eHealth Ontario
It's working for you

eHealth Ontario Site Support Guide

Clinical Data Repository (CDR)

Reference Guide & Privacy and Security Procedures and Obligations

This guide is for sites that have implemented an electronic interface to one of the eHealth Ontario Clinical Data Repositories (CDRs) and have signed or will sign the EHR Interface Services Schedule. It will assist these sites with information around processes and contacting eHealth Ontario for support as well as CDR related privacy and security procedures and obligations.

Ontario
eHealth Ontario

Version: 2.2

1 Table of Contents

2 General Information

2.1 Purpose and Scope

The site support guide is a comprehensive document that outlines the processes related to the use of one of the Clinical Data Repositories (CDRs). These processes include:

- How to register & connect new users and sites to one or more of the Clinical Data Repositories (CDRs).
- High-level support processes between the various parties when incidents arise during use of the CDR
- Privacy & Security obligations related to the CDR.
- Your operational responsibilities for handling of CDR data

2.2 Audience

This document is intended for the operators of Regional Clinical Viewers (i.e. Hamilton Health Science's Clinical Connect) who will act as the 'application interface' between the CDR data repositories housed at eHealth Ontario and sites who view clinical data within one of the CDRs.

This document is intended as an accompaniment to the EHR Interface Services Schedule the operator organizations have signed or will sign in order to display CDR data on their Regional Clinical Viewer.

2.3 Related Documents

The Guide should be read in conjunction with the following information found at eHealthOntario.on.ca:

- eHealth Ontario Personal Health Information Privacy Policy
- EHR Access and Correction Policy
- EHR Assurance Policy
- EHR Consent Management Policy
- EHR Inquiries and Complaints Policy
- EHR Logging and Auditing Policy
- EHR Privacy and Security Training Policy
- EHR Privacy Breach Management Policy
- EHR Retention Policy
- eHealth Ontario Federation Identity Provider Policy and Standard
- EHR Security Policies
    - Acceptable Use of Information and Information Technology Policy
    - Access Control and Identity Management Policy for System Level Access
    - Business Continuity Policy
    - Cryptography Policy
    - Electronic Service Provider Policy
    - eHealth Ontario Federation Identity Provider Standard

  - Information Security Incident Management Policy
  - Information and Asset Management Policy
  - Information Security Policy
  - Local Registration Authority Practices Policy
  - Security Logging and Monitoring Policy
  - Network and Operations Policy
  - Physical Security Policy
  - System Development Lifecycle Policy
  - Threat Risk Management Policy
- eHealth Ontario Service Interaction Guide

3 CDR Support Model

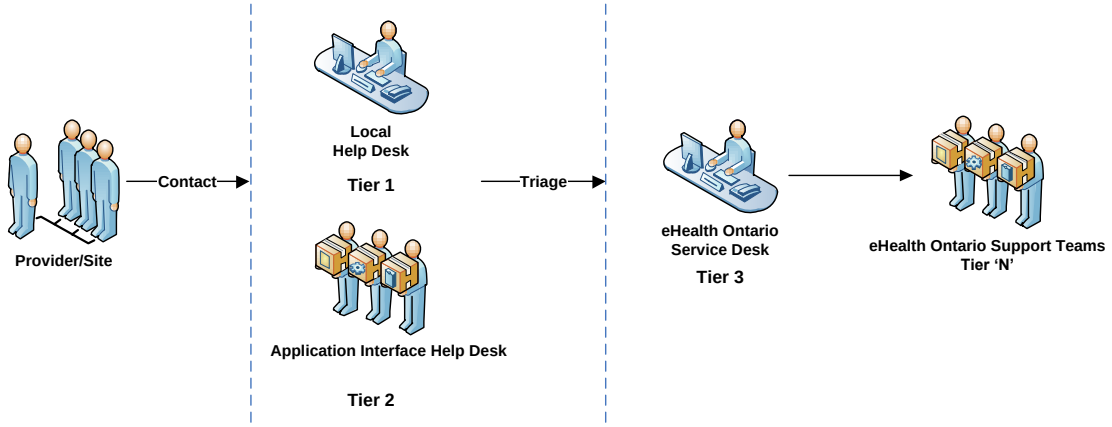


Figure 1 – High Level Support Model

As depicted in Figure 1 above, when a provider/site is experiencing a CDR issue the following process should be adhered to. Please refer to the Service Interaction Guide for further details.

1. **TIER 1:** Provider/site contacts their Local Help Desk at their organization. The Local Help Desk will collect the required details about the issue from the provider. The Local Help Desk will then investigate the issue and resolve if possible
    - Please note that Local Help Desks have their own independent processes regarding investigation of issues. In addition, not all sites may have a Local Help Desk.
2. **TIER 2:** If the Local Help Desk cannot resolve the issue, the site contacts the Application Interface Help Desk. The Local Help Desk will provide the Application Interface Help Desk the required details about the issue. The Application Help Desk will then investigate the issue and resolve if possible.
    - Please note that this process is governed by a separate support process governed between you and the local sites you manage.
3. **TIER 3:** If the Application Interface Help Desk cannot resolve the issue, the Application Interface Help Desk will contact the eHealth Ontario Service Desk on the site's behalf. The Application Interface Help Desk will provide the eHealth Ontario Service Desk the required details about the issue. This will allow eHealth Ontario to investigate the issue and resolve.
4. **TIER 'N':** If the eHealth Ontario Service Desk cannot resolve the issue on the spot, the issue will be re-directed to various Support Teams within eHealth Ontario, depending on the issue being experiences. These Support Teams are known as Tier 'N'.

Given that the support processes between the Site-Local Help Desk and Local Help Desk –Application Interface are governed by separate agreements, this guide will focus on the support processes between Application Interface-eHealth Ontario. However, both the Local Site Help Desk (Tier 1) and Application Interface Help Desk (Tier 2) are responsible for the following accountabilities before the incident being escalated to eHealth Ontario Service Desk:

- Troubleshooting issues
- Providing resolution where possible
- Determining potential impact of the issues
- Escalating to the appropriate support groups and/or the eHealth Ontario Service Desk

Incident Management Support Flow

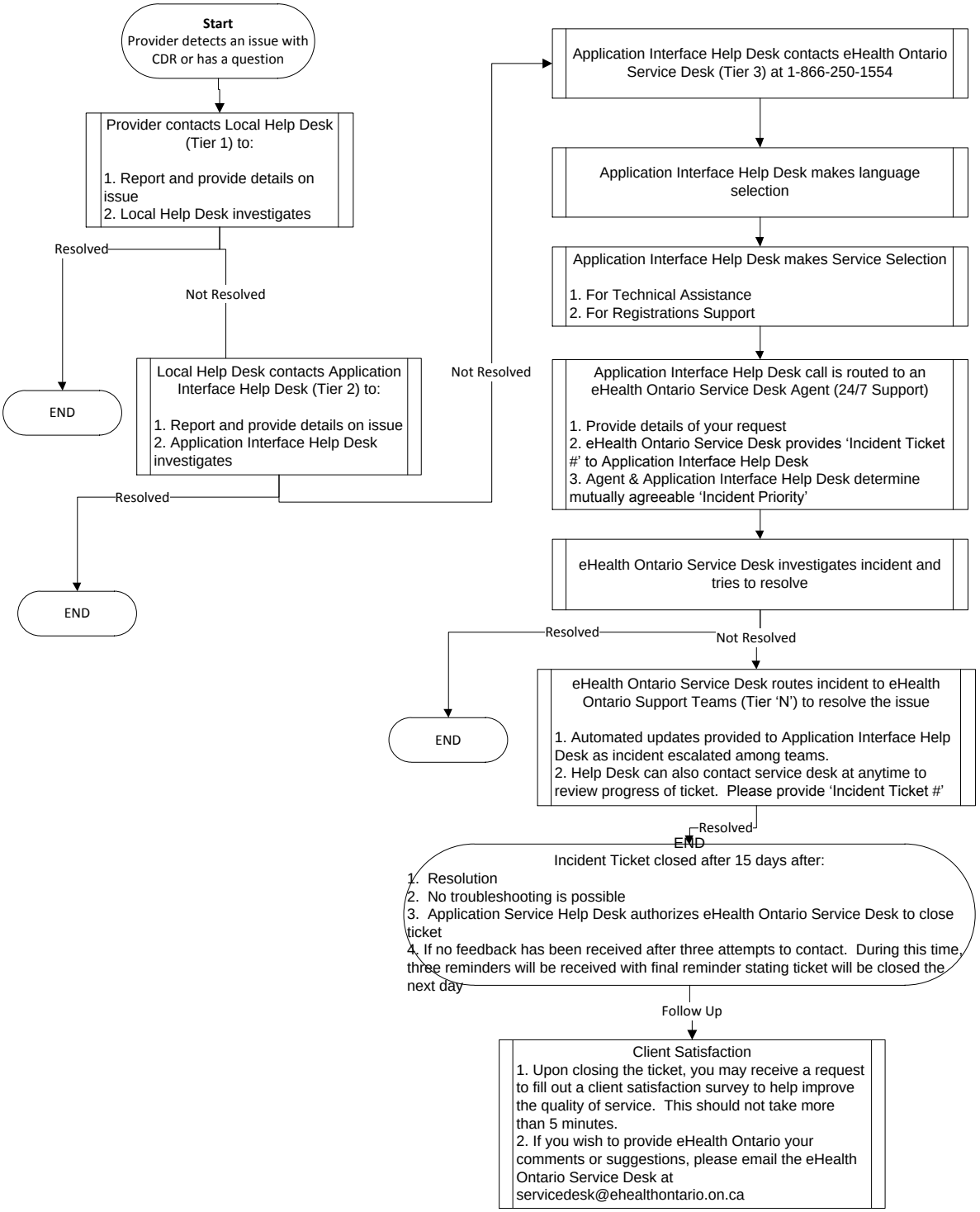


Figure 2 – Incident Management Support Flow

3.1 When to Contact the eHealth Ontario Service Desk

Application Interface Help Desks should contact the eHealth Ontario Service Desk for any and all incidents being experienced by the:

1. Application Interface Owner
2. Incidents escalated from the Site and Local Help Desk that could not be resolved

These incidents include the following:

- Troubleshooting CDR public key infrastructure PKI certificate issues
- Troubleshooting service related interface issues
- Reporting a CDR application error
- Reporting missing results in one of the CDRs
- Reporting data quality issues in one of the CDRs
- Reporting a actual or suspected privacy breach
- When requesting information from eHealth Ontario about:
    - CDR functionality
    - Privacy and security of personal health information

The eHealth Ontario Service Desk is the single point of contact for opening incident tickets for CDR related issues.

3.2 How to Contact the eHealth Ontario Service Desk

Application Interface Help Desks can contact eHealth Ontario through:

Email:* servicedesk@ehealthontario.on.ca
Phone:* 1-866-250-1554
Fax: 416-586-4040
(Please phone the eHealth Ontario Service Desk to notify them when faxing any information related to an incident or service request.)

*Note: Phone is the primary method of contact for the eHealth Ontario Service Desk. There is currently no service level agreement for incidents or service requests via email.

The Hours of Operation for the eHealth Ontario Service Desk is 7/25/365 to report all incidents.

3.3 Information to Provide the eHealth Ontario Service Desk

When the Application Interface Help Desk contacts the eHealth Ontario Service Desk to open an incident, certain information about the incident needs to be provided to the Service Desk Agent. This includes:

- Your name
- Your site location
- Your contact information, include backup contacts where applicable
- Indicate to eHealth Ontario support staff what data is trying to be sent or accessed (e.g. DI data, primary care data, acute care data, lab data, etc..).
- Indicate the eHealth Ontario service environment affected e.g. production or testing
- Description of issue <include date and time the issue occurred, the number of users impacted if known>
- Steps to reproduce issue and troubleshooting diagnostic steps taken

• Local Site (hospital /organization name)
• Site Contact Information
• Authorized caller identifier
• Local/Site ticket number
• Description of issue
• Impact of issue
• Date and time when issue first appeared
• Priority determined by Local/Site Help Desk or Subject Matter Expert
• Workaround (if available)

When reporting data quality issues related to missing results or incorrect data the following information needs to be supplied to the eHealth Ontario Service Desk:

- Your contact information <phone #> <email address>
- The name of your organization or the organization that you are reporting on behalf of <physician's office, hospital, department>
- The name of the organization that submitted the result
- The message details (organization, patient name and MRN)
- The information that is missing (if reporting a single missing result)
- If the CDR result information is incorrect, provide details around why you think it is incorrect

This information must be supplied according to the Procedures for Communicating Sensitive Files via Email in Appendix A.

Collection of this information may necessitate the Application Interface Help Desk to liaise with the provider experiencing the issue or the Local Site Help Desk.

eHealth Ontario recommends that support processes between the Provider-Local Help Desk and Local Help Desk-Application Interface Help Desk include steps to collect this information at first point of contact. This will expedite ticket triaging, investigation and resolution by eHealth Ontario if the incident escalates to Tier 3. If the Application Interface Help Desk or Local Help Desk has to go back to collect this information, this will take additional time and lengthen the period of time the incident is open before investigation can begin and/or it is resolved.

When following up on an existing incident, Application Interface Help Desks need to reference the Incident Ticket # provided by the eHealth Ontario Service Desk when the incident was first reported.

3.4 When Does eHealth Ontario Contact You

The eHealth Ontario Service Desk may contact the Application Interface Help Desk in order to:

- Clarify an incident or request you have reported
- Notify you of maintenance activities at our site that may impact service
- Report a failure in the CDR application
- Provide information regarding our release dates and application improvement activities
- Contact the Local Help Desk or Provider for follow up/investigation on an issue, gather more information, or communicate information about the service incident

The eHealth Ontario Privacy Office and Security Office may contact the Application Interface Help Desk to:

- Request additional information to fulfill CDR access and correction requests
- Support Privacy and Security incident management

4 Operational Responsibilities for CDR Data

Under the *Personal Health Information Protection Act, 2004* (PHIPA), eHealth Ontario is responsible for keeping an electronic record of all accesses to CDR data whether held in an eHealth Ontario system or a third party system.

Due to this legislative requirement, eHealth Ontario must have access to a copy of the audit logs held by RCV operators which would display:

- Who accessed which information
- When that information was accessed
- What location the query was made from

eHealth Ontario may be asked to provide a report on these audit logs for privacy investigations to fulfill patients requests.

5 Privacy and Security

5.1 Consent Management

Quick Tip

The CDRs give patients, or their substitute decision maker(s) (SDM), the option to allow or restrict access to patient data within the solution. Should a patient choose to place a consent directive in one of the CDRs, he /she must fill out the EHR Consent form at http://www.ehealthontario.on.ca/docs and send it to eHealth Ontario. Providers may help a patient fill out the form and forward it to eHealth Ontario on the patient's behalf.

The CDRs give patients or their substitute decision maker(s) (SDM) the option to allow or restrict access to their patient data when viewed. . If a patient restricts access to his / her data by applying a consent directive, providers querying the CDR will be unable to access information relating to that patient information to which a consent directive has been applied.

Consent directives can be made, modified or removed to restrict access the following 'levels' of patient information in the CDRs:

- **Global**: All Health Care Providers (HCPs) would be restricted from accessing any of the patient's Personal Health Information (PHI) contained in the CDRs. Please note that this excludes demographic data available in the Client Registry and the Consent Registry
- **Domain:** Block all providers from accessing patient records in CDR domain
- **HIC-Agents**: Specific HCPs (Dr. Smith) from a specific HIC (i.e. Hospital A) would be restricted from accessing any PHI from that patient in the CDRs.
- **Agent**: Specific HCPs (Dr. Smith) would be restricted from accessing any PHI from that patient in the CDRs.

5.1.1 Applying Consent Directives

If a patient contacts a Health Information Custodian (HIC) and wishes to either place a restriction on access to his / her information, or wishes to reinstate access (remove the restriction), the HIC should:

1. Capture the consent directive information on the EHR Consent Form at http://www.ehealthontario.on.ca/docs , and
2. Submit the consent directive information to eHealth Ontario by faxing it to 416-586-4397 or 1-866-831-0107

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 EHR Consent Form at http://www.ehealthontario.on.ca/docs , and / or contact us directly at 416-946-4767.

In all instances, eHealth Ontario will apply the consent directives within 7 days of verifying the identity of the patient making the request. The health care provider or organization who received the consent directive request from the

patient then notifies the patient that his / her request has been fulfilled. If you cannot notify the patient, the HIC will let eHealth Ontario know so that eHealth Ontario can notify him / her on your behalf.

Note that consent directive requests sent to eHealth Ontario on behalf of patients should come from the Designated Privacy Contact at the HIC. A designated Privacy Contact is either the Privacy Officer or someone designated as a delegate according to the agreements signed with eHealth Ontario.

5.2 Access Requests by Patients

Quick Tip
When a patient requests to view or correct data your practice has contributed, follow your internal procedures for allowing access or correction to that data. Make note of this request.

When a patient requests to access or correct data that other HICs have contributed, direct the patient to contact eHealth Ontario at 1-866-250-1554as soon as possible to make the request.

5.2.1 Access to Data Requests

Under *Personal Health Information Protection Act* (PHIPA), patients or their substitute decision makers have a right to access data held by a HIC about them. When a HCP receives a request for records he / she has collected, created, and / or contributed by the provider to one of the CDRs, the provider must follow Part V of PHIPA as well as all its related internal policies, procedures and practices to respond directly to the patient.

In instances where request for access involves information contributed by another HIC or by multiple HICs, providers are required to:

1. 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
2. Direct the individual to contact eHealth Ontario at 1-866-250-1554 or info@ehealthontario.on.ca

As per the *EHR Access and Correction Policy*, eHealth Ontario may seek assistance from the HIC when responding directly to a request for access by a patient. The HIC should provide eHealth Ontario a contact person at the organization that can assist with this work.

5.2.2 Requests for Audit Logs

When a provider receives a request from a patient to view the audit logs associated with their records stored in one of the CDRs, the provider is required to:

1. Notify the individual that he / she is unable to process the request for access, and
2. Direct the individual to contact eHealth Ontario at 1-866-250-1554 or info@ehealthontario.on.ca

5.3 Correction Requests

When a HIC receives a request for correction directly from an individual related to health records that were created and contributed to one of the CDRs solely by that HIC, he / she 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 the patient wants 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 an individual related to records that were created and contributed to one of the CDRs by another HIC or by more than one HIC, the provider must respond to the patient no later than two days upon receiving the request by:

- Notifying the patient that the request for correction involves PHI not within their custody or control, and
- Directing the individual to contact eHealth Ontario at 1-866-250-1554 or info@ehealthontario.on.ca

eHealth Ontario will coordinate the response to this request, and may seek assistance from the HIC(s) when responding to the individual. The HIC should provide eHealth Ontario a contact person at the organization that can assist with this work.

5.4 Privacy Inquiries

5.4.1 Complaints & Inquiries

Quick Tip
When an individual patient submits an inquiry or complaint related the CDRs, direct him/her to contact eHealth Ontario with their inquiry or complaint.

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

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

- Notify the individual that you are unable to respond to the inquiry/complaint, and
- Direct the individual to contact eHealth Ontario at 1-866-250-1554 or info@ehealthontario.on.ca

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

5.4.2 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 individual access requests, consent obligations or incident/breach management processes, please direct them to contact eHealth Ontario at 1-866-250-1554 or info@ehealthontario.on.ca

Please ensure that the provider or you do not include any personal information (PI) or personal health information (PHI) in any emails to eHealth Ontario.

5.5 Breach Management

5.5.1 Security Incident and Breach Management

This section includes instructions for HICs reporting to eHealth Ontario any security incidents or breaches (defined below).

A security incident is an unwanted or unexpected situation that results in:

- Failure to comply with the organization's security policies, procedures, practices or requirements
- Unauthorized access, use or probing of information resources
- Unauthorized disclosure, destruction, modification or withholding of information
- A contravention of agreements with eHealth Ontario by the organization, users at the organization, or employees, agents or service providers of the organization
- An attempted, suspected or actual security compromise
- Waste, fraud, abuse, theft, loss of or damage to resources

The 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 one of the CDRs.

5.5.2 Privacy Breach Management

Quick Tip
A HIC shall report an actual or suspected privacy breach to eHealth Ontario by calling the 24/7 service desk at 1-866-250-1554 as soon as possible.

The *EHR Privacy Breach Management Policy* describes detailed steps to be taken in the event of a privacy breach/incident.

A HIC shall report an actual or suspected privacy breach to eHealth Ontario by calling the 24/7 service desk at 1-866-250-1554 as soon as possible, but in any event no later than the end of the following business day. Reporting a breach / incident to eHealth Ontario is required when a HIC becomes aware of an actual or suspected privacy breach caused or contributed to 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.

In instances where a breach is caused by a HIC who solely created and contributed the data to one of the CDRs, the HIC shall follow its internal policies, procedures, and practices to notify the individual(s) to whom the PHI relates at the first reasonable opportunity in accordance with PHIPA to contain, investigate and remediate the privacy breach.

In instances where a breach was solely caused by a HIC that did not solely create and contribute the PHI to one of the CDRs, the HIC, in consultation with the 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*.

5.5.3 Instructions for Health Care Providers – Security Incident

If you become aware of, or suspect, a security incident or breach of one of the CDRs or data by you or any of your employees, agents, or service providers, you must immediately report it to Designated Privacy Contact. If you are unable to reach your Designated Privacy Contact or support team to report a breach, contact eHealth Ontario service desk at 1-866-250-1554 and open a security incident ticket. You are required to cooperate in any incident or breach containment activities or with any investigation. During the investigation, you may be required to provide additional information which may include PHI or PI, in order to contain or resolve the incident or breach.

Important: It is extremely important that you do not disclose any patient personal health information and/or personal information to the service desk when initially reporting a security incident or breach.

5.5.4 Instructions for Designated Privacy Contact – Security Incident

If you become aware of, or suspect, an incident or breach related to one of the CDRs or data by any of your organization's staff members, including employees, agents or service providers, you must immediately report the incident or breach to the eHealth Ontario service desk 1-866-250-1554 and open a security incident ticket.

Important: It is extremely important that you do not disclose any patient personal health information and/or personal information to the service desk when initially reporting a security incident or breach. It is expected that you 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, please have the following information ready:

1. The time and date of the reported incident
2. The name and contact information of the agent or electronic service provider who reported the incident
3. Details about the reported incident, (e.g., type and how it was detected)
4. Any impacts of the reported incident, and
5. 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 incident response lead or team will be engaged to deal with the situation. A remediation plan will be developed in consult with the requestor.

6 Registering Users for Service

Providers will be able to access a CDR contained within the Application Interfaces via a variety of Point of Service (POS) applications (i.e. the web, hospital information system, etc.)

Providers should be reminded that not all POS applications are available to all providers at this time. Providers should contact their Application Interface Operators to find out if they have access to CDR data via which POS application. In addition, not all providers that have access to the Application Interface may necessarily have access to one of the CDRs. They should contact their Application Interface Operator, to find out.

Depending on organization, providers will use one of various credentials to login to one of the CDRs contained within the Application Interfaces.

1. ONE ID ® credentials issued by eHealth Ontario
2. Local credentials issued by your health care organization
3. Credentials issued by the application interface owners

New users are registered by contacting their Local Registration Authority (LRA) at their organization to complete the registration form. Users will be provided credentials to log-in to one of the CDRs using a unique user name and password.

Appendix A: Procedures for Communicating Sensitive Files via email

Overview

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.

This document 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 PI and/or PHI.

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 please contact the eHealth Ontario service desk at 1-866-250-1554.

Instructions to file encryption and password creation

Use of WinZip encryption software

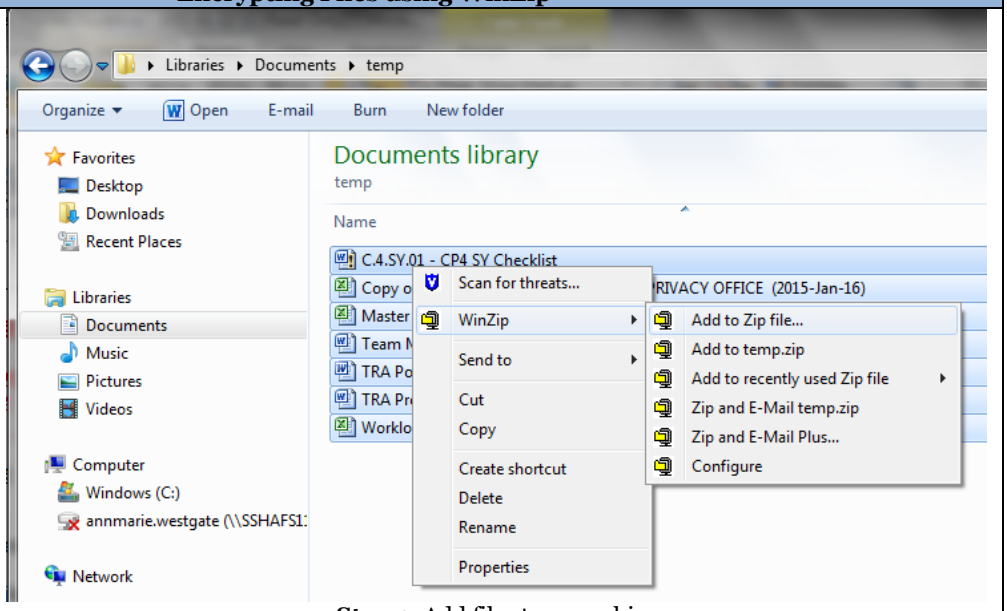
WinZip 16.0 standard versions are eHealth Ontario's suggested encryption tool.

Encrypting Files using WinZip

Step 1. Create Archive
Open the file location.

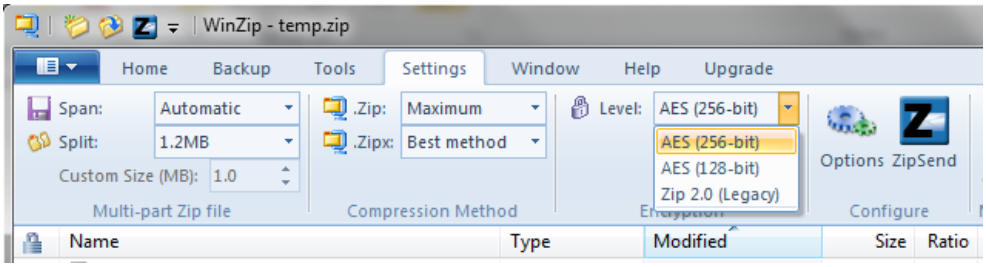
Navigate to the folder where the files are. Using the mouse, select the files you wish to zip. On the dialogue box that opens float your mouse over WinZip and choose to **Add to Zip file…**

Assign the file name you wish to use.

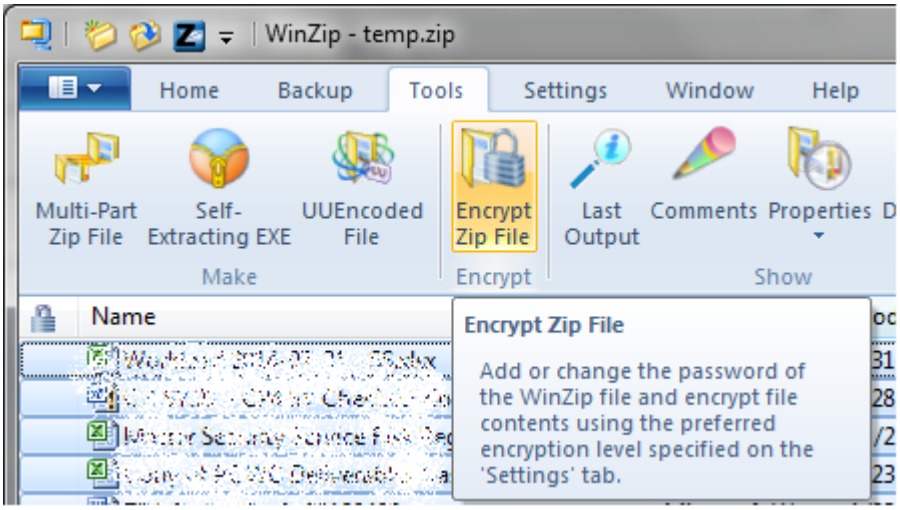


Step 1. Add files to an archive

<table>
<tr><th colspan="2">Encrypting Files using WinZip</th></tr>
<tr><td>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).</td><td> 

Step 3 Choose an encryption mechanism</td></tr>
<tr><td>Step 4. Encrypt the entire file

From the Tools menu, click on Encrypt Zip File</td><td> 

Step 4. Encrypt the Zip File</td></tr>
</table>

Encrypting Files using WinZip	
Step 5. Create a strong password Enter a password and then confirm it. See Section **Error! eference source not found.** below for how to create a strong password.	 **Fig.4** 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.

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 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.

The following requirements apply to password management:

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*

File transfer

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 B: Sample Incident Report Form

Privacy/Security Incident/Breach Management Report

Part I - Identification and Reporting

1. Background Information

Incident/Breach Summary	
Name of reporting organization	
Point of contact and contact details	

2. Incident/Breach Details

Date & time incident/breach reported	
Date & time Incident/breach discovered	
Date & time incident/breach occurred	
Place of incident/breach	
Name and title of person who discovered incident/breach	
How the incident/breach was discovered	
Organization(s) or individual(s) affected by the incident/breach (e.g., employees, service providers)	

3. Type of Privacy/Security Breach

Type of Privacy Incident/Breach?	Privacy breach - ☐ Yes ☐ No Privacy Incident - ☐ Yes ☐ No ☐ N/A
	☐ Policy infraction ☐ Agreement infraction ☐Unauthorized collection ☐ Unauthorized use ☐Unauthorized disclosure ☐ Unauthorized disposal ☐Other details

4. Information Assets Involved

Please identify the information assets involved in the breach (e.g. server, USB devices, EHR application) and its location (e.g. IT Department, remote location)	

5. Information Involved

Please identify the type of information involved in the incident/breach	Type of data (e.g. personal information, personal health information)	Example of data elements (e.g. name, health card information, SIN, diagnoses information)	Format of data
			☐Encrypted ☐ Identifiable ☐De-identified ☐Statistical ☐Aggregated

Part II – Containment

6. Incident/Breach Containment

Please describe the immediate steps taken to contain the incident/breach (e.g. recovery of information, computer system shut down, locks changed).	Date & Time	Activities

Part III – Notification

7. Individuals and Organizations Notified

Please identify the individuals or organizations notified	Name of Organization	Date & Time	Activities

8. Internal Communications

Please identify the individuals/departments	Name/Title of the Individual/Department	Date & Time	Activities

notified of the privacy/security incident/breach			

Part IV – Investigation

9. Breach investigation

Investigation Summary	
Outcome of the Investigation	
Root cause of the breach (if known)	
Estimated number of individuals affected (e.g., patients, employees, external stakeholders)	
Potential harm to individuals & the Agency resulting from the breach (e.g., security risk, identity theft, financial loss, reputational damage)	
Risk of on-going or further exposure	

Part V – Remediation and Prevention

10. Please identify the remediation activities to prevent the incident from occurring again.

Remediation Recommendation	Schedule Date	Owner	Progress	Complete Date
Recommendations/Actions items are captured in the attached document.				YYYY/MM/DD

Report completion and approval

Report completed by:	Date //
Report reviewed by:	Date YYYY/MM/DD
Report approved by: Click here to enter text.	Date YYYY/MM/DD

Appendix C: Glossary

Acronym	Description
CDR	Clinical Data Repository
HICs	Health Information Custodians
HCP	Health Care Provider
PHI	Personal Health Information
PI	Personal Information
PHIPA	Personal Health Information Protection Act
SDM	Substitute Decision Maker
RCV	Regional Clinical Viewers