

# eHealth Ontario Site Support Guide

## Diagnostic Imaging Common Service

Reference Guide & Privacy and Security Procedures and Obligations

**Version: 1.0**

**Document Owner: Diagnostic Imaging Common Service**

All-inclusive account of procedures designed to assist health care organizations connect new users and sites to Diagnostic Imaging Common Service.

# Contents

<b>Introduction</b>	<b>4</b>
<b>1. Support</b>	<b>4</b>
1.1 Contacting the Service Desk for Support	4
1.1.1 How to reach eHealth Ontario service desk	4
1.1.2 Reporting an incident or creating a service request	5
1.1.3 Checklist to help expedite your ticket	6
1.1.4 Incident, service request and technical escalation process	6
1.1.5 Progress of your incident ticket	7
1.1.6 Client satisfaction	7
1.2 Support Processes	8
1.2.1 High level depiction of the DI Common Service support model	8
1.2.2 Client site helpdesk and application interface support group accountabilities	8
1.2.3 When should you call eHealth Ontario service desk?	8
1.2.4 When does eHealth Ontario service desk contact you?	9
1.2.5 When does the eHealth Ontario privacy/security office contact you?	9
1.2.6 Data quality assurance	9
<b>2. Operational Responsibilities for DI Common Service Data</b>	<b>9</b>
<b>3. Privacy and Security</b>	<b>10</b>
3.1 Patient Consent	10
3.1.1 Consent Management	10
3.1.2 Applying Consent Directives	10
3.1.3 Overriding a Consent Directive	12
3.2 Access Requests	13
3.2.1 Access requests made by patients for DI Common Service data	13
3.2.2 Requests from health care provider sites for audit logs for their site	14
3.3 Correction Requests	14
3.4 Privacy Complaints and Inquiries	15
3.5 Privacy-Related Questions from Health Care Provider Sites	15
3.6 Security Incident and Breach Management	15
3.7 Privacy Breach Management	16
3.8 Instructions for Health Care Providers	17
3.9 Instructions for Privacy Officers	17
<b>4. Site Support and Users</b>	<b>18</b>
4.1 Registering Users for Service	18
<b>Appendix A: Procedures for Communicating Sensitive Files via email</b>	<b>19</b>

---

<b>Appendix B: Sample Incident Report Form</b>	<b>24</b>
<b>Appendix C: Glossary</b>	<b>30</b>

## Introduction

The site support guide is a comprehensive document outlining various processes which were created to assist health care organizations when connecting new users and sites to Diagnostic Imaging (DI) Common Service. The guide provides information regarding support and maintenance as well as privacy and security procedures and obligations.

## 1. Support

eHealth Ontario will provide health care organizations with support in the various forms as outlined below:

### 1.1 Contacting the Service Desk for Support

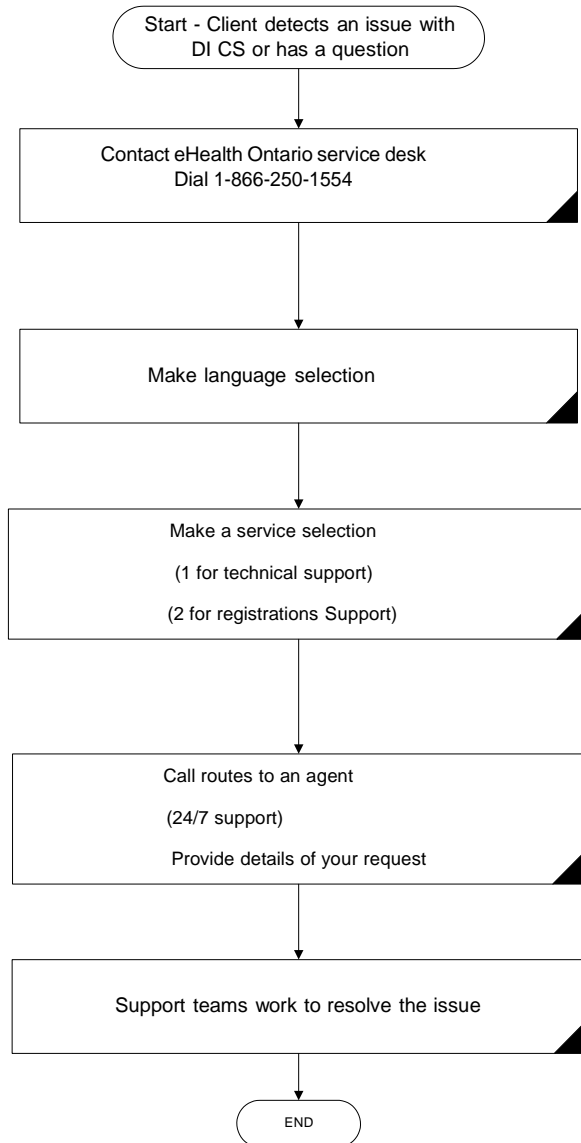
The eHealth Ontario service desk is the single point of contact for opening tickets for DI Common Service related issues.

#### 1.1.1 How to reach eHealth Ontario service desk

The eHealth Ontario Service Desk contact information is:

<p><u>Contact Information</u></p>	<p>Email:* <a href="mailto:servicedesk@ehealthontario.on.ca">servicedesk@ehealthontario.on.ca</a>            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.)</p> <p><i>*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.</i></p>
<p><u>Hours of Operation</u></p>	<p><b>Service Desk:</b> -7/24/365 to call to report all incidents.</p>

### Incident Management Support Flow



#### 1.1.2 Reporting an incident or creating a service request

**Phone** - The fastest way to report a high severity issue/incident (e.g. production is down or environment is severely degraded) is to contact eHealth Ontario service desk via telephone to open an incident or service request ticket.

**1-866-250-1554 – option 1**

**Email** - For service requests (i.e. medium and low severity issues). However, currently no service level agreements exist for incidents or service requests via email.

[servicedesk@ehealthontario.on.ca](mailto:servicedesk@ehealthontario.on.ca)

**1.1.3 Checklist to help expedite your ticket**

Be ready with the following details:

- Your name
- Your site location
- Your contact information, include backup contacts where applicable
- 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

**1.1.4 Incident, service request and technical escalation process**

Step 1 Open ticket	Contact eHealth Ontario to open a ticket at 1-866-250-1554 Choose service desk option from phone prompt
Step 2 Engagement with frontline service desk team	<p>A service desk agent works with you to identify issue(s) and commences troubleshooting steps</p> <p>A service desk agent may engage with an eHealth Ontario Technical Lead as necessary</p> <p>The support agent may request additional information from you to assist in troubleshooting process</p> <p>Once all action items have been completed, if the service desk agent cannot resolve the problem, it will be escalated to eHealth Ontario’s next level support team</p>
Step 3 Issue escalated to eHealth Ontario next level support team	<p>Incident is assigned to the next level of support</p> <p>Assigned next level of support contacts you</p> <p>The next level of support reviews incident and continues troubleshooting activities where required, other support teams are engaged to continue efforts to resolve your issue</p>

### 1.1.5 Progress of your incident ticket

**Updates** - Automated updates are provided as the incident is escalated among teams. Feel free to review the progress of your incident ticket by contacting the service desk anytime.

**Service request priority** - The incident priority is determined mutually by the support agent and you, the client.

**Incident ticket closure** - Your incident ticket will be closed 15 days after the incident ticket is resolved, no further troubleshooting is possible, or you authorize the eHealth Ontario support team to close the ticket. Your ticket will be closed if no feedback has been received after three attempts to contact you. During this time, you will receive three reminders with the final reminder stating that your ticket will be closed the next day.

### 1.1.6 Client satisfaction

eHealth Ontario service desk values and promotes client satisfaction. We welcome client feedback and encourage you to get involved through the following channels:

#### **Client satisfaction survey**

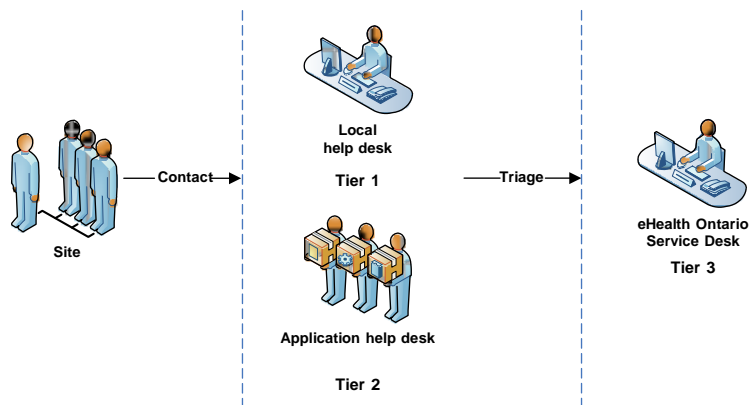
Upon closing a ticket, eHealth Ontario randomly selects incidents to be surveyed. You may receive a request to fill in an online questionnaire. We would very much appreciate it if you would help us ensure the quality of our service by completing a brief, five minute survey.

#### **General feedback**

If you wish to provide us your comments or suggestions, please email us anytime at [servicedesk@ehealthontario.on.ca](mailto:servicedesk@ehealthontario.on.ca).

## 1.2 Support Processes

### 1.2.1 High level depiction of the DI Common Service support model



### 1.2.2 Client site helpdesk and application interface support group accountabilities

When any issues with the interface used to access DI Common Service data are detected, your local site helpdesk along with your site's application interface support teams provide support by assisting in:

- troubleshooting any issues;
- providing a resolution where possible;
- determining potential impact of the issues; and
- escalating to the appropriate support groups and/or eHealth Ontario service desk

### 1.2.3 When should you call eHealth Ontario service desk?

Contact the eHealth Ontario service desk when you have information on/questions regarding the following issues:

- Requesting assistance with troubleshooting DI Common Service public key infrastructure PKI certificate issues
- Requesting assistance with troubleshooting service related interface issues
- Reporting a DI Common Service application error
- Reporting missing results in DI Common Service
- Reporting data quality issues in DI Common Service
- Reporting a privacy breach



When requesting information from eHealth Ontario about DI Common Service regarding questions about:

- DI Common Service functionality
- Privacy and security of personal health information

#### 1.2.4 When does eHealth Ontario service desk contact you?

- For clarification regarding an incident or request you have reported
- To notify you of maintenance activities at our site that may impact service
- To report a failure in the DI Common Service application
- To provide information regarding our release dates and application improvement activities

#### 1.2.5 When does the eHealth Ontario privacy/security office contact you?

- For requesting additional information to fulfill DI Common Service access requests
- For incident management purposes

#### 1.2.6 Data quality assurance

Sites are required to perform regular data quality checks to ensure that data being sent to DI Common Service is accurate and complete. The accuracy of data within DI Common Service is important to eHealth Ontario. Should you find missing results or incorrect data; please notify us by contacting the service desk.

The following information should be supplied to assist us with the investigation for missing or incorrect data:

- 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 DI result accession #
- The information that is missing (if reporting a single missing result)
- If the DI result information is incorrect, provide details around why this is so

## **2. Operational Responsibilities for DI Common Service Data**

Under the Personal Health Information Protection Act, 2004 (PHIPA), eHealth Ontario is responsible for keeping an electronic record of all accesses to DI Common Service 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. eHealth Ontario may be asked to provide an audit report on these access logs.

### **3. Privacy and Security**

#### **3.1 Patient Consent**

##### **Quick Tip**

The EHR system gives patients, or their substitute decision maker, the option to allow or restrict access to patient data. Should a patient choose to place a consent directive in the DI Common Service, he /she must fill out the EHR Consent form at <http://www.ehealthontario.on.ca/en/initiatives/resources> 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.

##### **3.1.1 Consent Management**

The electronic health record (EHR) gives patients or their substitute decision maker the option to allow or restrict access to patient data within DI Common Service. If a patient restricts access to his / her data by applying a consent directive, providers querying DI Common Service 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 or allow the following:

- All of a patient's records (Global/Domain Consent Directive) <sup>1</sup>
- A particular report or image (Record-level Consent Directive)
- All records from a particular organization (HIC-Agent Consent Directive).

##### **3.1.2 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 reinstate access (remove the restriction), the HIC should:

---

<sup>1</sup> The Domain Consent Directive allows a person to withhold or withdraw consent for one but not all of the EHR repositories. At this time, there is only one EHR repository; therefore the Domain and the Global Consent Directives are the same until other repositories are added.

- Capture the consent directive information on the EHR Consent Form at <http://www.ehealthontario.on.ca/en/initiatives/resources> , and
- 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/en/initiatives/resources>, and / or contact us directly at 416-946-4767.

In all instances, eHealth Ontario will apply consent directives within seven days of verifying the identity of the patient 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 you cannot notify the patient, let us eHealth Ontario will notify him / her on your behalf at your direction.

### 3.1.3 Overriding a Consent Directive<sup>2</sup>

#### Quick Tip

DI Common Service permits a health care provider to temporarily override a patient's consent directive. If you perform a consent override, you will be asked by eHealth Ontario to confirm the purpose of the override, and to subsequently notify the patient of the override occurrence. An override can only be performed at the express consent of a patient. A consent directive override will be in effect for four hours.

DI Common Service permits a health care provider in special cases to temporarily override a patient's consent directive.

Providers can temporarily override a consent directive under the following circumstance:

- With the express consent from the patient or the patient's substitute decision maker.

A temporary override will be logged in DI Common Service, along with the identity of the overriding health care provider. The override will be in effect for no more than four hours.

eHealth Ontario will notify the HIC if one of his / her agents overrides the consent directive. Once contacted by eHealth Ontario, it is the responsibility of the HIC to:

1. Investigate the override to ensure it was for one of the reasons stated above, and
2. Notify the patient of the override at the first opportunity.<sup>3</sup>

---

<sup>2</sup> Providers accessing DI Common Service via the ClinicalConnect Viewer will not have the functionality to perform a consent directive override until ClinicalConnect is fully integrated with the consent management solution.

<sup>3</sup> For more information on what to include in this notice to the patient, please see the *EHR Consent Management Policy* at <http://www.ehealthontario.on.ca/en/initiatives/resources>. If you cannot notify the patient, contact eHealth Ontario and we will notify the patient on your behalf.

For details on what to include in this notice to the IPC, review our *EHR Consent Management Policy* at <http://www.ehealthontario.on.ca/en/initiatives/resources>.

## 3.2 Access Requests

### 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 416-946-4767 as soon as possible to make the request.

### 3.2.1 Access requests made by patients for DI Common Service data

Under PHIPA, patients or their substitute decision makers have a right to access data held by a HIC. When a provider receives a request for records he / she has collected, created and / or contributed, he / she must follow Part V of PHIPA as well as all its related internal policies, procedures and practices before responding.

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

- Notify the individual that the request for access involves PHI not within his / her custody or control, and
- Direct the individual to contact eHealth Ontario at 1-866-250-1554 or online at <http://www.ehealthontario.on.ca/en/contact>

As per the *EHR Access and Correction Policy* at <http://www.ehealthontario.on.ca/en/initiatives/resources> eHealth Ontario may seek assistance from the HIC when responding directly to a request for access.

### 3.2.2 Requests from health care provider sites for audit logs for their site

When a provider receives a request for access directly from an individual related to audit logs for records stored in DI Common Service, the HIC is required to:

- Notify the individual that he / she is unable to process the request for access, and
- Direct the individual to contact eHealth Ontario at 1-866-250-1554 or online at <http://www.ehealthontario.on.ca/en/contact>

### 3.3 Correction Requests

When a HIC receives a request for correction directly from an individual related to health records that were created and contributed to DI Common Service solely by that HIC, he / she is required to follow Part V of PHIPA and its internal policies, procedures and practices.

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 his / her 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 by another HIC or by more than one HIC, he/she must respond no later than two days upon receiving the request by:

- Notifying the individual 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 through <http://www.ehealthontario.on.ca/en/contact>.

eHealth Ontario will coordinate the response to this request, and may seek assistance from the HIC(s) when responding to the individual.

### 3.4 Privacy Complaints and Inquiries

#### Quick Tip

When an individual submits an inquiry or complaint related to DI Common Service, 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 DI Common Service, or his / her agents and / or service providers, the HIC is required to follow his / her own internal policies, procedures, and practices.

When a HIC directly receives an inquiry/complaint related solely to DI Common Service 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 online through <http://www.ehealthontario.on.ca/en/contact>.

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

### 3.5 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 individual access requests, consent obligations or incident/breach management processes, contact eHealth Ontario at 1-866-250-1554.

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

### 3.6 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 your organization, users at your organization, or employees, agents or service providers of your 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 DI Common Service.

### **3.7 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* at [http://www.ehealthontario.on.ca/en/initiatives/resources\\_describes](http://www.ehealthontario.on.ca/en/initiatives/resources_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 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 DI Common Service, 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 DI Common Service, 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* at <http://www.ehealthontario.on.ca/en/initiatives/resources>.

### 3.8 Instructions for Health Care Providers

If you become aware of, or suspect, a security incident or breach of DI Common Service or data by you or any of your employees, agents, or service providers, you must immediately report it to your privacy office. If you do not have a privacy office or you are unable to reach your privacy office or support team to report a breach, contact our 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.

### 3.9 Instructions for Privacy Officers

If you become aware of, or suspect, an incident or breach related to DI Common Service 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 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.

## **4. Site Support and Users**

### **4.1 Registering Users for Service**

Users of the DI Common Service access data via various interfaces. For some sites, access to the interfaces is managed locally; this includes login credentials assigned to users. Users of eHealth Ontario's web viewer r require a ONE® ID login ID. To obtain your ONE ID, contact your Local Registration Authority to complete a registration form.

## **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.

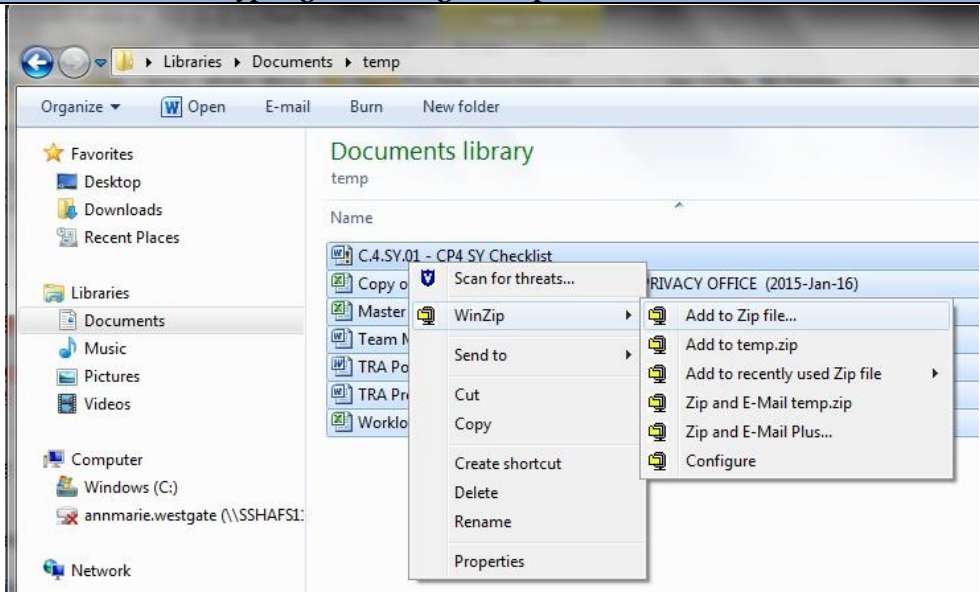
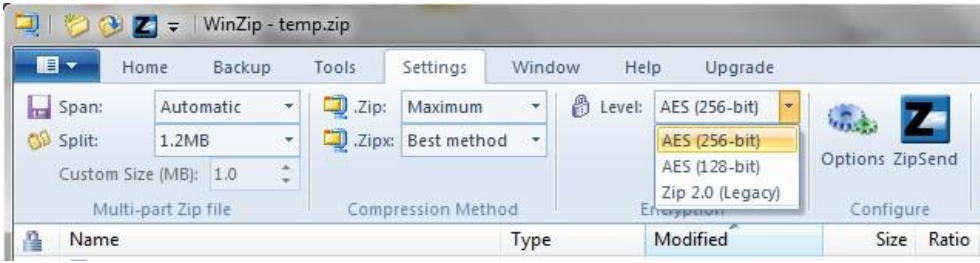
eHealth Ontario’s limit on email attachments is 10 MB per email.

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**

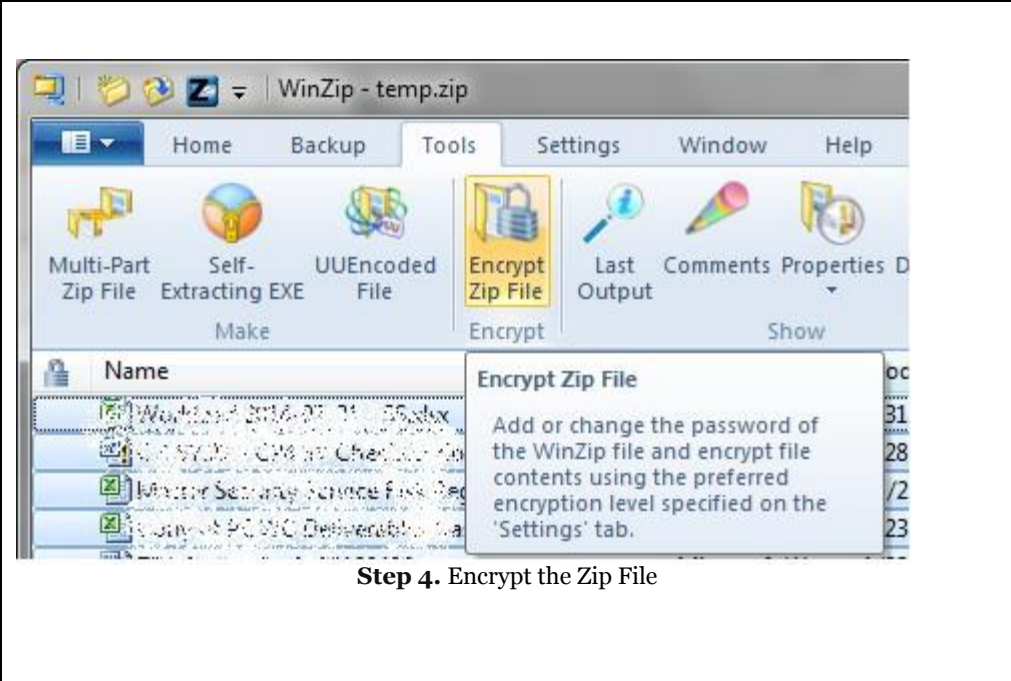
**WinZip 16.0** standard versions are eHealth Ontario’s suggested encryption tool.

<b>Encrypting Files using WinZip</b>	
<p><b>Step 1. Create Archive</b> Open the file location.</p> <p>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 <b>Add to Zip file...</b></p> <p>Assign the file name you wish to use.</p>	 <p style="text-align: center;"><b>Step 1. Add files to an archive</b></p>
<p><b>Step 2. Open the Archive:</b> Double click on the zip file to open the archive.</p> <p><b>Step 3. Choose a stronger encryption mechanism</b> Use AES 256-bit encryption. In the <b>Settings</b> tab, ensure the encryption level selected is <b>AES (256-bit)</b>.</p>	 <p style="text-align: center;"><b>Step 3 Choose an encryption mechanism</b></p>

**Encrypting Files using WinZip**

**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.

### **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 - <input type="checkbox"/> Yes <input type="checkbox"/> No Privacy Incident - <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
	<input type="checkbox"/> Policy infraction <input type="checkbox"/> Agreement infraction <input type="checkbox"/> Unauthorized collection <input type="checkbox"/> Unauthorized use <input type="checkbox"/> Unauthorized disclosure <input type="checkbox"/> Unauthorized disposal <input type="checkbox"/> 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
			<input type="checkbox"/> Encrypted <input type="checkbox"/> Identifiable <input type="checkbox"/> De-identified <input type="checkbox"/> Statistical <input type="checkbox"/> 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

9. Individuals and Organizations Notified

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

Internal Communications

Please identify the individuals/departments notified of the privacy/security incident/breach	Name/Title of the Individual/Department	Date & Time	Activities

Part IV – Investigation

11. 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

12. 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 2013/07/10
Report reviewed by:	Date YYYY/MM/DD
Report approved by: Click here to enter text.	Date YYYY/MM/DD

---

## Appendix C: Glossary

---

<b>Acronym</b>	<b>Description</b>
DI	Diagnostic Imaging
HICs	Health Information Custodians
PHI	Personal Health Information
PI	Personal Information
PHIPA	Personal Health Information Protection Act

## **NOTICE AND DISCLAIMER**

All rights reserved. No part of this document may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of eHealth Ontario.

eHealth Ontario and all persons involved in the preparation of this document disclaim any warranty as to accuracy or currency of the document. This document is provided on the understanding and basis that none of eHealth Ontario, the author(s) or other persons involved in its creation shall be responsible for the accuracy or currency of the contents, or for the results of any action taken on the basis of the information contained in this document or for any errors or omissions contained herein. No one involved in this document is attempting herein to render legal, privacy, security, or other professional advice.