eHealth Ontario

Health Care Provider Guide

The Electronic Health Record (EHR)

Version 2.0

Ontario

Contents

General Information

Purpose and Scope

This guide describes the functions and associated benefits provided by the Electronic Health Record (EHR) and the related privacy, security and legal considerations, roles and responsibilities which health care providers and organizations using the EHR and its underlying data repositories must adhere to.

Audience

This document is intended for health care providers across Ontario's health care sector that may be an organization or a person, who has signed or will sign the appropriate eHealth Ontario access agreement(s) and use the EHR to access the clinical data information related to their patients.

Related Documents

This guide should be read in conjunction with the following information found at www.eHealthOntario.on.ca:

- eHealth Ontario Privacy and Data Protection Policy and sub-policies
- EHR Access and Correction Policy
- EHR Assurance Policy
- EHR Consent Management Policy
- EHR Inquiries and Complaints Policy
- EHR Logging and Auditing Policy
- EHR Privacy Breach Management Policy
- EHR Retention Policy
- EHR Security Policies and Standards
- Information Security Policy
    - Acceptable Use of Information and Information Technology Standard
    - Access Control and Identity Management Standard for System Level Access
    - Business Continuity Standard

- Cryptography Standard
- Electronic Service Provider Standard
- Information Security Incident Management Standard
- Information and Asset Management Standard
- Local Registration Authority Practices Standard
- Security Logging and Monitoring Standard
- Network and Operations Standard
- Physical Security Standard
- System Development Lifecycle Standard
- Threat Risk Management Standard
- eHealth Ontario Federation Identity Provider Policy and Standard

The Electronic Health Record

Overview

An electronic health record (EHR) is a secure lifetime record of Ontarians' health history. It gives health care teams, including family doctors, nurses, emergency room clinicians and specialists, real-time access to relevant medical information, so you can provide the best care for your patients / clients. eHealth Ontario has built the provincial system that gives health care providers at hospitals, family practices, long-term care homes, pharmacies and more access to patients' EHRs so they can quickly look up lab results, publicly funded dispensed medications, digital images (like x-rays and MRIs), hospital discharge summaries and more.

There are various channels to view the data in the EHR, which may vary per region. For details of the viewing channels, please see Appendix F.

Personal health information (PHI) from primary, acute and community care that may be available in a patient's electronic health record includes:

- Allergy information
- Cardiovascular reports
- Diagnostic imaging reports (e.g., x-rays)
- Emergency department visits
- Home care and long-term care information
- Hospital discharge summaries and reports
- Infection control information
- Lab reports
- Medical history
- Drug and Pharmacy Service Information
- Mental health and addictions information
- Neurophysiology reports
- Patient consultation reports
- Patient demographics

- Respiratory reports
- Visit or encounter details

More information on the various data repositories that hold this information and the various ways to view the information is available in the appendices.

Prerequisite

Technical Prerequisites

- ONE ID credential or federated access to login using a clinical information system
- Minimum browser and system configuration requirements

Non-Technical Prerequisites

- Must be a health care information custodian (HIC) or authorized to view through a HIC
- Sign legal agreements
- Meet privacy and security requirements

Responsibilities

eHealth Ontario Responsibilities

eHealth Ontario shall comply with the following obligations:

- Provide EHR data and viewing functionalities as described in this document, for registered health care providers 24/7
- Restrict access to any record contained within the data repositories that has been restricted by one or more consent directives issued by the patient
- Temporarily grant access to a patient's health information contained within the data repositories that is restricted by consent directives when the health care provider overrides the consent directive with the patient's or his/her substitute decision maker's (SDM) approval, or in the circumstances where providing care is required to reduce the risk of bodily harm to the patient or other persons (if permitted)
- Provide support for privacy-related questions or concerns about the data viewed in the EHR
- Update the EHR data repositories to expand and enhance the functionalities and data sources provided

- Conduct privacy and security assessments to ensure that the collection, storage, use and disclosure of personal information/personal health information (PI/PHI) complies with legislative and privacy protection requirements
- Provide support and expertise in identifying and recommending to health care providers their security obligations and requirements. Health care providers are supplied with requirements based on the number of users, access methods, and the scope of integration to the EHR
- Assist providers in meeting their legislative obligation for responding to a patient's access and correction requests

Health Care Provider Responsibilities

- They must contact their Account Management liaison to determine whether they need to do the security assessment or whether meeting the security requirements listed below is sufficient.

Data Contributor Responsibilities

Health care providers that contribute data to the EHR shall comply with the following obligations:

- Follow the supporting EHR security policies and EHR privacy policies when contributing to the EHR. See Related Documents for a complete listing of policies
- Agree to complete and adhere to the requirements of the EHR Security Assessment for Federated or Data Contribution Organizations

Identity Provider Responsibilities

Identity Providers are organizations that leverage technology and related supporting services, policies, processes, and procedures that are used to create, maintain, secure, validate, assert and manage electronic identities to the Electronic Health Record. Those who provide the identity management service for an organization shall comply with the following obligations:

- Follow the requirements of the eHealth Ontario Identity Provider Policy and Standard
- Follow the supporting EHR Security Policies and Standards when providing an identity management service. See Related Documents for a complete listing.
- Agree to complete and adhere to the requirements of the EHR Security Assessment for Federated or Data Contribution Organizations.

EHR Privacy Data Viewer Responsibilities

Health care providers who view the EHR data and/or their Privacy Office (if applicable) must comply with the obligations set out in the relevant eHealth Ontario access agreement signed with eHealth Ontario by their organization or by themselves and:

- Agree to follow the Electronic Health Record Privacy Policies available and listed in the Related Documents section to protect privacy and security when using eHealth Ontario products as well as implement and assist users to follow EHR privacy and security policies, where applicable
- Use the EHR only for approved clinical purposes
- Always indicate the person and the organization that the user represents when accessing patients' health information within the EHR
- Obtain the patient's or the SDM's name, relationship to the patient and their consent prior to requesting temporary override of patient's consent directives to access health information
- Report and assist with privacy breach and security incident (actual or suspected) investigations
- Complete annual privacy and security end user training (as applicable)
- Respond or direct patients to appropriate area/group for privacy-related questions, concerns, or requests (i.e. access requests, correction requests and consent directive requests)
- Audit and monitor user activity in the EHR and report on compliance

EHR Security Data Viewer Responsibilities

The following are the minimum EHR Security Policy and Standards requirements for the EHR solution. All health care providers participating in the EHR must be 100% compliant.

Information Security

- Health care providers must develop, implement and maintain information security policy standards and/or procedures for their organization that uphold the principles of the EHR Security Policy and Standards.

Acceptable Use of Information and Information Technology

- A password must have the following characteristics:
    - Contain a minimum of eight characters and include a combination of upper and lower case letters, numbers and/or special characters (e.g. !, $, #, _, ~, %, ^)
    - Must not be obvious, easily guessable, or found in a common words dictionary
    - Must not use acronyms, birthdays, sequential numbers, names of family members, birthdays, anniversaries or pets
    - Never include three consecutive characters (e.g. "AAA")

- Password must never be disclosed to anyone or written down.
- Change user passwords frequently, at least every 90 days.
- On suspicion or confirmation that a user's password has been disclosed or compromised, that user must immediately change their password and notify their internal point of contact identified in the security incident management process.

Managing devices and procedures used to participate in the EHR Solution

- Use only systems/devices and processes approved for clinical practice by the health care provider (no unapproved personal devices) , either locally or from a remote location (e.g., practice-related workstations or remote access tools with controls for disk encryption, passwords and antivirus)
- All persons must ensure that if PHI resides on a mobile device (e.g., phones, laptops, tablets) used to access the EHR solution and that device is taken offsite, it must be encrypted, or the device itself must utilize full disk encryption.
- The health care provider must encrypt the contents of sensitive emails or use approved, secure file transfer solutions such as ONE Mail®, that apply encryption of email in transit to other ONE Mail users.

Electronic Service Providers (ESPs)

- The health care provider must maintain documentation related to support contracts, agreements, and response times for all providers of electronic services who support their organization's participation in the EHR
- The health care provider must assess the potential risks posed by all new ESPs prior to entering into a contract, and identify methods for mitigating any identified risks.

Information Security Incident Management

- The health care provider must establish an internal point of contact (e.g., service desk, office manager, office administrator) to whom actual or suspected incidents are reported to and investigated.
- Ensure that all users, their agents and ESPs are aware of their responsibility to immediately report actual or suspected security incidents.
    - Users must immediately notify their organization help desk or security officer if they suspect or know that any credentials have been or may be breached or compromised. Organization help desk or system administrator must notify eHealth Ontario.

- eHealth Ontario may, in its sole discretion, suspend or revoke a user's access to eHealth Ontario's products, services, or technology infrastructure should such user breach any security policies required as part of the Data Viewer Requirements.
- Health care providers must cooperate with eHealth Ontario on the management of breaches of policy (Information Security Incident Management). This responsibility includes, but is not limited to, assisting with the development and distribution of communications regarding management of breaches or incidents.

Network and Operations

- The health care provider must implement and manage network controls in a way that separates and protects internal computers (your network) from the Internet (perimeter).
- For example, if your organization provides "guest" WIFI Internet access to patients, ensure this "guest" network is separate from the health care provider internal network, thus preventing unauthorized individuals from accessing the health care provider's network.

Malware

- The health care provider must ensure implementation of malware detection on all systems/devices used by the health care provider to participate in the EHR solution.
- The health care provider must ensure their malware detection and patches are up-to-date as per the System Incident Management Process.

Physical Security

- The health care provider must ensure that workspaces are protected against unauthorized physical access. Methods for preventing physical access may include, but are not limited to:
  - Segmenting public and office work spaces
  - Using locked cabinets to store equipment and sensitive information
  - Fitting vulnerable doors and windows with locks or bolts
  - Installing and monitoring closed-circuit television (CCTV)
  - Installing intruder detection systems on external doors and testing accessible windows regularly
  - The health care provider must ensure they have procedures to address the destruction of information in line with the guidance from the Information and Privacy Commissioner of Ontario (IPC).

Identity Validation and Enrollment Management

- The Legally Responsible Person (LRP) (or delegate) is responsible for:
    - Being aware and providing oversite for the registration and enrollment practices.
    - Ensuring a Sponsor and LRA is defined for authorizing individual access. The LRP can be designated as the Sponsor or LRA. The LRA is responsible for:
        - Validating the identity of any of the health care provider's agents who will have access to EHR information on the health care provider's behalf, using a combination of documentary and contextual evidence, including the review of at least one piece of government-issued photo ID.
        - Ensuring that all registrants are 16 years of age or older.
        - Maintaining identity records in alignment with known facts, e.g. making updates to correct errors or revoking duplicate accounts.
    - Participating Organization must ensure that any credentials used by the user to directly or indirectly gain access to the products, services or technology infrastructure are safeguarded.
    - Accounts are reviewed on an annual basis to ensure appropriate and up to date access.

Privacy and Security Considerations

Communicating Sensitive Files

Unencrypted PI and PHI must not be emailed to eHealth Ontario. EHR Policies require that adequate safeguards be applied every time a sensitive document or file is stored or transferred through communication channels that are not considered safe and secure (e.g., regular internet email, CDs, DVDs, USB sticks and/or flash memory cards). For further information, please refer to Appendix G.

Patient Consent

Consent Management

The EHR gives patients or their SDMs the option to allow or restrict access to patient data when viewed. If a patient restricts access to his/her data, by applying a consent directive, providers querying the EHR will be unable to access the information to which a consent directive has been applied unless the provider performs a temporary override of access.

Consent directives can be made, modified or removed to restrict or allow the following in the EHR:

- Global: Restricting access to all PHI in all clinical domains and all EHR systems (except demographic data available in the Client Registry and the Consent Registry)
- Domain: Restricting access to all PHI in an Ontario Laboratory Information System[1] (OLIS)
- HIC-Records: Restricting or allowing access to all PHI on a specific patient originating from a specific health information custodian (HIC)
- Record- Level: Restricting or allowing access to a particular record of personal health information
- HIC-Agents: Restricting or allowing all agents of a specific participating HIC from accessing the patient's PHI in the EHR

[1] For OLIS, this may also be referred to as a patient-level restriction.

- Agent: Restricting or allowing a specific agent of a HIC (individual person) from accessing to the patient's PHI in the EHR

Note: At this time, consent directive granularity that is supported varies for the EHR element. Refer to the table below for more information.

Applying Consent Directives

If a patient contacts a HIC and wishes to either place a restriction on access to his / her information, or wishes to reinstate access (revoke the restriction), the HIC should complete the EHR Health Information Custodian Consent Directive Request Form

eHealth Ontario will send the HIC a confirmation that the request has been fulfilled. The HIC should then provide notice to the patient that the consent directive has been successfully applied.

In instances where a patient requests to place a consent directive on or reinstate access to records contributed by more than one HIC, the patient should complete the Patient Consent Directive Request Form or contact eHealth Ontario directly at 1-866-250-1554.

The consent directives will be applied within 7 days[2] of verifying the identity of the patient (and SDM, if applicable) making the request. The party who received the request for the consent directive then notifies the patient that his/her request has been fulfilled. If the patient cannot be notified, eHealth Ontario will notify him/her on behalf of the HIC upon direction.

Note: As indicated on the forms, the patient (or SDM) must call ServiceOntario INFOline toll-free at 1-800-291-1405 (TTY 1-800-387-5559) for information in the Digital Health Drug Repository (DHDR) and Ontario Laboratories Information System (OLIS).

Overriding a Consent Directive

The EHR permits providers to temporarily access a patient's restricted information by overriding a patient's consent directive under the following circumstances (note that not all circumstances are available for OLIS and DHDR):

- With the express consent from the patient or the patient's SDM;

---

[2] For OLIS, patient-level consent directives will be applied within 2 days

- If the provider believes, on reasonable grounds, that the override is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm to the patient to whom the PHI relates and where it is not reasonably possible to obtain the consent of the patient in a timely manner; or
- If the provider believes on reasonable grounds that the override is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm to a person other than the patient to whom the PHI relates or to a group of persons.

The reason for the override and the availability of the temporary access to information may vary depending on the EHR element. The table below (Table 1) outlines the variation in the placing of consent directives and provider consent overrides based on the different repositories and viewing methods.

EHR Element	Reasons for a Temporary Override	Level of Consent Supported	Contact to Place Consent Directive
acCDR	Express Consent[3] Significant harm to the individual Significant harm to another individual ***Note:*** *not available in the ClinicalConnect Clinical Viewer*	Agent HIC-Agent HIC-Record Global Domain	eHealth Ontario Participating Organization Privacy Officers
OLIS[4]	Express Consent ***Note:*** *not available in the ClinicalConnect Clinical Viewer*	Domain Record Note: record-level consent directives are to be specified at the time the test is conducted	Service Ontario

[3] Express consent may only be received from the patient or the patient's substitute decision maker.
[4] Refer to appendix for a description of who may see OLIS data subject to a consent directive.

EHR Element	Reasons for a Temporary Override	Level of Consent Supported	Contact to Place Consent Directive
Diagnostic Imaging-Common Services (DI-CS)	Express Consent ***Note:*** *not available in the ClinicalConnect Clinical Viewer or ConnectingOntario ClinicalViewer*	Domain HIC-Agents HIC-Record Record	eHealth Ontario Participating Organization Privacy Officers
DHDR	**Express Consent**	**Domain**	**Service Ontario**

Table 1: Consent Directives and Overrides

An override in the ConnectingOntario ClinicalViewer will result in all portlets with a consent directive to be unmasked. Although the DHDR data (in the Dispensed Medications tab in the ClinicalViewer) may not be required to provide care, an override in another portlet will also release this data and the express consent form must be completed in addition to the Consent Override Dialogue box. Therefore, before performing an override on any portlet in the ClinicalViewer:

1. Confirm if a block is placed on the Dispensed Medications tab. If it is blocked, print a hard-copy express consent form[5].
2. Inform the patient of why you are overriding their consent.
3. If the patient agrees to the override and the Dispensed Medications tab is blocked, obtain consent and document the receipt of consent by requesting a wet signature from the patient or substitute decision maker on the express consent form and complete the Consent Directive Dialogue Box.
4. Inform the patient for how long the unblocked information will be available.

An override in the ClinicalConnect viewer may not be performed for acCDR, DI-CS or OLIS data.

An override performed for the purpose of eliminating or reducing a significant risk of serious bodily harm on OLIS, DI CS and DHDR will not override the consent block.

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

A temporary consent override will be logged in the EHR interface, along with the identity of the overriding health care provider and an explanation as to what kind of consent was obtained. An audit of this information can be requested by the patient or your organization. Refer to the table above (Table 1) for the duration in which the override will be in effect for each EHR element. Once the duration maximum has been met, the access will once again be blocked.

eHealth Ontario will notify the HIC's Privacy Officer if one of the HIC's agents overrides a consent directive[6]. Once contacted by eHealth Ontario, it is the responsibility of the HIC's Privacy Officer to:

1. Investigate the override to ensure it was for one of the permitted reasons stated above, and
2. Notify the patient of the override at the first opportunity[7].

If a consent directive override is applied for the purpose of eliminating or reducing a significant risk of serious bodily harm to a person other than the patient to whom the PHI relates or to a group of persons, the HIC should provide a written notice to the Information and Privacy Commissioner of Ontario (IPC) as soon as possible indicating that this type of override has occurred. For more information on what to include in this notice to the IPC, please see the EHR Consent Management Policy.

Note: eHealth Ontario will notify the Privacy Officer identified on the Client Information Form (CIF) of a consent directive override.

Access Requests

Access Requests Made by Patients

Under the Personal Health Information Protection Act (PHIPA), patients or their SDM have a right to access data held by a HIC about the patient. When a provider receives a request for records collected, created and contributed by the provider to the EHR and its repositories, the provider must follow Part V of PHIPA as well as all any related internal policies, procedures and practices to respond directly to the patient.

In instances where requests for access involves information contributed by another HIC or by multiple HICs, the provider is required to:

---

[6] An override notification will not be provided to the Privacy Officer for OLIS. Override notifications are provided directly to the patient.

[7] For more information on what to include in this notice to the patient, please see the *EHR Consent Management Policy*. If you cannot notify the patient, contact eHealth Ontario, and eHealth Ontario will notify the patient on your behalf. Note that for DHDR and OLIS, MOHLTC will provide a notice to the patient directly.

- Notify the patient that the request for access involves PHI not within the custody or control of the HIC that received the request for access, and
- Direct the patient to contact eHealth Ontario at 1-866-250-1554 or complete the EHR Access and Correction Request Form.

As per the EHR Access and Correction Policy, eHealth Ontario will inform the HIC of a request for access and may seek assistance from the HIC when responding directly to a request for access.

Note: As indicated on the forms, the patient (or SDM) must call ServiceOntario INFOline toll-free at 1-800-291-1405 (TTY 1-800-387-5559) for requests for DHDR and Access and Privacy Office, Ministry of Health and Long-Term Care at Care at 416-327-7040 or generalapo@ontario.ca for OLIS.

Requests for Audit Logs

There are three types of access requests that a patient or their SDM can make with respect to their EHR:

1. List of providers who viewed the patient's PHI
2. History of instruction to block or allow access
3. History of temporary access to blocked PHI

When a provider receives a request for access directly from a patient related to audit logs for records stored in the EHR, the HIC is required to follow Part V of PHIPA as well as all/any related internal policies, procedures and practices to respond directly to the patient. Where the HIC is unable to generate and provide copies of records in response to the request for access:

- Notify the patient that the HIC is unable to process the request for access, and
- Direct the patient to contact eHealth Ontario at 1-866-250-1554 or complete the EHR Access and Correction Request Form.

All access requests and audit log requests should come from the privacy office at your organization. If you do not have a privacy office, you may contact eHealth Ontario directly.

Note: As indicated on the forms, the patient (or SDM) must call ServiceOntario INFOline toll-free at 1-800-291-1405 (TTY 1-800-387-5559) for requests for DHDR and for history of instruction to block or allow access and history of temporary access to blocked PHI for OLIS, contact the Access and Privacy Office, Ministry of Health and Long-Term Care at Care at 416-327-7040 or generalapo@ontario.ca for a list of providers who have viewed PHI OLIS.

Correction Requests

When a HIC receives a request for correction directly from a patient related to health records that were created and contributed to the EHR solely by that HIC, the HIC is required to follow Part V of PHIPA and its internal policies, procedures and practices to respond directly to the patient in respect of the request for correction.

- At the request of the patient, when a correction request is fulfilled, the HIC must notify eHealth Ontario of the correction and request an audit report of who has accessed the patient's record, in the event that the patient would like to inform other HICs who may have accessed their record. The HIC must then notify relevant sites that have viewed the patient's record of the correction.

Where a HIC receives a request for correction directly from a patient related to records that were created and contributed to the EHR by another HIC or more than one HIC, the HIC must respond no later than two business days after receiving the request for correction by:

- Notifying the patient that the request for correction involves PHI not within their custody or control, and
- Directing the patient to contact eHealth Ontario at 1-866-250-15541554 or complete the EHR Access and Correction Request Form

eHealth Ontario will forward the request to the HICs that created and contributed the PHI. The HIC is required to follow Part V of PHIPA and its internal policies, procedures and practices to respond directly to the patient in respect of the request for correction.

Note: Where the HIC is unable to make the correction, the HIC must instruct eHealth Ontario as soon as possible to make the correction or append the statement of disagreement in accordance with Part V of PHIPA.

Privacy Complaints and Inquiries

When a HIC directly receives an inquiry/complaint related solely to that HIC's records in the EHR, or related to the HIC and its agents and service providers, the HIC is required to follow its own internal policies, procedures, and practices to address the inquiry/complaint.

When a HIC directly receives an inquiry/complaint related solely to the EHR or to eHealth Ontario's agents or electronic service providers that it is unable to address, the HIC must:

- Notify the person that the HIC is unable to respond to the inquiry/complaint, and
- Direct the patient to contact eHealth Ontario at 1-866-250-1554 or complete the EHR Inquiries and Complaints Form

eHealth Ontario may seek assistance from the HIC(s) when responding directly to inquiries or complaints received by eHealth Ontario.

Note: As indicated on the forms, the patient (or SDM) must call ServiceOntario INFOline toll-free at 1-800-291-1405 (TTY 1-800-387-5559) for inquiries or complaints relating to DHDR and the Access and Privacy Office, Ministry of Health and Long-Term Care at Care at 416-327-7040 or generalapo@ontario.ca for inquiries or complaints relating to OLIS.

Retention

PHIPA requires HICs to ensure that its records are retained for a specified period, and transferred and disposed of in a secure manner. HICs must ensure records are protected and disposed of in accordance with the EHR Information and Asset Management Standard.

HICs will retain records containing the following information for the corresponding retention period:

Information Type	Retention Period
Audit logs and audit reports that contain PHI created and maintained for compliance purposes	The longer of 30 years or when PHI is removed from the EHR.
Information collected to respond to patients related to their: • Request for Access or Request for Correction under PHIPA; • Request to make, modify, or withdraw a Consent Directive under PHIPA; or • Inquiries or Complaints under PHIPA.	Two years after the request was made. For complaints, retain for two years after the complaint has been closed by the HIC, eHealth Ontario, or the IPC, whichever is longer.
Information created about a patient as part of an investigation of Privacy Breaches and/or Security Incidents.	Two years after the Privacy Breach has been closed by the HIC, eHealth Ontario or the Information and Privacy Commissioner of Ontario, whichever is longer.
Information used for identity provider registration that contains PI	Seven years after last use

Information Type	Retention Period
End User Credential Information where HIC is an Identity Provider	Permanent
System-level logs, tracking logs, reports and related documents for privacy and security tasks that do not contain PHI	For a minimum of two years
Authentication Events where HIC is an Identity Provider	60 days online, 24 months total in archive
Assurance-related documents	10 years

Table 2: Record Retention Periods

The specific records that are included in each of the information types can be found in Appendix A of the EHR Retention Policy.

Privacy and Security Training

HICs are required to provide privacy and security training to their Health Care providers prior to their access to the EHR[8]. The training should ensure that Health care providers are aware of their duties under applicable privacy legislation, such as PHIPA, as well as relevant privacy and security policies and procedures in respect of the EHR by including the content outlined in the EHR Privacy and Security Training Policy. eHealth Ontario has developed the role-based training materials to facilitate the delivery of training which can be found in the EHR Privacy Toolkit and the EHR Security Toolkit. Privacy and Security Training should be completed prior to being provisioned an account for accessing the EHR. All end users must receive the applicable privacy training before accessing the system.

[8] Privacy and security training applies only to ConnectingOntario CDR, and DHDR at this time.

HICs are required to track which of their agents, electronic service providers, and any end users have received privacy and security training. After initial training has taken place, training must be provisioned on an annual basis.

Privacy-Related Questions from Health Care Provider Sites

If a health care provider has any questions regarding the privacy-related processes described above, including how to respond to patient access requests, consent obligations or incident/breach management processes, contact your site Privacy Officer as a first point of contact. As a secondary point of contact, the eHealth Ontario Privacy Office can be reached at 1-866-250-1554.

Please ensure that you do not include any PH or PHI in any emails sent to eHealth Ontario.

Requests for Privacy Audit Reports

As a HIC, you may require an audit report with respect to the EHR to meet your auditing requirements. In the event that you are unable to fulfil this requirement using your own internal system logs, you may request an audit report from eHealth Ontario. Some examples of the types of audit reports that eHealth Ontario is able to provide are listed below:

Report Type	Description
Monthly End User Audit	One month of names of patients whose records were retrieved by all users of HIC
Quarterly End User Audit	Four consecutive months of names of patients whose records were retrieved by all users of HIC
Access to PHI Report by User	Names of patients whose records were retrieved by specific user of HIC

Table 3: Types of Audit Reports

- By organization request: eHealth Ontario will provide you with a report of all users in your organization who have accessed the EHR data in the timeframe set out in the request.

- By user request: eHealth Ontario will provide you with a report of all accesses to the EHR data by a particular user from your organization in the timeframe set out in the request.
- Access to PHI by patient request: Health Ontario will provide you with a report of all accesses to a particular patient's EHR data from all users in your organization in the timeframe set out in the request.
- Consent directive override report by organization: eHealth Ontario will provide you with a list of all consent directives overrides that have been performed by all users in your organization in the timeframe set out in the request.
- Consent directive history report by organization: eHealth Ontario will provide you with a list of all consent directive changes requested from your organization in the timeframe set out in the request.

Note: audit report requests should come from the privacy office at your organization. If you do not have a privacy office, you may contact eHealth Ontario directly.

To make a request for an audit report, contact the eHealth Ontario Service Desk at 1-866-250-1554 and specify the EHR element you are requesting an audit report for.

Privacy Incident and Breach Management

A privacy incident is:

- A contravention of the privacy policies, procedures or practices implemented by your organization or any applicable policies of eHealth Ontario, where this contravention does not constitute non-compliance with applicable privacy law.
- A contravention of any agreements entered into between eHealth Ontario and your organization, where the contravention does not constitute non-compliance with applicable privacy law.
- A suspected privacy breach.

A privacy breach is:

- The collection, use or disclosure of PI or PHI that is in contravention of applicable privacy law; and/or
- Any other circumstances where there is an unauthorized or inappropriate collection, use or disclosure, copying, modification, retention or disposal of PI or PHI including theft and accidental loss of data.

The privacy and security incident and breach management process does not apply to the handling of internal HIC incidents or to any HIC, their agents or their electronic service providers who do not view or contribute PHI to the EHR.

In instances where a breach is caused by a HIC who solely created and contributed the data to the EHR, the HIC shall follow its internal policies, procedures, and practices to notify the patient(s) to whom the PHI relates at the first reasonable opportunity in accordance with PHIPA and to contain, investigate and remediate the privacy breach. Once the HIC has determined that a Privacy breach has occurred, the HIC shall report the privacy breach to eHealth Ontario.

Instructions for Health Care Providers

If you become aware of, or suspect, a privacy or security incident or breach of EHR data by you or any of your employees, agents, or service providers, you must immediately report the incident or breach to your privacy / security office. If you do not have a privacy /security office, or you are unable to reach your privacy / security office or support team to report a breach, please contact the 24/7 eHealth Ontario Service Desk at 1-866-250-1554 and advise the eHealth Ontario agent that you would like to open a privacy / security incident ticket.

If you become aware of, or suspect, a privacy or security incident or breach of EHR data by you or any of your employees, agents, or service providers, you must immediately report the incident or breach to your privacy / security office. If you do not have a privacy /security office, or you are unable to reach your privacy / security office or support team to report a breach, please contact the 24/7 eHealth Ontario Service Desk at 1-866-250-1554 and advise the eHealth Ontario agent that you would like to open a privacy / security incident ticket.

It is extremely important that you do not disclose any patient PI and/or PHI to the eHealth Ontario Service Desk when initially reporting a privacy or security incident or breach.

It is expected that you will cooperate with any investigations conducted by eHealth Ontario in respect of any privacy or security incidents or breaches in relation to EHR data. During an investigation by eHealth Ontario you may be required to provide additional information which may include PI or PHI, in order to contain or resolve the incident or breach. Any PI or PHI that is requested by eHealth Ontario should be sent as an encrypted document via email following the Procedures for Communicating Sensitive Files via email. See Appendix G for details.

Instructions for Privacy Officers

If you become aware of, or suspect, an incident or breach related to EHR data by any of your organization's staff members, including employees, agents or service providers, you must immediately[9] report the incident or breach

[9] For ConnectingOntario CDR and DI CS, the breach must be reported as soon as possible, but in any event no later than the end of the next business day once the HIC has determined that a Privacy Breach has occurred or has reasonable suspicion that a Privacy Breach has occurred.

to eHealth Ontario's Service Desk 1-866-250-1554 and advise the Service Desk that you would like to open a breach/ incident ticket.

The EHR Privacy Breach Management Policy describes detailed steps to be taken in the event of a privacy incident or breach[10].

In instances where a breach was solely caused by a HIC that did not solely create and contribute the PHI to the EHR, the HIC, in consultation with other HICs (who contributed data) and eHealth Ontario, shall identify the individual to investigate the breach. The specific roles for each party involved in the privacy breach are noted in the EHR Privacy Breach Management Policy.

Security Incident Management

The EHR Information Security Management Policy describes detailed steps to be taken in the event of a security breach/incident.

A security incident is any violation or imminent threat of violation of information security policies, standards, procedures or practices or any information security event that may compromise operations or threaten the security of an information system or business process.

If you become aware of, or suspect, a security incident or breach of the EHR or data by you or any of your employees, agents, or service providers, you must immediately report the incident or breach to your Security Office. If you do not have a Security Office, or you are unable to reach your Security Office or support team to report a breach, please contact the eHealth Ontario service desk at 1-866-250-1554 and advise the service desk that you would like to open a security incident ticket.

Incidents must be reported to eHealth Ontario no later than the end of the next business day when a HIC becomes aware of an actual or suspected security incident caused or contributed by:

- Another HIC or the agents or electronic service providers of another HIC,
- More than one HIC or the agents or electronic service providers of more than one HIC,
- eHealth Ontario or its agents or electronic service providers, or
- Any other unauthorized persons who are not agents or electronic service providers of eHealth Ontario or any other HIC.

[10] OLIS and DHDR may not follow the steps outlined in the EHR Privacy Policies.

You are expected to cooperate in any incident or breach containment activities or with any investigation undertaken by eHealth Ontario. During the investigation by eHealth Ontario, you may be required to provide additional information which may include PI or PHI, in order to contain or resolve the incident or breach.

Important: It is extremely important that you do not disclose any patient PI and/or PHI to the service desk when initially reporting a security incident or breach. It is expected that you will cooperate with any investigations conducted by eHealth Ontario in respect of any security incidents or breaches related to data.

When reporting a confirmed or suspected security incident or breach, please have the following information ready:

- The time and date of the reported incident
- The name and contact information of the agent or electronic service provider that reported the incident
- Details about the reported incident, (e.g., type and how it was detected)
- Any impacts of the reported incident, and
- Any actions undertaken to contain the incident either by the agent or electronic service provider that reported the incident or the point of contact.

Once a call has been logged with the service desk, the eHealth Ontario security team will be engaged. Your organization may be required to lead the incident remediation efforts.

Instructions for Security Officers

If you become aware of, or suspect, an incident or breach related to EHR data by any of your organization's staff members, including employees, agents or service providers, you must immediately[11] report the incident or breach to eHealth Ontario's Service Desk 1-866-250-1554 and advise the Service Desk that you would like to open a breach/ incident ticket.

[11] For ConnectingOntario CDR and DI CS, the breach must be reported as soon as possible, but in any event no later than the end of the next business day once the HIC has determined that a Privacy Breach has occurred or has reasonable suspicion that a Privacy Breach has occurred.

Appendix A: Clinical Data Repository (CDR)

Overview

The CDR is an eHealth Ontario data repository that allows authorized hospital- and community-based health care providers to view clinical information originating from acute-care and primary-care sites that are contributing to the repository. CDR data can include clinical reports such as Home and Community Care Service reports, discharge summaries, emergency department reports, visits, encounters, as well as elements of the Cumulative Patient Profile (CPP) held within an Electronic Medical Record (EMR). The CDR gives authorized providers important information to make informed decisions about treating their patients.

With the support of information technology, the CDR identifies, collects and stores priority data from existing databases and registries, i.e. Hospital Information Systems (HISs) and Electronic Medical Records (EMRs).

Benefits

Benefits to You

- Enhanced care and experience
    - Reduce redundancy and frustration
    - Help improve interactions with point-of-care access to information
    - Improve transition between health care providers
    - Improved productivity and satisfaction
- Improve efficiency of decision-making and the ability to monitor health outcomes
    - Provide electronic access to integrated health care information
    - Help improve inter-professional care and coordination of services
    - Improved organizational and system coordination and capacity
- Accelerate the development and delivery of electronic health records
    - Provide significant cost-savings, enabling an integrated and sustainable approach to manage, coordinate and plan care
    - Build foundational information technology (IT) elements that can be leveraged for other organizational, regional and provincial health initiatives

Benefits to Your Patients

- Patients receive enhanced, timelier and more coordinated care

Appendix B: Ontario Laboratory Information System (OLIS)

Overview

OLIS is a province-wide repository of lab information that can be accessed via clinical viewers. OLIS accepts data feeds from labs in the province such as public health Ontario laboratories, community and hospital laboratories. The goal is to have 100%of all lab tests performed in Ontario in OLIS. For the most up-to-date list of current data providers and the latest about OLIS, visit: www.ehealthontario.on.ca/initiatives/view/olis.

Benefits

Benefits to You

- Enables timely and secure access to information for decision making at point-of-care
- Facilitates more comprehensive and broader laboratory test information as produced by laboratories outside of your organization
- Provides an effective tool to integrate and track patient laboratory history over time, monitor progress of treatments and support chronic disease management
- Provides enhanced coordination of care between multiple practitioners and within health care teams
- Improves workflow and reduces dependency on paper-based systems

Benefits to Your Patients

- Ensures fewer gaps in patient information as patients move between hospital, practitioner's office (e.g. family physicians, specialists), home care and long-term settings
- Reduces duplicate and unnecessary tests or exams due to greater availability and sharing of information
- Improved decision making within circle of care leading to improved outcomes

Patient Query Search: Step by Step

The new OLIS functionality may differ in look and feel from one clinical viewer to the next. Your organization will provide you with training specific to your system. Regardless of the system you use, an OLIS patient query will involve the same steps:

1. Select a patient (e.g. by viewing that patient's chart).

2. Filter results by specifying information. For instance, you can select specific types of tests, or those tests from a specific ordering/attending/admitting health care provider, or that were processed by a specific specimen collection centre or lab. At a minimum, you must specify the date range for the search.
3. OLIS will search for all lab results that meet the stated criteria.
4. You may also sort the list of returned results (e.g. test type, or date).

Specific Privacy and Security Considerations

Your Privacy Obligations

As custodians of patient PHI and health care providers have obligations under PHIPA and Ontario Regulation 329/04 (the "Regulation").

eHealth Ontario has the authority as an agent of the Ministry of Health and Long-Term Care (MOHLTC) – a HIC – under PHIPA and under section 6.2 of O.Reg. 329/04 to operate and manage OLIS, as eHealth Ontario is receiving PHI from the MOHLTC for the purpose of creating or maintaining one or more EHRs.

In accordance with PHIPA, health care providers may only collect lab data from the OLIS system for the purpose of providing health care, or assisting in the provision of health care, to the provider's patients. Once lab information from OLIS has been copied into the provider's local record in any format (paper or electronic), it can be used for any purpose permitted by PHIPA or other applicable law.

When collecting, using, retaining and disclosing OLIS data, each health care provider is responsible for ensuring that he or she complies with their obligations set out in:

- All agreements entered into between eHealth Ontario and the health care provider or the organization for which the health care provider works (whether as employee, partner, agent, or under contract);
- All agreements entered into between the health care provider or the organization for which the health care provider works;
- PHIPA and Ontario Regulation 329/04 (the regulation);
- Any other applicable legislation or regulation; and e. Any applicable judicial or administrative tribunal judgments, orders, rulings, or decisions.

Each health care provider should ensure that his or her employees, agents and service providers handling PHI on the provider's behalf are in compliance with the provider's obligations, listed above, and are aware of, and comply with, any specific obligations under PHIPA or the regulation applicable to the provider's employees, agents or service providers.

A more complete description of provider privacy responsibilities can be found in PHIPA and the regulation.

Your Security Obligations

Health care providers who view the EHR data must comply with the obligations set out in the relevant eHealth Ontario access agreement signed with eHealth Ontario by their organization or by themselves and meet the requirements of the EHR Security Data Viewer Responsibilities at minimum.

Consent Directives

Restricting access at either the patient or test level means only the following are allowed to see it:

- The health care providers who were named on the lab requisition (e.g., the ordering or copied provider)
- The reporting lab, the lab that performed the test and the organization that placed the test request

In cases where a health care provider obtains the express consent of the patient or the patient's SDM to override a directive restricting access, MOHLTC as the custodian of OLIS, requires the provider to make a note in the patient's chart and clarify for the patient that although the consent override is temporary in respect of OLIS, the information that the patient has allowed the provider to view will be saved in the system, flagged as sensitive information, and may be available to other providers involved in the patient's care.

Further, in the case that the SDM has provided consent to override the consent directive, MOHLTC, as the custodian of OLIS, requires the provider to note in the patient's chart the name of the SDM and the relationship of the SDM to the patient. In the event the computer application and/ or the viewer service(s) does not have the functionality to support this, (i.e. log electronically) the health care provider is required to record the SDM's name and the SDM's relationship to the patient manually. This information must be available to eHealth Ontario upon request.

Appendix C: Diagnostic Imaging Common Service (DI-CS)

Overview

This Diagnostic Imaging Common Services (DI CS) is an eHealth Ontario initiative that enhances the delivery of patient care in Ontario by building on the success of the regional diagnostic imaging repositories. Repositories give authorized health care providers access to diagnostic images and corresponding reports from hospitals and independent health facilities within their region. The Diagnostic Imaging Common Service provides consolidated access to digital health information from the regional DI repositories so that users can view reports and images from across the province. It provides comprehensive secure access to a patient's provincial longitudinal digital

imaging record from anywhere and at any time. The digital imaging common service standard is used by system implementers to support the sharing of digital imaging reports and images.

Benefits

Benefits to You

- Access to diagnostic images and reports across Ontario
- Faster and easier access to images and reports 24/7
- Real-time clinical collaboration, increasing access to a broader range of specialists
- Eliminates the need to physically transfer images in hardcopy or on compact discs

Benefits to Your Patients

- Eliminates unnecessary travel
- Reduces wait times and lengths of stay thanks to faster exam reports and clinical decisions by physicians and specialists
- Reduces duplicate and unnecessary exams

Appendix D: Digital Health Drug Repository (DHDR)

Overview

The Digital Health Drug Repository (DHDR) represents the first foundational component of the Ministry of Health and Long-Term Care's Comprehensive Drug Profile Strategy (CDPS). The CDPS aims to improve the health and wellness of Ontarians and the quality of care they receive by providing health care providers with information to enable the Best Possible Medication History for a patient.

More information regarding the ministry's provision of access to information about publicly funded drugs and pharmacy services, as well as all monitored drugs (regardless of payor), can be found at: www.ontario.ca/mydruginfo.

Contents of the DHDR Data

Health care providers who are providing care or assisting in the provision of care to an individual are able to access information about:

- Publicly funded drugs dispensed in Ontario and paid for by the Ontario Drug Benefit (ODB) program and any other public drug programs (e.g., Special Drugs Program), including monitored drugs covered by these programs
- Drugs dispensed in Ontario to households pending eligibility with the Trillium Drug Program
- Monitored drugs (narcotics and controlled substances) dispensed in Ontario paid for by private insurance or cash, and
- Pharmacy services provided by a pharmacist in Ontario paid for by the Ministry, including:
    - MedsCheck Program medication reviews
    - Pharmacist administration of vaccines
    - ColonCancerCheck Fecal Occult Blood Test (FOBT) kits for colorectal cancer screening
    - Pharmacy Smoking Cessation Program services
    - Naloxone kits provided for harm reduction through the Ontario Naloxone Program for Pharmacies
    - Medications provided for Medical Assistance in Dying (MAID)

For drugs, health care providers are able to view the date, name, dosage form, strength, quantity and estimated days' supply of the drugs which have been dispensed to a patient. In addition, prescriber and pharmacy information is displayed. For pharmacy services, providers will see the date, a description of the service and the pharmacy information. In some instances, prescriber information will be available, which may be the name of the pharmacist that provided the service. Quantity and days' supply default to a value of 1.

Limitations of the DHDR Data

DHDR data is limited to:

- Information that the Ministry has the authority to disclose under the terms of PHIPA and the Narcotics Safety and Awareness Act, 2010 (NSAA);
- Information that has been submitted to the Ontario Public Drug Programs claims adjudication system or Narcotics Monitoring System to date in respect of the drug and pharmacy service data.

The information that is being made accessible has been provided to the Ministry by pharmacies, and may not necessarily include all of the current medications that a patient may be utilizing at any time, or all the pharmacy services that a patient has received.

The inclusion of information about a particular drug indicates that a record of dispensing was submitted to the Ministry by a pharmacy but does not necessarily confirm that the patient picked up the drug from the dispensing pharmacy, or that the patient is taking the drug as prescribed.

Drug products that are not captured in the repository, include unmonitored drugs paid for directly by patients or by private insurance, over-the-counter medications, or herbal products. These are not part of the information being made accessible to providers.

If a patient has blocked access to their information in the DHDR, providers will only be able to access this information with the express consent of the patient or their substitute decision-maker. It is important that health care providers discuss the information available through the DHDR with their patients to confirm their complete list of medications to develop the Best Possible Medication History.

The information being made available in the DHDR is advisory only and is not intended to replace sound clinical judgment in the delivery of health care services.

Talking to Patients about DHDR

The MOHLTC is making drug and pharmacy service information about patients available to health care providers through the DHDR to support the delivery of high-quality health care. It is important that providers continue to engage with their patients to confirm their complete list of medications, and to help them understand how this information may be used in their care to develop the Best Possible Medication History and for other clinical purposes.

Your patients may not be comfortable with the idea that this information is being shared, and should be aware that they have the right to block access to their information. However, patients are being encouraged to consult with their health care providers about the potential impacts that blocking access may have on the care that they receive. You can help your patients to understand the importance of making their medication and pharmacy service history accessible to help you make informed decisions about the care you provide. You can also assure your patients that their health care providers are required by law to protect the privacy of their personal health information.

Your patients are unlikely to be familiar with the details of the technology being used to make their information available to you. While they may have a general awareness of “electronic health records”, they are unlikely to recognize specific references to “the DHDR”. Therefore, the MOHLTC recommends that conversations with patients focus on “health care provider access to drug and pharmacy service information” rather than the DHDR solution specifically.

Benefits

Benefits to You

- Access to clinically relevant drug and pharmacy service information enabling the Best Possible Medication History (BPMH);
- Enhanced integration of available drug data through existing provincial digital health assets and other point of care systems such as, EMR, HIS, to quickly, securely and efficiently access data to enable the BPMH;
- Enhanced patient safety and continuity of care; and
- Improved collaboration between health care providers through the sharing of patient clinical data.

Benefits to Your Patients

- Enhanced patient experience with the health care system since care will be provided by well-informed health care providers;
- Improved patient-centered care by providing health care providers secure electronic access to a patient's drug and pharmacy service information and allowing them more time for diagnosis, treating and communicating with the patient; and
- Improved patient outcomes and decreased risk of adverse drug events.

Specific Privacy and Security Considerations

Patient Consent

The health care provider must print and complete a "Temporary Unblocking of Access to Your Drug and Pharmacy Service Information" form, which is available in the clinical viewer. If the patient's SDM is providing consent, the type of relationship with the patient must be included on the form. The health care provider must obtain the patient's / SDM's authorization and wet signature on the form and keep the form securely on file for audit purposes.

Appendix E: The Provincial Registries

Overview

The Provincial Registries (Provincial Client Registry and Provider Registry) are repositories that form the backbone of the Electronic Health Record (EHR). They are the "source of truth" for patient information as well as regulated provider information.

Provincial Client Registry (PCR)

The Provincial Client Registry (PCR) is the authoritative source for patient or client demographics and identifiers supporting electronic health records (EHRs) in Ontario. It provides a provincial patient identity and resolution service for health care providers to search for a patient, register a patient, and to enable access to a patient's electronic health record, linking records from multiple points of care.

The PCR aggregates patient identity data in real-time from the Ministry of Health and Long-Term Care's Registered Persons Database (RPDB), hospitals, and participating health care organizations to provide current patient demographics and a comprehensive list of patient identifiers.

Provincial Provider Registry (PR)

The Provincial Provider Registry (PPR) is the authoritative source of information regarding health care providers and organizations supporting the electronic health care record in Ontario. It assists health care providers in their electronic referral workflows and in keeping their local provider dictionaries current.

The PPR aggregates provider identity data from the Ministry of Health and Long-Term Care's Corporate Providers Database and from regulatory colleges (under the Regulated Health Professions Act or RHPA) to provide a comprehensive provider profile. It enables the identification of regulated provider persons and organizations that provide health services in Ontario, including details such as licensing status, specialties, and practice locations.

Benefits

Benefits to You

- Facilitate the sharing of clinical information by establishing a common patient identity across all points of service;
- Improve data quality and clinical workflow efficiency;
- Positively identify regulated provider persons;
- Provide information on providers (e.g., licensing status, practice locations).

Benefits to Your Patients

- Improve patient safety associated with patient misidentification;
- Enable the creation of an integrated longitudinal EHR;
- Reduce manual efforts related to maintaining and searching for provider information;
- Decrease time for clients to see providers (referrals, consults).

Appendix F: EHR Viewing Channels

There are numerous channel by which the EHR data repositories can be accessed. Below are some but not an extensive list. We will continue to grow this list of viewing channels as information becomes available

ConnectingOntario ClinicalViewer

The ConnectingOntario ClinicalViewer is a secure, web-based portal that provides real-time access to digital health records including:

- Hospital Visits
- Lab results
- Dispensed drugs
- Diagnostic Images
- Home and Community Care Information

With the support of information technology, the ClinicalViewer:

- Identifies and collects priority data: the CDR stores data from existing databases and registries
- Provides the ability to exchange information: a Health Integration Access Layer (HIAL) integrates and securely shares clinical data from multiple sources
- Provides access to information: access options, such as a provider portal and direct integration, allow clinicians to seamlessly access patient information online

The ClinicalViewer benefits clinicians and care providers at more than 859 health care organizations, representing the following sectors:

- Acute care

- Community support services
- Complex continuing care
- Long-term care
- Mental health and addictions
- Primary care
- Rehabilitation
- Pharmacies

ClinicalConnect

ClinicalConnect is a secure, web-based portal that gives health care providers real-time access to their patients' electronic medical information from all acute care hospitals, Local Health Integration Networks' (LHIN) Home and Community Care Services and Regional Cancer Programs in South West Ontario, in addition to various provincial clinical data repositories.

Provides timely and secure access to comprehensive patient health care information including, but not limited to:

1. Hospital Visits
2. Lab Results
3. Dispensed drugs
4. Diagnostic Images
5. Transcribed Reports
6. Home and Community care Information

Key modules and functionality within ClinicalConnect include:

- Patients lists (including option to customize)
- New results flag for new and abnormal results
- Patient visits (historical and future scheduled)
- Transcriptions (discharge, OR, Consult and Progress notes)
- Labs reports, including graphing and trending

- Diagnostic service reports and radiology images from hospitals
- Pharmacy orders for select in-patient hospital pharmacy orders, ODB covered medications and narcotics
- Allergies
- Health information including client demographics, personal & medical contacts, service list, placement list, LTCH choices and bookings, community support resources, diagnosis, primary care group, risks, safety issues,

ClinicalConnect is available via desktop computers, tablets or mobile devices. Physicians in some LHINs have the option to electronically download hospital data into their EMRs. In addition, hospital sites federated with ONE ID, can 'Single Sign On' (SSO) directly to ClinicalConnect from their HIS.

Electronic Medical Record (EMR) Integration

In partnership with eHealth Ontario, OntarioMD – a subsidiary of the Ontario Medical Association – maintains a provincial specification for EMR systems. EMR products certified against the 4.0 or higher specification are able to connect automatically with OLIS to receive lab results in the EMR.

The patient query enables users to search lab test histories for particular patients – regardless of who ordered the test. This enables you to:

- Pre-load a new patient's chart with historical laboratory results ordered by another health care provider
- Check previous versions of a test to see what the trend is
- Check to see if a particular type of test has already been done (e.g., to avoid redundant testing)

Important reminders:

- OMD-certified EMRs data filters must be set so that OLIS data is not reconciled with a pre-existing patient in the EMR patient database and must automatically be flagged for review and sign off in an unmatched queue.
- All reports must be reviewed and signed off by the named practitioner before being incorporated into the EMR patient record and those reports that are not matched with an existing patient must be filtered automatically.
- Practitioners should only be accessing information on behalf of a HIC that is providing or assisting with the provision of healthcare to their patients in the context of the OLIS Practitioner Query (Z04 query).

Specific Privacy and Security Considerations

In special cases (with consent from the patient or the patient's substitute decision-maker) the patient consent directive restricting access to the test can be overridden by a provider, from within the EMR.

Such an override is logged in the EMR system, along with the identity of the overriding health care provider, and an assertion as to what kind of consent was obtained. In addition, OLIS logs all accesses to its data, and an audit of this information can be requested by the patient.

In cases where a health care provider obtains the express consent of the patient to override a directive restricting access, it is recommended that the provider clarify for the patient that although the consent override is temporary in respect of OLIS, the information that the patient has allowed the provider to view will be saved in the EMR system, flagged as sensitive information, and may be available to other providers involved in the patient's care.

Off-boarding

In cases where a health care provider leaves the practice, you must adhere to the following:

- Be sure to revoke access to users who have left the practice or no longer require access to OLIS Data and disable any associated automated Practitioner or patient queries to OLIS at the first reasonable opportunity and in any event no later than 5 business days after the user has left the practice or no longer requires access to OLIS Data;
- Delete any OLIS Data queued in the user's inbox awaiting sign off or deletion within 5 business days of the user leaving the practice or no longer requiring access; and
- In the event the practice has delegated user account management to the Certified EMR Vendor, the practice is to instruct the EMR Vendor to perform the above tasks within the required timeframes.
- Remove user from pull down menu in the EMR so that they cannot be selected from the UAO drop down list

Electronic Child Health Network (eCHN) Integration

eHealth Ontario and eCHN are collaborating to make laboratory information from OLIS available to authorized users of eCHN via eCHN's WebChart.

Specific Privacy and Security Considerations

The eCHN WebChart application enables Users to override a consent directive applied to data within eCHN's system where; (a) there is a clinical/emergency requirement; or (b) access has been granted directly by patient or the patient's SDM (expressed consent).

However, the MOHLTC, as the health information custodian of OLIS, does not permit authorized Users who access OLIS to override a consent directive applied to OLIS data without the patient's (or their SDM's) express consent. Therefore, eCHN's Users must not perform the consent override on OLIS data without obtaining express consent from the patient or their SDM, even for reasons of clinical emergency.

Consequently, eCHN has modified its WebChart user interface to permit eCHN users to override the patient's consent directive, for OLIS data, only with the express consent of the patient or SDM, and not for reasons of clinical emergency (eCHN has technically disabled the clinical/emergency override option within WebChart for OLIS data). Overriding a patient's consent directive for OLIS data without express consent from the patient or the patient's SDM will constitute a breach of the User's (or User facility's) agreement with eHealth Ontario, and will be subject to the remedies available under the agreement.

Please contact eHealth Ontario's Privacy Office at privacy@ehealthontario.on.ca, if you have any questions about consent management for OLIS data. Please indicate in the email that you are an eCHN User.

Appendix G: Procedures for Communicating Sensitive Files

eHealth Ontario policies require that adequate safeguards be applied every time a sensitive document or file is stored or transferred through communications channels that are not considered safe and secure such as regular internet email, CDs, DVDs, USB sticks and/or flash memory card.

One Mail should be used to securely transmit sensitive data to other One Mail users. However, when transmitting sensitive data to any other mail users, WinZip or similar software is recommended.

This section provides instructions on how to apply a strong level of protection to sensitive files and reports, using WinZip, a commercially available application that can be used both to reduce the size of a document and to apply strong protection.

It is important to keep in mind that the encryption tool described in this document is a password-based cryptosystem. The protection of file encryption can be broken if the associated password is compromised. Therefore, it is required that the password protection guidelines described in the "password sharing" section be applied by anyone who uses the tool and is involved in the file encryption process.

Authorized Uses

This process can be used whenever there is an occasional need for any sensitive information to be transferred over email consistent with regular business processes, including documents that contain personal information and/or personal health information.

If sending sensitive information over non secure email is an ongoing business process, considerations should be made to automate the process and use an enterprise mechanism to securely transfer the information.

eHealth Ontario's limit on email attachments is 10 MB per email.

For further assistance or information not covered in this document, please contact the eHealth Ontario Service Desk at 1-866-250-1554.

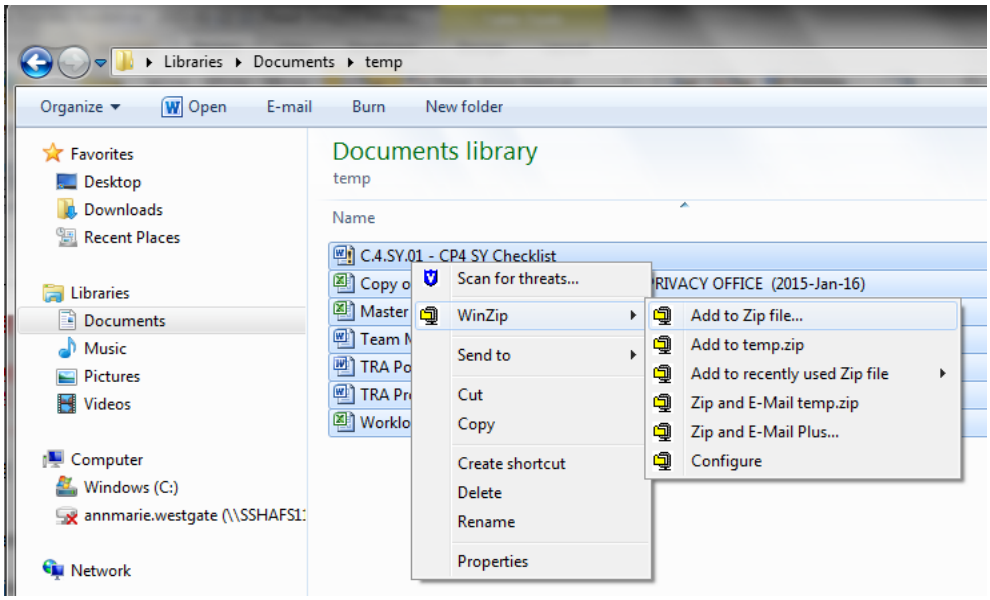
Use of WinZip Encryption Software

WinZip is eHealth Ontario's suggested encryption tool.

Encrypting Files Using WinZip

Step 1. Create Archive

- Open the file location.
- Navigate to the folder where the files are. Using the mouse, select the files you wish to zip. On the dialogue box that opens float your mouse over WinZip and choose to
- Add to Zip file…
- Assign the file name you wish to use.

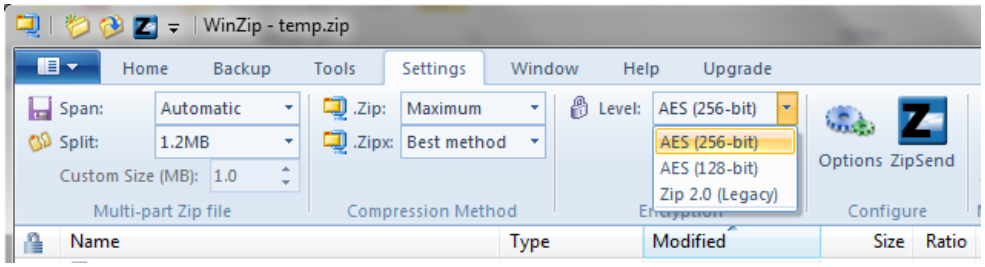


Step 2. Open the Archive:

- Double click on the zip file to open the archive.

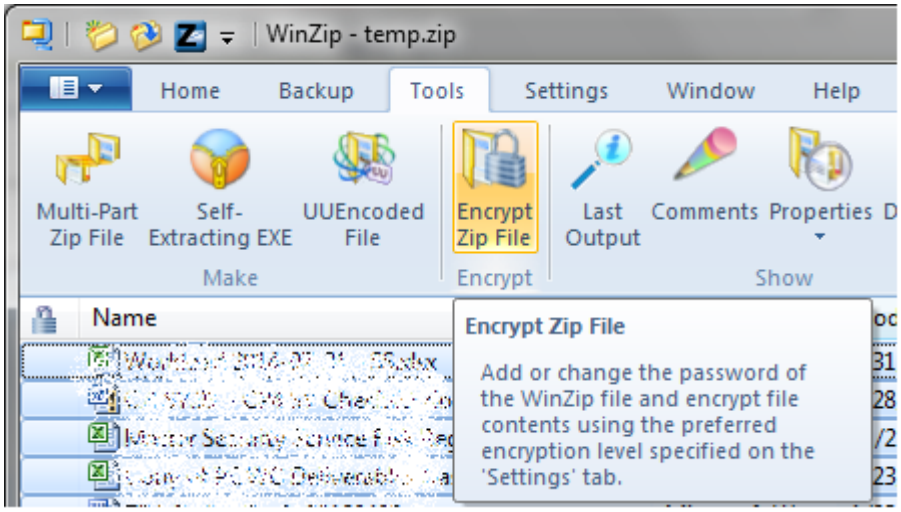
Step 3. Choose a stronger encryption mechanism

- Use AES 256-bit encryption.
- In the Settings tab, ensure the encryption level selected is AES (256- bit).



Step 4. Encrypt the entire file

- From the Tools menu, click on Encrypt Zip File



Step 5. Create a strong password

- Enter a password and then confirm it.
- See Section Error! Reference source not found below for how to create a strong password.

The file must be encrypted and password protected before the sender transfers it to the requester as an attachment to an email message.

WinZip, described in this document, supports symmetric encryption. This requires the exchange of a shared secret (password in this case). In other words, the sender of the encrypted file must communicate the password to the intended recipient of the file. WinZip does not provide a method for retrieving files from an encrypted archive if a password is forgotten. The password creation and sharing therefore requires special attention.

Other Encryption Methods

If your computer does not have WinZip installed, you may contact your site help desk for assistance or use Microsoft Word or Excel for encryption. Steps for encrypting in Word or Excel are as follows:

- Open the document.
- Click on the File tab, and click on Info.
- Select Protect Document.
- In the pull down menu, choose Encrypt with Password.
- Enter a password and then click OK confirm it.

File Transfer and Sharing

Once the file has been encrypted and password protected it is temporarily saved to the network share or local hard drive share. The file can then be attached to an email and sent to the help desk. Do NOT attach any screen shot directly within the email with any PHI/PI. It must first be encrypted and password protected.

The password should be communicated by phone to the file recipient or by using an "out of band" method (e.g. if emailing the document, send password by phone, fax or mail). In other words, the password should not be sent at the same time using the same method as the encrypted file.

Password Creation

- Create a strong password to protect encrypted files.
- Create and use a different password for each different WinZip archive.
- Use 8 characters or more.
- Passwords must contain characters from three of the following four categories: uppercase characters (A-Z); lowercase characters (a-z); numeric (0-9); and special characters (e.g. !, $, #, _, ~, %, ^).
- Example of a bad password is 1234Password!
- Example of a good password is iT_iS_A_warM_daY22

Once a password has been created, the sender will transfer the file to the requester by email. Be careful to send the email to the correct recipient. When the requester receives the email, the requester then calls the sender to acquire the password.

Password Sharing

Passwords must be securely shared when being sent to eHealth Ontario from a HIC. The procedures are as follows:

- Determine the authorized recipient of the information
- Make the encrypted file available to the recipient using agreed process (e.g. SFTP, email)
- The requestor calls the sender by phone
- The sender verbally verifies the recipient's identity:
    - name
    - title, business unit, organization
    - name of received / retrieved encrypted file

- Verbally provide the verified recipient with the password to open the encrypted file
- Request and obtain verbal confirmation that the recipient has been able to extract the file(s)
- The sender securely destroys the written copy (if any) of the password and deletes any copies of the file from any local or network drives

Password Recovery

WinZip does not provide a mechanism for password recovery. Therefore, in the case of long-term storage of encrypted files, a method of password recovery must be in place to access these files (e.g. if an employee leaves and their files need to be accessed).

An example of a password recovery method is storing the password in a sealed envelope which can only be accessed by upper management and will only be accessed for password recovery purposes.

File Deletion

Once a file has been decrypted and used, it must be deleted by both the sender and the requester of the file.

Appendix H: Glossary

Term	Definition
BPMH	Best Possible Medication History
CDPS	Comprehensive Drug Profile Strategy
CDR	Clinical Data Repository
CPP	Cumulative Patient Profile
DHDR	Digital Health Drug Repository
DI	Diagnostic Imaging
DI-CS	Diagnostic Imaging Common Service
DI-R	Diagnostic Imaging Repository
eCHN	Electronic Child Health Network
EHR	Electronic Health Record
EMPI	Enterprise Master Patient Index
EMR	Electronic Medical Record
FOBT	Fecal Occult Blood Test
HIAL	Health Integration Access Layer
HIC	Health Information Custodian
HIS	Hospital Information System
IHF	Independent Health Facility

Term	Definition
MAID	Medical Assistance in Dying
MOHLTC	Ministry of Health and Long Term Care
NMS	Narcotics Monitoring System
NSAA	Narcotics Safety and Awareness Act
ODB	Ontario Drug Benefit
OLIS	Ontario Laboratory Information System
PCR	Provincial Client Registry
PHI	Personal Health Information
PHIPA	Personal Health Information Protection Act
PI	Personal Information
PR	Provider Registry
RPDB	Registered Persons Database
SDM	Substitute Decision Maker

Copyright Notice

All rights reserved

Trademarks