Ontario's Electronic Health Record Privacy and Security Training for Technical and Operational Support

Version 1.1

Welcome to the Privacy and Security Training for Technical and Operational Support

Hi my Name is Susan. 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 email address

Getting Started

- Before you Begin - this course consists of 1 module with 23 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.

Course Objective

By the end of this training, you will understand your privacy and security obligations 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. When Providing Technical and Operational Support for 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

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

When you support Ontario's Electronic Health Record you may view personal health information.

View means that you have viewed, handled or otherwise dealt with 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; 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 have a legal obligation to protect individual's privacy with respect to personal health information.
- You have access to Ontario's Electronic Health Record to perform technical or operational support in your role and must understand acceptable 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; and
- Electronic Health Record Privacy and Security Policies.

The *EHR Portal User Agreement* binds you to the obligations covered in this training. You will acknowledge the terms during your first login, or prior to logging in 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 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.
- 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)

Why Do I Have Access to Personal Health Information?

I do not provide health care, why do I have to access Personal Health Information?

Although you do not provide direct health care to patients, you have access to personal health information in Ontario's Electronic Health Record when providing technical or operational support.

- Access will be granted according to your role by your Local Registration Agent.
- Access will be revoked if you leave the organization or change roles.

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

Click on your role to learn what is expected of you:

1. Administrator – Manage systems that interact with Ontario's Electronic Health Record
2. Tester – Perform development and testing activities to support Ontario's Electronic Health Record
3. Clinical Validator (Health Infomatician) - Perform data quality assurance activities on personal health information in Ontario's Electronic Health Record
4. Site Help Desk – provide technical support to Clinical End Users and intake point for Ontario's Electronic Health Record
5. TELUS Service Desk – provide first line of support for ConnectingOntario

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.

Administrator (1/4)

What is my role when accessing Ontario's Electronic Health Record?

You have access to Ontario's Electronic Health Record to manage systems and errors associated with your organization or practice's transactions that are processed in the Health Information Access Layer for Ontario's Electronic Health Record.

Administrator (2/4)

What is expected of me when accessing Personal Health Information?

Follow your organization's or practice's procedures as well as the do's and don'ts.

In addition:

- Only access personal health information that is needed to perform your role.
  - Be able to map each access to personal health information to a ticket or for a specific purpose. **Accessing your own records or those of your family members, friends or colleagues, etc. is not permitted in Ontario's Electronic Health Record.**
- Keep personal health information confidential, even after the service contract or employment has ended, by observing key security safeguards identified in this training.
- All access is logged and monitored - do not disable these capabilities or overwrite, modify, erase or deactivate logs.
- Talk to your Privacy Officer or Security Officer if you have questions.

Administrator (3/4)

What do I need to know when addressing errors or bugs for Ontario's Electronic Health Record?

Follow your organization's or practice's procedures:

- Securely store and delete personal health information
  - Personal health information must be stored in a secure location. Access to this location must be limited to required personnel.
- When exporting personal health information, have documented approval from your manager or ensure it is part of your defined job responsibilities.

Administrator (4/4)

How do I report an issue/ send personal health information to eHealth Ontario?

1. Request a ticket be opened via email or telephone to the eHealth Ontario Service Desk. Do not include personal health information in your request.
2. Transmit the encrypted personal health information using a secure file transfer solution or a secure email system approved by your organization (i.e. ONE Mail) when requested by the eHealth Ontario agent, if required.
3. Delete the sent email from your outbox (SHIFT+DELETE) .

Tester (1/4)

What is my role when accessing Ontario's Electronic Health Record?

You have access to Ontario's Electronic Health Record to perform development and testing activities to support Ontario's Electronic Health Record.

Tester (2/4)

What is expected of me when accessing Personal Health Information?

Follow your organization's or practice's procedures as well as the do's and don'ts.

In addition:

- Only access personal health information that is needed to perform your role.
  - Be able to map each access to personal health information to a ticket or for a specific purpose. **Accessing your own records or those of your family members, friends or colleagues, etc. is not permitted in Ontario's Electronic Health Record.**
- Keep personal health information confidential, even after the service contract or employment has ended, by observing key security safeguards identified in the training.
- All access is logged and monitored - do not disable these capabilities or overwrite, modify, erase or deactivate logs.
- Talk to your Privacy Officer or Security Officer if you have questions.

Tester (3/4)

What do I need to know when performing development and testing activities?

- Follow the testing instructions provided to you.
- Only use non-production environments.
  - Non-production environments must not be connected to the Ontario's Electronic Health Record production environments.
  - When conducting performance testing, personal health information must not be accessed. If you encounter personal health information, report this immediately to your Privacy Officer.
- If you are required to export or receive personal health information, save it in a secure location, not in a non-production environment or tracking system. Access to this location must be limited to required personnel.
  - Have documented approval from your manager or ensure it is part of your defined job responsibilities to export personal health information.
- Document configuration changes, such as through a change control process.
- Ensure that all security deficiencies or vulnerabilities identified during testing reviews are identified, communicated, corrected or the risk is accepted by the appropriate party prior to production implementation.
- Assess the impact and follow Change Management procedures to notify affected parties when modifying production services.

The information I am testing is blocked, what do I need to know?

The blocked information may mean that a consent directive has been placed on the personal health information.

Do not override this consent directive unless the test relates specifically to testing consent directive functionality.

  - In the event you override a consent directive not related to testing functionality, an investigation of the access will be conducted by your Privacy Officer.
    - Be prepared to explain the reason for the consent directive override.
    - Your organization or practice will notify the individual when his or her blocked personal health information has been viewed to inform who accessed the record of personal health information and the reason for the consent directive override.

Tester (4/4)

How do I report an issue identified during testing or send personal health information to eHealth Ontario?

1. Input the personal health information into the Test Report template, encrypt the template and save to your corporate computer.
   - Remove personal health information from a bug report where it is not required.
   - Do not print personal health information.
2. Request a ticket be opened and assigned to ConnectingOntario AMS via email or telephone to the eHealth Ontario Service Desk. Do not include personal health information in your request.
3. Transmit the encrypted Test Report using a secure file transfer solution or a secure email system approved by your organization (i.e. ONE Mail) when requested by ConnectingOntario AMS.
4. Delete the sent email from your outbox (SHIFT+DELETE) and the Test Report from your computer.

Clinical Validator (1/3)

What is my role when accessing Ontario's Electronic Health Record?

You have access to the Ontario's Electronic Health Record to perform data quality assurance activities by reviewing, comparing and validating personal health information.

Clinical Validator (2/3)

What is expected of me when accessing Personal Health Information?

Follow your organization's or practice's procedures as well as the do's and don'ts.

In addition,

- Only access personal health information that is needed to perform your role.
  - Be able to map each access to personal health information to a ticket or for a specific purpose. **Accessing your own records or those of your family members, friends or colleagues, etc. is not permitted in Ontario's Electronic Health Record.**
- Securely store and delete personal health information.
  - Personal health information must be stored in a secure location. Access to this location must be limited to required personnel.
  - When logging issues or requests, do not store personal health information in the tracking system or your request.
- Keep personal health information confidential, even after the service contract or employment has ended, by observing key security safeguards identified in the training.
- All access is logged and monitored - do not disable these capabilities or overwrite, modify, erase or deactivate logs.
- Talk to your Privacy Officer or Security Officer if you have questions.

Clinical Validator(3/3)

What do I need to know when performing validation activities?

- Follow the testing instructions provided to you.
- Confirm that the personal health information generated from your health information system matches the personal health information displayed in Ontario's Electronic Health Record.
- Ensure that any correction made to any personal health information in the health information system has been replicated in the Ontario's Electronic Health Record as expected and appropriate.
- Assist users accessing Ontario's Electronic Health Record with any concerns they may have with data integrity, verification and accuracy.
- If you are required to export or receive personal health information, save it in a secure location, not in a non-production environment or tracking system. Access to this location must be limited to required personnel.
  - Have documented approval from your manager or ensure it is part of your defined job responsibilities to export personal health information.

The information I am testing is blocked, what do I need to know?

The blocked information may mean that a consent directive has been placed on the personal health information.

Do not override this consent directive unless the test relates specifically to testing consent directive functionality.

- In the event you override a consent directive not related to testing functionality, an investigation of the access will be conducted by your Privacy Officer.
  - Be prepared to explain the reason for the consent directive override.
  - Your organization or practice will notify the individual when his or her blocked personal health information has been viewed to inform who accessed the record of personal health information and the reason for the consent directive override.

Site Help Desk (1/6)

What is my role when accessing Ontario's Electronic Health Record?

You have access to Ontario's Electronic Health Record to provide technical support to Clinical End Users of Ontario's Electronic Health Record.

This includes intake on system errors and bugs, privacy inquiries and complaints, privacy breaches, and security incidents.

Site Help Desk (2/6)

What do I need to know when I intake a request or issue for Ontario's Electronic Health Record?

- Securely store and delete personal health information
  - Personal health information must be stored in a secure location. Access to this location must be limited to required personnel.
  - When logging issues or requests, do not store personal health information in the tracking system.
- When exporting personal health information, have documented approval from your manager or ensure it is part of your defined job responsibilities.

Site Help Desk (3/6)

What is expected of me when in contact with Personal Health Information?

- Follow your organization's or practice's procedures as well as the do's and don'ts.
- Only access personal health information that is needed to perform your role.
  - Be able to map each access to personal health information to a ticket or for a specific purpose. **Accessing your own records or those of your family members, friends or colleagues, etc. is not permitted in Ontario's Electronic Health Record.**
- Keep personal health information confidential, even after the service contract or employment has ended, by observing key security safeguards identified in the training.
- All access is logged and monitored - do not disable these capabilities or overwrite, modify, erase or deactivate logs.
- Talk to your Privacy Officer or Security Officer if you have questions.

Site Help Desk (4/6)

How do I report an a system error, bug or other issue to eHealth Ontario?

1. Input the personal health information into the Tracking Report template, encrypt the template and save to your corporate computer.
   - Remove personal health information from the report where it is not required.
   - Do not print personal health information.
2. Request a ticket be opened and assigned to ConnectingOntario AMS via email or telephone to the eHealth Ontario Service Desk. Do not include personal health information in your request.
3. Transmit the encrypted Tracking Report using a secure file transfer solution or a secure email system approved by your organization (i.e. ONE Mail) when requested by ConnectingOntario AMS.
4. Delete the sent email from your outbox (SHIFT+DELETE) and the Tracking Report from your computer.

Site Help Desk (5/6)

I am investigating the issue and the information in the system is blocked. What do I do?

The blocked information may mean that a consent directive has been placed on the personal health information.

Do not override this consent directive; you do not have permission to access this information.

- In the event you override a consent directive an investigation of the access will be conducted by your Privacy Officer.
  - Be prepared to explain the reason for the consent directive override.
  - Your organization or practice will notify the individual when his or her blocked personal health information has been viewed to inform who accessed the record of personal health information and the reason for the consent directive override.

Site Help Desk (6/6)

What do I need to know when receiving privacy requests, privacy breaches, and security incidents for Ontario's Electronic Health Record?

Perform your intake following your organization or practice's procedures, then:

- Direct privacy issues, requests or breaches to your Privacy Officer. If you are unaware of or do not have a Privacy Officer, contact eHealth Ontario.
- Direct security incidents to your Security Officer; If you are unaware of or do not have a Security Officer, contact eHealth Ontario.

Do not email personal health information to eHealth Ontario. If the personal health information is required, provide it securely to an authorized agent when requested.

Examples

Examples of privacy and security inquiries, complaints or requests you may receive:

From a patient:

- The patient wants a consent directive.
- Patient has a question or concern about the Ontario's Electronic Health Record.
- Patient wants to see a copy of his or her record.
- Patient wants to know who has looked at his or her record.
- Patient does not want anyone to see his or her record.
- Patient requests anything related to privacy.
- Patient would like to know what security controls are in place for Ontario's Electronic Health Record.

From the Clinician:

- The patient has a request.
- Clinician doesn't know how to override a consent directive.
- Clinician wants to give the patient a log of who has accessed his or her record.
- Clinician wants to know whether he or she can look at information from another hospital or clinic.
- Clinician wants to know whether he or she can use the information for research or another purpose.
- Clinician thinks someone may have used his or her credentials to access the solution.
- Clinician would like to report a privacy breach or security incident.

TELUS Service Desk (1/3)

What is my role when accessing Ontario's Electronic Health Record?

You are the first line of technical support for Ontario's Electronic Health Record.

TELUS Service Desk (2/3)

What do I need to know when providing support for Ontario's Electronic Health Record?

- Follow your organization's or practice's procedures as well as the do's and don'ts.

In addition:

- Instruct callers to report an issue to the ConnectingOntario Service Desk. Personal health information must be encrypted and password protected when transmitted via email.
- Only access personal health information that is needed to perform your role.
  - Be able to map each access to personal health information to a ticket or for a specific purpose. **Accessing your own records or those of your family members, friends or colleagues, etc. is not permitted in Ontario's Electronic Health Record.**
- Securely store and delete personal health information
  - Personal health information must be stored in a secure location. Access to this location must be limited to required personnel.
  - When logging issues or requests, do not store personal health information in the tracking system.
- When exporting personal health information, have documented approval from your manager or ensure it is part of your defined job responsibilities.
- All access is logged and monitored - do not disable these capabilities or overwrite, modify, erase or deactivate logs.

TELUS Service Desk (3/3)

What do I need to know when addressing errors or bugs for Ontario's Electronic Health Record?

- Ensure issues received are from authorized persons at the site or verify their identity using the scripts provided to you.
- Only collect personal health information when it is absolutely necessary.
  - If personal health information is required, instruct the requestor to email the encrypted and password protected information to the ConnectingOntario Service Desk.
- Log the issue in a ticket if appropriate, but do not include any personal health information in the ticket (including HEAT, Remedy).
- You may only forward email from the Ontario's Electronic Health Record Support Mailbox to the appropriate responder (i.e. Tier 2) if the responder is on ONE Mail and when they request.

eHealth Ontario

I may access personal information or personal health information when providing technical and operational support for eHealth Ontario systems and services. What am I required to do prior to accessing the system?

You must ensure direct or incidental access to personal information and personal health information is granted through the formal provisioning channels (i.e. ONE ID Registration or Logical Access Request Process).

Before submitting your request ensure:

1. Purpose of access is within your role and defined job responsibilities.
2. Required approvals have been obtained.
3. Privacy Fundamentals and this training are complete.

When you have access to the system(s), you must follow your privacy and security responsibilities for each activity you perform.

eHealth Ontario

Learn More

eHealth Ontario systems and services include all systems and repositories managed by eHealth Ontario when providing:

- Health Information Network Provider (HINP) services such as ONE Network and ONE Mail services to a health information custodian.
- Ontario Regulation 329/04, s6.2 services to create or maintain an electronic health record such as ConnectingOntario.
- Agent services such as Provincial Client Registry (ProvCR) and Ontario Laboratories Information Systems (OLIS).
- Electronic Service Provider products and services such as hosting.

eHealth Ontario

Click on the activity you may perform:

Data Analytics/ Statistics
- Solution Development & Maintenance
- Solutions Architecture/Infrastructure Architecture/Standards
- Product Roadmap Management
- Technology Planning
- Product Management
- Account Management
- Enterprise Planning and Reporting

Data Integrity/ Data Quality
- Data Quality Management
- Account Management

Specification,/Penetration/Error Testing
- Security Operations
- Solutions Development
- Data Quality Management
- Testing
- Quality Assurance
- Account Management

Clinical Validation Testing
- Data Quality Management

Build and Deploy
- Application Services
- Application Support
- Technology Platform Services
- Integration
- Service Transition

Generate/ Review Reports
- Privacy
- Application Services
- Account Management
- Product Management
- Enterprise Planning and Reporting

Troubleshooting / Support
- Infrastructure Service Delivery
- Application Services
- Application Support
- Account Management

Health Checks
- Infrastructure Service Delivery
- Application Services

Consent Management/Access and Correction/Privacy Audit Support
- Privacy

Data Analytics/ Statistics (1/2)

What is my role when accessing eHealth Ontario systems and services ?

You have access to eHealth Ontario systems and services to generate and analyze reports for business intelligence and functionality.

Data Analytics/ Statistics (2/2)

What is expected of me when accessing Personal Health Information?

- Only access personal health information that is needed to perform your role.
  - Remove personal information or personal health information from reports if it is not required.
  - Be able to map each access to personal health information to a ticket or for a specific purpose. **Accessing your own records or those of your family members, friends or colleagues, etc. is not permitted in eHealth Ontario systems and services.**
  - When exporting personal health information, have documented approval from your manager or ensure it is part of your defined job responsibilities.
- Securely store and delete personal health information
  - Personal health information must be stored in a secure location. Access to this location must be limited to required personnel. Personal health information must not be stored in SharePoint.
  - When logging issues or requests, do not store personal health information in the tracking system or your request.
- Keep personal health information confidential, even after the service contract or employment has ended, by observing key security safeguards identified in the training.
- All access is logged and monitored - do not disable these capabilities or overwrite, modify, erase or deactivate logs.
- Talk to your Privacy Officer or Security Officer if you have questions.

Data Integrity/ Data Quality (1/3)

What is my role when accessing eHealth Ontario systems and services?

You access eHealth Ontario systems and services to ensure the integrity and accuracy of data.

Data Integrity/ Data Quality (2/3)

What is expected of me when accessing Personal Health Information?

- Only access personal health information that is needed to perform your role.
  - Be able to map each access to personal health information to a ticket or for a specific purpose. **Accessing your own records or those of your family members, friends or colleagues, etc. is not permitted in eHealth Ontario systems and services.**
  - When exporting personal health information, have documented approval from your manager or ensure it is part of your defined job responsibilities.
- Securely store and delete personal health information
  - Personal health information must be stored in a secure location. Access to this location must be limited to required personnel. Personal health information must not be stored in SharePoint.
  - When logging issues or requests, do not store personal health information in the tracking system or your request.
- Keep personal health information confidential, even after the service contract or employment has ended, by observing key security safeguards identified in the training.
- All access is logged and monitored - do not disable these capabilities or overwrite, modify, erase or deactivate logs.
- Talk to your Privacy Officer or Security Officer if you have questions.

Data Integrity/ Data Quality (3/3)

The information I am reviewing is blocked, what do I need to know?

The blocked information may mean that a consent directive has been placed on the personal health information.

Do not override this consent directive; you do not have permission to access this information.

- In the event you override a consent directive an investigation of the access will be conducted by your Privacy Officer.
  - Be prepared to explain the reason for the consent directive override.
  - The individual will be notified when his or her blocked personal health information has been viewed to inform who accessed the record of personal health information and the reason for the consent directive override.

Testing (Penetration Testing, Conformance Testing, Error Testing) (1/3)

What is my role when accessing eHealth Ontario systems and services?

You have access to eHealth Ontario systems and services to ensure systems and applications run according to the standards.

Testing (Conformance Testing, Penetration Testing, Error Testing) (2/3)

What is expected of me when accessing Personal Health Information?

- Only access personal health information that is needed to perform your role.
  - Be able to map each access to personal health information to a ticket or for a specific purpose. **Accessing your own records or those of your family members, friends or colleagues, etc. is not permitted in eHealth Ontario systems and services.**
- Securely store and delete personal health information
  - Personal health information must be stored in a secure location. Access to this location must be limited to required personnel. Personal health information must not be stored in SharePoint.
  - When logging issues or requests, do not store personal health information in the tracking system or your request.
- Keep personal health information confidential, even after the service contract or employment has ended, by observing key security safeguards identified in the training.
- All access is logged and monitored - do not disable these capabilities or overwrite, modify, erase or deactivate logs.
- Talk to your Privacy Officer or Security Officer if you have questions.

Testing (Conformance Testing, Penetration Testing, Error Testing) (3/3)

What do I need to know when performing development and testing activities?

- Follow the testing instructions provided to you.
- Only use non-production environments.
  - Non-production environments must not be connected to production environments.
  - When conducting performance testing, personal health information must not be accessed. If you encounter personal health information, report this immediately to your Privacy Officer.
- If you are required to export or receive personal health information, save it in a secure location, not in a non-production environment or tracking system. Access to this location must be limited to required personnel.
  - Have documented approval from your manager or ensure it is part of your defined job responsibilities to export personal health information.
- Document configuration changes, such as through a change control process.
- Ensure that all security deficiencies or vulnerabilities identified during testing reviews are identified, communicated, corrected or the risk is accepted by the appropriate party prior to production implementation.
- Assess the impact and follow Change Management procedures to notify affected parties when modifying production services.

The information I am testing is blocked, what do I need to know?

The blocked information may mean that a consent directive has been placed on the personal health information.

Do not override this consent directive unless the test relates specifically to testing consent directive functionality.

- In the event you override a consent directive not related to testing functionality, an investigation of the access will be conducted by your Privacy Officer.
  - Be prepared to explain the reason for the consent directive override.
  - Your organization or practice will notify the individual when his or her blocked personal health information has been viewed to inform who accessed the record of personal health information and the reason for the consent directive override.

Clinical Validation (1/3)

What is my role when accessing eHealth Ontario systems and services?

You have access to eHealth Ontario systems and services to perform data quality assurance activities by reviewing, comparing and validating personal health information.

Clinical Validation (2/3)

What is expected of me when accessing Personal Health Information?

- Only access personal health information that is needed to perform your role.
  - Be able to map each access to personal health information to a ticket or for a specific purpose. **Accessing your own records or those of your family members, friends or colleagues, etc. is not permitted in eHealth Ontario systems and services.**
- Securely store and delete personal health information
  - Personal health information must be stored in a secure location. Access to this location must be limited to required personnel.
  - When logging issues or requests, do not store personal health information in the tracking system or your request.
- Keep personal health information confidential, even after the service contract or employment has ended, by observing key security safeguards identified in the training.
- All access is logged and monitored - do not disable these capabilities or overwrite, modify, erase or deactivate logs.
- Talk to your Privacy Officer or Security Officer if you have questions.

Clinical Validation(3/3)

What do I need to know when performing validation activities?

- Follow the testing instructions provided to you.
- Confirm that the personal health information generated from your health information system matches the personal health information displayed in eHealth Ontario systems and services.
- Ensure that any correction made to any personal health information in the health information system has been replicated in eHealth Ontario systems and services as expected and appropriate.
- Assist users accessing eHealth Ontario systems and services with any concerns they may have with data integrity, verification and accuracy.
- If you are required to export or receive personal health information, save it in a secure location, not in a non-production environment or tracking system. Access to this location must be limited to required personnel.
  - Have documented approval from your manager or ensure it is part of your defined job responsibilities to export personal health information.

The information I am testing is blocked, what do I need to know?

The blocked information may mean that a consent directive has been placed on the personal health information.

Do not override this consent directive unless the test relates specifically to testing consent directive functionality.

- In the event you override a consent directive not related to testing functionality, an investigation of the access will be conducted by your Privacy Officer.
  - Be prepared to explain the reason for the consent directive override.
  - Your organization or practice will notify the individual when his or her blocked personal health information has been viewed to inform who accessed the record of personal health information and the reason for the consent directive override.

Build/Deploy (1/2)

What is my role when accessing eHealth Ontario systems and services?

You have access to provide tools and techniques to automate and streamline build and development functions to optimize processes.

Your activities may include planning, building, preparing and deploying.

Build/Deploy (2/2)

What is expected of me when accessing Personal Health Information?

- You may have incidental access to personal health information when performing your role.
  - Be able to map each access to personal health information to a ticket or for a specific purpose. Accessing your own records or those of your family members, friends or colleagues, etc. is not permitted in eHealth Ontario systems and services.
  - Non-production environments must not be connected to production environments. If you encounter personal health information, report this immediately to your Privacy Officer.
- When logging issues or requests, do not store personal health information in the tracking system or your request.
- Document configuration changes, such as through a change control process.
- Ensure that all security deficiencies or vulnerabilities identified during testing reviews are identified, communicated, corrected or the risk is accepted by the appropriate party prior to production implementation.
- Assess the impact and follow Change Management procedures to notify affected parties when modifying production services.
- All access is logged and monitored - do not disable these capabilities or overwrite, modify, erase or deactivate logs.
- Talk to your Privacy Officer or Security Officer if you have questions.

Generate/ Review Reports (1/2)

What is my role when accessing eHealth Ontario systems and services?

You have access to generate scripts, logs and reports for lines of businesses to support internal and external investigations, audits, access, consent management for systems and services.

Generate/ Review Reports (2/3)

What is expected of me when accessing Personal Health Information?

- Only access personal health information that is needed to perform your role.
  - Be able to map each access to personal health information to a ticket or for a specific purpose. **Accessing your own records or those of your family members, friends or colleagues, etc. is not permitted in eHealth Ontario systems and services.**
- Securely store and delete personal health information
  - Personal health information must be stored in a secure location. Access to this location must be limited to required personnel. Personal health information must not be stored in SharePoint.
  - When logging issues or requests, do not store personal health information in the tracking system or your request.
- When exporting personal health information, have documented approval from your manager or ensure it is part of your defined job responsibilities.
- When sharing personal health information
  - Personal health information may only be shared from one ONE Mail account to another. An approved secure file transfer solution must be used when sharing information outside of ONE Mail.
  - Password should be communicated in a secure manner (i.e. directly to the individual or via telephone).
  - Ensure only the intended recipients are provided the message and password.
- Keep personal health information confidential, even after the service contract or employment has ended, by observing key security safeguards identified in the training.
- All access is logged and monitored - do not disable these capabilities or overwrite, modify, erase or deactivate logs.
- Talk to your Privacy Officer or Security Officer if you have questions.

Generate/ Review Reports (3/3)

The information I am testing is blocked, what do I need to know?

The blocked information may mean that a consent directive has been placed on the personal health information.

Do not override this consent directive unless the test relates specifically to testing consent directive functionality.

- In the event you override a consent directive not related to testing functionality, an investigation of the access will be conducted by your Privacy Officer.
  - Be prepared to explain the reason for the consent directive override.
  - The individual will be notified when his or her blocked personal health information has been viewed to inform who accessed the record of personal health information and the reason for the consent directive override.

Troubleshooting/Support

What is my role when accessing eHealth Ontario systems and services?

You have access to address technical errors, bugs and connectivity, update personal health information as part of a correction request; and support the application or modification of consent directives.

Troubleshooting/Support

What is expected of me when accessing Personal Health Information?

- Only access personal health information that is needed to perform your role.
  - Be able to map each access to personal health information to a ticket or for a specific purpose. **Accessing your own records or those of your family members, friends or colleagues, etc. is not permitted in eHealth Ontario systems and services.**
- Securely store and delete personal health information
  - Personal health information must be stored in a secure location. Access to this location must be limited to required personnel. Personal health information must not be stored in SharePoint.
  - When logging issues or requests, do not store personal health information in the tracking system or your request.
- When exporting personal health information, have documented approval from your manager or ensure it is part of your defined job responsibilities.
- When sharing personal health information
  - Personal health information may only be shared from one ONE Mail account to another. An approved secure file transfer solution must be used when sharing information outside of ONE Mail.
  - Password should be communicated in a secure manner (i.e. directly to the individual or via telephone).
  - Ensure only the intended recipients are provided the message and password.
- Keep personal health information confidential, even after the service contract or employment has ended, by observing key security safeguards identified in the training.
- Retain and dispose of personal health information and related records (such as logs) as directed by the *Electronic Health Record Retention Policy* for ConnectingOntario and Diagnostic Imaging Common Services and the *eHealth Ontario Personal Health Information Policy* for MOHLTC assets.
- All access is logged and monitored - do not disable these capabilities or overwrite, modify, erase or deactivate logs.
- Talk to your Privacy Officer or Security Officer if you have questions.

Troubleshooting/Support

What must be recorded when closing an error or bug request?

If you are responsible for closing an error or bug request (or when telling someone to close the request), you must record:

- If personal health information was accessed, transmitted, or otherwise handled;
- The reason for that; and
- The date that it was accessed, transmitted, or handled.

The information I am testing is blocked, what do I need to know?

The blocked information may mean that a consent directive has been placed on the personal health information.

Do not override this consent directive unless the test relates specifically to testing consent directive functionality.

- In the event you override a consent directive not related to testing functionality, an investigation of the access will be conducted by your Privacy Officer.
  - Be prepared to explain the reason for the consent directive override.
  - Your organization or practice will notify the individual when his or her blocked personal health information has been viewed to inform who accessed the record of personal health information and the reason for the consent directive override.

(Daily) Health Checks (1/2)

What is my role when accessing eHealth Ontario systems and services?

You have access to eHealth Ontario systems and services to perform an end to end assessment of the ability of eHealth Ontario systems and services to meet defined availability and recovery service-level targets. You conduct end to end solution checks to identify gaps and remediation activities.

(Daily) Health Checks(2/2)

What is expected of me when accessing Personal Health Information?

- Only access personal health information that is needed to perform your role.
  - Be able to map each access to personal health information to a ticket or for a specific purpose. **Accessing your own records or those of your family members, friends or colleagues, etc. is not permitted in eHealth Ontario systems and services.**
- Securely store and delete personal health information
  - Personal health information must be stored in a secure location. Access to this location must be limited to required personnel. Personal health information must not be stored in SharePoint.
  - When logging issues or requests, do not store personal health information in the tracking system or your request.
- When exporting personal health information, have documented approval from your manager or ensure it is part of your defined job responsibilities.
- When sharing personal health information
  - Personal health information may only be shared from one ONE Mail account to another. An approved secure file transfer solution must be used when sharing information outside of ONE Mail.
  - Password should be communicated in a secure manner (i.e. directly to the individual or via telephone).
  - Ensure only the intended recipients are provided the message and password.
- Keep personal health information confidential, even after the service contract or employment has ended, by observing key security safeguards identified in the training.
- All access is logged and monitored - do not disable these capabilities or overwrite, modify, erase or deactivate logs.
- Talk to your Privacy Officer or Security Officer if you have questions.

Consent Management/Access and Correction/ Privacy Audit Support (1/2)

What is my role when accessing eHealth Ontario systems and services?

You have access to eHealth Ontario systems and services to provide operational support such as responding to requests from patients or participating organizations that may involve access to personal information or personal health information.

Consent Management, Access and Correction and Privacy Audit Support (2/2)

What is expected of me when accessing Personal Health Information?

- Only access personal health information that is needed to perform your role.
  - Be able to map each access to personal health information to a ticket or for a specific purpose. **Accessing your own records or those of your family members, friends or colleagues, etc. is not permitted in eHealth Ontario systems and services.**
- Securely store and delete personal health information
  - Personal health information must be stored in a secure location. Access to this location must be limited to required personnel. Personal health information must not be stored in SharePoint.
  - When logging issues or requests, do not store personal health information in the tracking system or your request.
- When exporting personal health information, have documented approval from your manager or ensure it is part of your defined job responsibilities.
- When sharing personal health information
  - Personal health information may only be shared from one ONE Mail account to another. An approved secure file transfer solution must be used when sharing information outside of ONE Mail.
  - Password should be communicated in a secure manner (i.e. directly to the individual or via telephone).
  - Ensure only the intended recipients are provided the message and password.
- Keep personal health information confidential, even after the service contract or employment has ended, by observing key security safeguards identified in the training.
- Retain and dispose of personal health information and related records (such as logs) as directed by the Electronic Health Record Retention Policy for ConnectingOntario and Diagnostic Imaging Common Services and the eHealth Ontario Personal Health Information Policy for Ontario Laboratory Information System.
- All access is logged and monitored - do not disable these capabilities or overwrite, modify, erase or deactivate logs.
- Talk to your Privacy Officer or Security Officer if you have questions.

How long is data stored for?

Retention of personal health information, audit logs and reports and system-level logs vary for eHealth Ontario systems:

Information type	eHealth Ontario System	Retention Period
Personal Health Information, including audit logs/reports that contain PHI, archival copies	ConnectingOntario, Diagnostic Imaging Common Services, FMBL,	Audit logs/reports for compliance purposes: 30 years Audit logs/reports for troubleshooting and operations: as long as needed but no longer than 60 days unless expressly authorized
	MOHLTC Assets: Ontario Laboratories Information System, Digital Health Drug Repository	Indefinitely
	Hosting Services	In accordance with the Client's existing retention policy
System-level Logs	All assets	Minimum of 2 years
Authentication Log s		60 days online, 2 years in archive

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 :
  - 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 accessed for unauthorized purposes; or
- Records of personal health information have been 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.

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:

- **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.

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.

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 Health Information as Authorized or Required to Perform your Role

Do:

- Access personal health information as authorized or required to perform your role in providing technical or operational services.

Don't:

- Troll for patients or perform wild card searches in Connecting Ontario.
- Allow "shoulder surfing"- allowing an unauthorized person to look over your shoulder when entering/accessing sensitive information.
- Discuss or access personal health information in public places where others may hear or see the information.
- Take a picture of data displayed on Ontario's Electronic Health Record.
- View blocked personal health information, in the event you have the ability to do so.

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.
- Securely encrypt and password protect personal health information emailed to eHealth Ontario.

Don't:

- Share personal health 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:

- Always change an initial or temporary password provided to you on first use.
- Create a strong and hard-to-guess password by following conventional guidelines and keep your password a secret.
- Commit your password to memory. Do not record it or store it in a file unless it can be secured.
- Change your password if you suspect it may have been compromised and notify your Privacy Officer, Security Officer or eHealth Ontario as applicable.

Don't:

- Leave your workstation logged into Ontario's Electronic Health Record and unattended.
- 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.
  - 2-factor authentication may be required when working remotely. Follow proper procedures to disconnect from a remote access connection (e.g., use disconnect option rather than simply closing the application).
- 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:

- 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, 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:

- 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

Physical Safeguards:

- 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

Technical Safeguards:

- 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