directives

What do I need to do to enable an individual to place a consent directive?

If an individual or a substitute decision maker asks for more information on consent directives, refer the individual to your Privacy Officer.

Note: An individual cannot remove personal health information in Ontario's Electronic Health Record, it can only be blocked.

Learn More and Examples

An individual or substitute decision maker can request a consent directive or '"lock-box" on their personal health information. This will block personal health information from being viewed in Ontario's Electronic Health Record.

With some exceptions, an individual may make, modify or withdraw the following consent directives to personal health information in Ontario's Electronic Health Record:

Consent Directive Type	Description	EHR System				
		ConnectingOntario Clinical Data Repository	Diagnostic Imaging Common Service Repository	Ontario Laboratories Information System	Digital Health Drug Repository	ClinicalConnect
Global	All personal health information.	✓				✓
Domain	All personal health information in a particular repository or system.		✓	✓	✓	✓
HIC-Record	All personal health information created and contributed by a particular organization or practice.	✓	✓			✓
Record	A particular record of personal health information.		✓			✓
HIC-Agent	All users from a particular organization or practice.	✓	✓			
Agent Consent Directives	A particular user.	✓				

Case Scenario

Jennifer wants to place a consent directive to block everyone from accessing her laboratory information in Ontario's Electronic Health Record.

What must you do?

You must direct Jennifer to your Privacy Officer. If you are unaware of or do not have a Privacy Officer, refer Jennifer to eHealth Ontario or ClinicalConnect Program Office.

Overriding Consent Directives

When am I permitted to view personal health information subject to a consent directive?

There are only 3 circumstances for a temporary unblock:

1. You have verbal or written consent from an individual or substitute decision maker (SDM) and the personal health information is required for health care purposes.
2. To prevent harm to the individual and you are not able to obtain consent in a timely manner.
3. To prevent harm to another individual or group of individuals.

Availability in the systems may vary.

Be sure to document the reason for the override in Ontario's Electronic Health Record for audit purposes.

How do I view personal health information subject to a consent directive in the ClinicalConnect ClinicalViewer?

An override may not be performed for ConnectingOntario Clinical Data Repository, DI CS and OLIS.

Express consent from individual or SDM to perform an override in the Home Meds tab:

1. Confirm if a block is in place.
2. Inform individual or SDM:
   - the reason for the override
   - 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 available for 4 hours to all users at the organization.
3. Click Override Consent
4. Print the hard-copy consent form and obtain signature from the individual or SDM
5. Select the Circumstance and fill out SDM information accordingly.
6. Click Override Consent and View Patient Record

MOHLTC Temporary Unblocking Access to Your Drug and Pharmacy Service Information (5047-87)

Overriding Consent Directives

How do I view personal health information subject to a consent directive in the ConnectingOntario ClinicalViewer?
Override for significant risk of bodily harm: select radio button in consent override pop-up. This may only be performed for ConnectingOntario Clinical Data Repository and will not unblock Dispensed Medications or Laboratory Data.

Express consent from individual **or SDM:**

1. Before you perform an override on any portlet, confirm if a block is placed on the Dispensed Medications tab by locating the Consent Override button.
2. Inform 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
ConnectingOntario Clinical Data Repository	Up to 11:59pm on the day that the override was initiated to the user that requested the override.
Ontario Laboratory Information System (OLIS) and DHDR	Available for 4 hours to all users at the organization or practice where the override occurred.

3. Click Override Consent
4. If Dispensed Medications is blocked: print the hard-copy consent form and obtain signature from the individual or SDM; If Dispensed Medications is not blocked obtain verbal or written consent.
5. Select the Circumstance fill out SDM information accordingly
6. Click Override Consent and View Patient Record

MOHLTC Temporary Unblocking Access to Your Drug and Pharmacy Service Information (5047-87)

Note: Access is logged and monitored.

What do I need to know after I have viewed personal health information subject to a consent directive?

- Only view information for the documented purpose you overrode the consent directive.
- Be prepared to explain the reason for the consent override if requested by the individual or your Privacy Officer.
- The individual will be informed when the blocked personal health information has been viewed. The individual will be notified of who viewed and the reason for the consent directive override.

Consent Override Nuances

- An override to prevent harm is not permitted in the Ontario Laboratories Information System, Diagnostic Imaging Common Service and the Digital Health Drug Repository and can only occur when expressly authorized by the individual or substitute decision maker. An attempt to perform an override to prevent harm will not unblock the PHI.
- The individual will receive a notice when a consent directive in any system is overridden.

When accessing via ClinicalConnect ClinicalViewer: an override may not occur for Diagnostic Imaging Common Service, Ontario Laboratories Information System and ConnectingOntario Clinical Data Repository.

When accessing via ConnectingOntario ClinicalViewer: an override will apply to other information/ portlets where a block has been applied. If the Dispensed Medications portlet is blocked and an override is being performed with express consent, you must receive a physical signature from the individual or substitute decision-maker.

Case Scenario

Lisa has been admitted for a broken arm due to a heavy fall from playing basketball. She is conscious and aware of her surroundings. Dr. Adam views Lisa's record to view her x-ray report, but there is a consent directive on her Diagnostic Imaging information.

What should he do next?

Dr. Adam must let Lisa know:

1. He would like to view her Diagnostic Imaging information to review the x-ray that was just completed to determine where the break is located.
2. Dr. Adam will not view the x-ray report for any other purpose.
3. Lisa's information will be viewable for 4 hours by any user at the organization or practice where the override was placed.
4. She has the option to grant or refuse Dr. Adam the override of the consent directive.

Understanding Access and Correction

What do I need to know about requests to access and correct personal health information?

Individuals have the right to request to view and obtain a copy of:

- Their personal health information in Ontario's Electronic Health Record.
- Reports about who has viewed their personal health information in Ontario's Electronic Health Record, *including user name, their actions, data accessed and date and time of action.*
- Consent directive history in Ontario's Electronic Health Record *including applying, changing or removing consent directives and consent directive overrides.*

How am I involved in an access or correction request?

If an individual wishes to view or obtain a copy of logs of access to their personal health information in Ontario's Electronic Health Record, refer the individual to your Privacy Officer.

- *When providing care to an individual, you may grant that individual access to their personal health information you collected, created or contributed if they make a verbal request.*

An individual has the right to request a correction if they believe the personal health information is incomplete or inaccurate refer the individual to your Privacy Officer.

- *Your Privacy Officer (or eHealth Ontario or ClinicalConnect Program Office) may request your assistance in determining if the request for a correction should be granted.*

Case Scenario

Johanna is suspicious that her cousin, a medical clerk at a hospital, has viewed her personal health information. She was suspicious as he knew about her recent MRI without her mentioning it. Johanna asks you if she can see who has viewed her personal health information.

Is this possible?

Yes, Johanna may make an access request for a report of who has viewed her personal health information. Direct Johanna to your Privacy Officer. If you are unaware of or do not have a Privacy Officer, refer Johanna to eHealth Ontario or ClinicalConnect Program Office.

How to Respond to Questions and Complaints

What do I need to do if an individual asks a question or wants to make a complaint?

- Answer questions directly if you can, and if not, direct the individual to your Privacy Officer.
- Direct all complaints to your Privacy Officer.

Learn More

An individual has a right to make an inquiry or complaint to your organization or practice or to eHealth Ontario, in accordance with your organization or practice's policies and procedures.

Individuals also have a right to make a complaint to the Information and Privacy Commissioner of Ontario (IPC).

Case Scenario

Johanna has received a report of who has viewed her personal health information in Ontario's Electronic Health Record and confirmed that her cousin did in fact view her personal health information. She is furious and would like something done.

How can you help Johanna?

Direct Johanna to your Privacy Officer who will launch an investigation. If you are unaware of or do not have a Privacy Officer, refer Johanna to eHealth Ontario or ClinicalConnect Program Office.

Understanding Privacy Breaches and Security Incidents

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
- Information security event that may compromise operations or threaten the security of Ontario's Electronic Health Record or related business process.

Purpose for Viewing:

Reminder:

You may not view personal health information outside of:

- Providing direct health care to an individual; or
- Eliminating or reducing the risk of bodily harm.

Access for research, training or secondary use is not permitted.

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.

All actions under your account are logged, monitored and reviewed on a regular basis.

- *You are accountable for your actions.*
- *Do not share your username and password with others.*

Examples

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

- **Inappropriate access of personal health information.**
  - Viewing personal health information:
    - For a reason other than health care.
    - About yourself.
    - About your children, partners, spouses, friends and family.
    - Of neighbours, public figures, exes, in-laws, etc. because you are curious ("snooping").
  - Searching personal health information for "educational purposes" as part of a research and/or teaching hospital.
- **Modification to your own or family members' personal health information.**
- **Inappropriate handling of printouts containing personal health information.**
  - Left behind in a coffee shop or other public space.
  - Wrongly disposed of in a recycling bin, rather than securely shredded.
- **Misdirected printing of personal health information.**
  - Printing to the wrong printer resulting in documents being viewed by unauthorized persons or being lost.
- **Misdirected fax or email with personal health information.**
  - Wrong fax number or email address of other healthcare practitioners or members of the public.
- **Sharing of login and password information**.
  - Colleague uses your account to quickly view an individual because you are already logged in.
- **Failure to log-off properly, leaving personal health information visible and system available for unauthorized access.**
- **Discussing personal health information with unauthorized individuals**:
  - Colleagues who are not providing or assisting in provision of health care.
  - Family or friends after work.
  - After employment ends or you retire.
- **Theft or loss of personal health information.**
- **Virus or malware infection.**

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.

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)

Viewing Personal Health Information for Health Care in Ontario's Electronic Health Record

Do:

- Only view for individuals to whom you are providing health care.
- Only view information subject to a consent directive override for the purpose for which it was overridden and for the time required.
  - For example, do not print personal health information for later use. It can only be used at that time, for that purpose.

Don't:

- Discuss or view information in public places where others may hear or see.
- Take a picture of information displayed.

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

Do:

- Only share with those in an individual's circle of care.

Don't:

- 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:

- Change your password if you suspect it may have been compromised and notify your Privacy Officer, Security Officer, eHealth Ontario or ClinicalConnect Program Office as applicable.
- 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.

Don't:

- 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.

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, eHealth Ontario or ClinicalConnect Program Office 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 health 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 or 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.

Recommend using phrases when creating your password (ILOv2EatPizza).

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