Ontario
eHealth Ontario

eHealth Ontario Site Support Guide

Version 5.2

Reference Guide

This guide will assist sites accessing OLIS with information around processes and contacting eHealth Ontario for support.

www.eHealthOntario.on.ca

Contents

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 the creation of this document 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.

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 the Ontario Laboratories Information System (OLIS). The guide provides information regarding support and maintenance as well as privacy and security procedures and obligations.

1. Support

eHealth Ontario will be providing health care organizations with support in the various forms that have been outlined below:

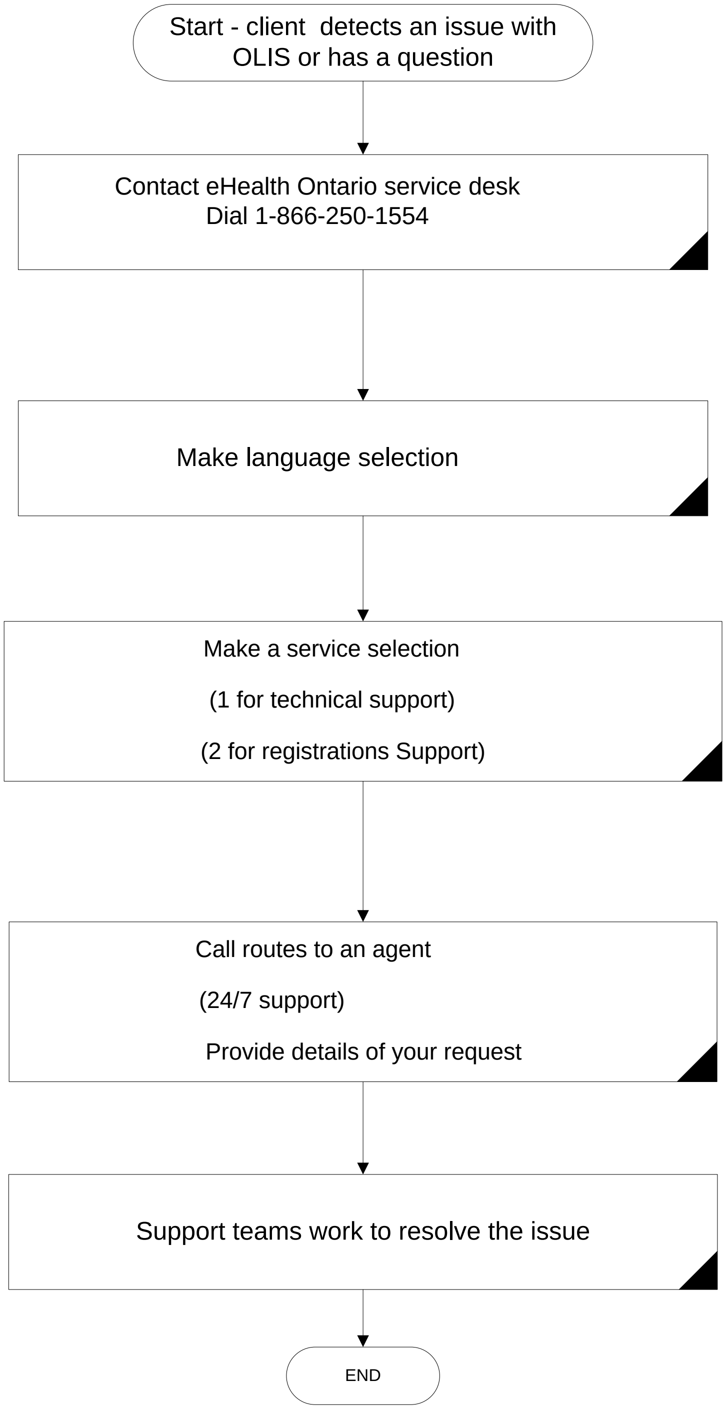
1.1 Contacting the Service Desk for Support

The eHealth Ontario service desk is the single point of contact for making service requests for OLIS related issues. The eHealth Ontario service desk is staffed 24/7 to respond to and service any requests made.

1.1.1 How to reach eHealth Ontario service desk

Service desk – open 7 days per week 24hrs per day
(905) 826 – 5551
Toll Free: 1-866-250-1554
Option 1 – Technical support
Option 2 – Registration support
servicedesk@ehealthontario.on.ca
registration.agents@ehealthontario.on.ca
For a list of other contacts within eHealth Ontario, visit:
http://www.ehealthontario.on.ca/en/contact

7/24 hr service request support flow



Start - client detects an issue with OLIS or has a question

Contact eHealth Ontario service desk
Dial 1-866-250-1554

Make language selection

Make a service selection

(1 for technical support)

(2 for registrations Support)

Call routes to an agent

(24/7 support)

Provide details of your request

Support teams work to resolve the issue

END

1.1.2 Creating a service request

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

1-866-250-1554 – option 1

Email - is best for medium and low severity issues.

servicedesk@ehealthontario.on.ca

1.1.3 Checklist to help expedite your service request

- Your name
- Your site location
- Your contact information, include backup contacts where applicable
- Indicate what eHealth Ontario service you are calling about e.g. OLIS web viewer
- Indicate the eHealth Ontario service environment affected e.g. production or conformance self- testing (CST)
- 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 Service request and technical escalation process

Step 1 Service request	You contact eHealth Ontario to open a service request Choose service desk option from phone prompt
Step 2 Engagement with frontline service desk team	A service desk agent works with you to identify issue(s) and commences troubleshooting steps A service desk agent may engage with an eHealth Ontario Technical Lead as necessary The support agent may request additional information from you to assist in troubleshooting process Once all action items have been completed, if the service desk agent cannot resolve the problem and no progress is being made on the incident, it may be escalated to eHealth Ontario’s next level support team

Step 3 Issue escalated to eHealth Ontario next level support team	Incident is assigned to the next level of support Assigned next level of support contacts you 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

1.1.5 Progress of your service request

Updates - To review the progress of your service request please contact the service desk. Additionally, automated updates are provided as the service request is escalated among teams.

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

Service request closure - Your service request will be closed 15 days after the service request ticket is resolved, no further troubleshooting is possible, or you authorize the eHealth Ontario support team to close the request. Your request 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 request 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

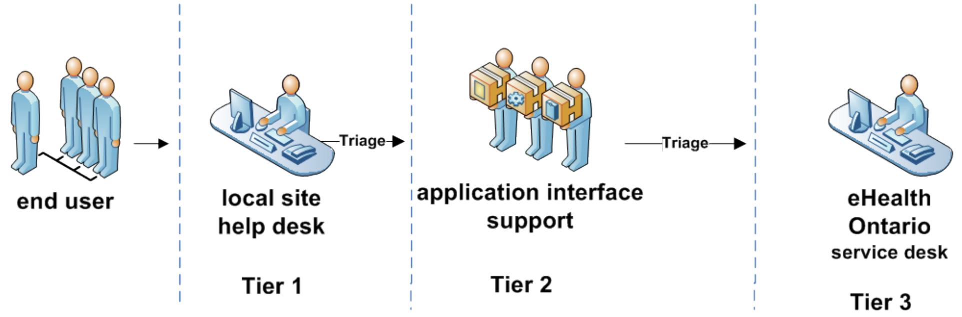
Upon closing a service request, eHealth Ontario randomly selects incidents to be surveyed. You may receive a request to fill in an online questionnaire. We would very much appreciate it if you would help us ensure the quality of our service by completing a brief, five minute survey.

General feedback

If you wish to provide us your comments or suggestions, please email servicedesk@ehealthontario.on.ca.

1.2 Support Processes

1.2.1 High level depiction of the OLIS support model



1.2.2 Client site helpdesk and application interface support group accountabilities

When any issues with the interface used to access OLIS data are detected, local site helpdesk along with the application interface support teams at each site provides support for sites users and will assist in:

- troubleshooting the 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 OLIS public key infrastructure PKI certificate issues
- Requesting assistance with troubleshooting OLIS related interface issues
- Reporting an OLIS application error
- Reporting missing laboratory results in OLIS
- Reporting data quality issues with laboratory results in OLIS
- Reporting a privacy breach

When requesting information from eHealth Ontario, for example when you have questions about OLIS:

- Questions about OLIS functionality
- Questions about test codes found in OLIS

- Questions about 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 OLIS application
- To provide information regarding our release dates and application improvement activities

1.2.5 When does the eHealth Ontario privacy office contact you?

- For requesting additional information to fulfill OLIS 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 OLIS is accurate and complete. The accuracy of data within OLIS is important to eHealth Ontario. Should you find missing lab reports or incorrect data, for example missing units of measure in the OLIS reports viewed; 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 this on behalf of <physician's office, hospital, lab, department>
- The name of the lab that submitted the result
- The lab report or accession #
- The test type that is missing (if reporting a single missing result)
- The date and time that the specimen was collected
- If the lab information is incorrect provide details around why you feel this information is incorrect "**do not provide any personal health information (PHI) to the service desk**"

2. Operational Responsibilities for OLIS Data

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

2.1 Logical Deletion of OLIS Data

eHealth Ontario has the ability to logically delete corrupted lab records. Each time this occurs, eHealth Ontario will provide the following information:

- Submitter – the laboratory identifier
- Order ID – this unique ID identifies a lab report
- Assigning authority – identifies type of facility: lab, hospital,
- Corresponding ID number – unique DN or laboratory identifier
- Insert date – date and timestamp that lab report was inserted into OLIS
- Include or exclude flag
- Deletion date

2.2 Consent Override Reporting Process

Patients may choose to apply an express consent override to OLIS data to temporarily remove the block on their personal health information. Each time this occurs, eHealth Ontario will send a report directly to each patient detailing the override activity that was performed on their OLIS record.

Where the request to override an OLIS consent directive comes from a patient's substitute decision maker (SDM), you must record the name of the SDM and their relationship to the patient in every instance.

2.3 Tactical Privacy Audit Solution (TPAS) Report Transfer Process

eHealth Ontario may be asked to produce reports on access to OLIS information received from Health Information Custodians (HICs) (providers/institutions) or patients. eHealth Ontario fulfills these requests on behalf of the Ministry of Health and Long-Term Care (MOHLTC)). eHealth Ontario refers to logs or reports produced to assist in responding to access requests as "tactical privacy audit solution (TPAS)" logs or alternatively, as TPAS reports.

There are two (2) kinds of access requests that eHealth Ontario can receive in respect to OLIS:

- An access request made by a HIC for OLIS access audit logs for that HIC's facility (e.g. hospital, CCAC, physician practice)
- An access request made by a patient to a HIC for:
  - What information is contained in OLIS about me?; and/or
  - Who has accessed my information in OLIS (i) in general; or (ii) from a particular facility?

3. Privacy and Security

3.1 Patient Consent

3.1.1 Background

As custodians of patient personal health information (PHI), health care providers working at sites have obligations under PHIPA and Ontario Regulation 329/04 (the regulation).

Patient consent model

OLIS data has a consent directive capability, which gives patients or their substitute decision maker (SDM) the option to restrict access to patient data in OLIS.

A patient may restrict access to either:

- All of his/her laboratory test results in OLIS; or
- A particular test (to be specified at the time the test is conducted).

In other words, if a patient restricts access to his/her results in OLIS, health care providers querying OLIS data will not be able to access any patient information that has been, or will be, submitted into OLIS, except the providers named on the lab order.

3.1.2 Overriding a consent directive

In special cases, with consent from the patient or the patient's SDM, the patient directive restricting access to the test may be overridden by a provider.

Such an override may be logged in the site's application interface, along with the identity of the overriding health care provider.

Some client site application interface enables users to override a consent directive applied to data within their application interface system where; (a) there is a clinical/emergency requirement; or (b) access has been granted directly by a patient or the patient's SDM (express consent). 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 express consent.

Therefore, some sites accessing OLIS are permitted to override a consent directive applied to OLIS data only where permission to do so has been expressly authorized by the patient or the patient's SDM prior to performing the consent directive override. 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 that site's) agreement with eHealth Ontario, and will be subject to the remedies available under the agreement.

3.1.3 Applying consent directives to OLIS data

If a patient contacts a health care provider at your site and wishes to place a restriction on access to his/her information in OLIS, or wishes to reinstate access (remove the restriction), please ask the patient to call Service Ontario at 1-800-291-1405 (TTY 1-800-387-5559) to apply/change the consent directive.

3.2 Access Requests

3.2.1 Access requests made by patients for OLIS data

Under PHIPA, patients or their SDMs have a right to access the patient's data held by a HIC about the patient. There are two types of access requests that a patient can make to the MOHLTC, as custodian of the OLIS data:

- What information is contained in OLIS about me; and/or
- Who has accessed my information in OLIS (i) in general; or (ii) from a particular facility.

As the MOHLTC is the custodian of OLIS data, only the MOHLTC can respond to an individual's access request.

If a patient requests OLIS data, or inquires as to whom in Ontario has viewed the patient's OLIS data, refer the individual to the MOHLTC access and privacy office at the following address:

Attention: Freedom of Information and Privacy Coordinator
Access and Privacy Office
Ministry of Health and Long-Term Care
6th Floor, 5700 Yonge Street
Toronto ON, M2M 4K5
416-327-7040
generalapo@ontario.ca

Note: Where a patient has requested information from a particular HIC about who has accessed their OLIS data from that organization/facility, it will be the responsibility of that HIC to respond to the request. A description of how a HIC may obtain OLIS audit logs to respond to such a request is provided in section 3.2.2 below**.**

3.2.2 Requests from health care provider sites for OLIS audit logs (for their site)

Sites (lead physician or privacy officer at a site) may require a record of who from their organization accessed OLIS data. The site may request an audit log from eHealth Ontario which will provide them with a record of the following:

- By facility request – a log of all users at the site who have accessed OLIS data in the timeframe set out in the request.
- By user request –a log of all accesses to OLIS data by a particular user from the site, within the timeframe set out in the request.

If site requires an OLIS audit log, the site's lead physician or privacy officer must contact eHealth Ontario's service desk at 1-866-250-1554 to make the request for the audit logs for that site.

eHealth Ontario service desk will open a service request ticket to fulfill the request. A representative from eHealth Ontario's privacy office will call the contact person on record from the site profile form submitted for that site to confirm the type of report requested. eHealth Ontario will then proceed with fulfilling the site's request for OLIS audit logs.

3.3 Inquiries and complaints received by Health Care Provider sites with respect to eHealth Ontario or OLIS data

If a health care provider receive any complaints or inquiries from users or patients with respect to OLIS data, the site must report the inquiry or complaint to eHealth Ontario's service desk (at the contact information below) as soon as reasonably possible after receipt, and work with eHealth Ontario to investigate and respond to complaints that arise with respect to OLIS data.

The contact information for eHealth Ontario's service desk is:

1-866-250-1554
servicedesk@ehealthontario.on.ca

If a health care provider receives a complaint or inquiry relating to eHealth Ontario in general (i.e. not related to OLIS data), or related to eHealth Ontario's privacy policies and procedures, the site should advise the individual to submit their complaint, concerns or inquiry by telephone, email, fax or mail to the Chief Privacy Officer:

eHealth Ontario Privacy Office
P.O. Box 148
777 Bay Street, Suite 701
Toronto, ON M5G 2C8
Fax: (416) 586-6598
Email: privacy@ehealthontario.on.ca
Telephone: (416) 946-4767

3.4 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, please contact the eHealth Ontario privacy operations department, at privacyoperations@ehealthontario.on.ca.

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

3.5 Privacy and Security Incident Management

An eHealth Ontario privacy and security incident management process was created to address any privacy breaches reported to eHealth Ontario. The process for reporting a privacy or security incident/breach is outlined below and covers the following scenarios:

i) Incidents or breaches detected by helpdesk contacts at a Health Care Provider sites

ii) Incidents or breaches detected by Users at Health Care Provider sites

iii) Incidents or breaches detected by eHealth Ontario which have an impact Health Care Provider sites

3.5.1 A privacy incident is:

- A contravention of the privacy policies, procedures or practices implemented by a health care provider site and eHealth Ontario, where this contravention does not constitute non-compliance with applicable privacy law.
- A contravention by a health care provider site of any agreements entered into between eHealth Ontario and that health care provider site, where the contravention does not constitute non-compliance with applicable privacy law.
- A contravention of agreements entered into between eHealth Ontario and a health care provider site accessing OLIS via that site’s application interface, where the contravention does not constitute non-compliance with applicable privacy laws.
- A suspected privacy breach

3.5.2 A privacy breach is:

- The collection, use or disclosure of Personal Health Information (PHI) in contravention of PHIPA and its regulation;
- The collection, use or disclosure of Personal Information (PI) in contravention of Freedom of Information and Protection of Privacy Act (FIPPA) and its regulations; or
- Any other circumstances where there is an unauthorized or inappropriate collection, use or disclosure, copying, modification, retention or disposal of PI/PHI including theft and accidental loss of data.

3.5.3 A security incident is:

- A failure to comply with the security policies, procedures, practices or requirements;
- Unauthorized access, use or probing of information resources;
- Unauthorized disclosure, destruction or modification of information; or
- A contravention of agreements by a health care provider site and its users or eHealth Ontario.
- An attempted, suspected or actual security compromise.
- Waste, fraud, abuse, theft, loss of or damage to resources.

Health care provider sites and eHealth Ontario are expected to train employees, agents and service providers involved in the incident management process set out below on their roles and responsibilities with respect of this process.

Health care provider sites are also required to communicate to their users the proper procedure for reporting confirmed or suspected privacy incidents/breaches involving the OLIS data accessed by that site in accordance with the steps contained in this document.

3.5.4 Privacy or security incidents/breaches detected by a health care provider site or its users

1. Upon detecting a privacy or security incident/breach the users must immediately contact their local helpdesk and /or in-house privacy officer.

2. Health care provider site designated contact(s) (authorized site contact, helpdesk contact and/or site privacy officer) “the contact” connects with the eHealth Ontario service desk by telephone at 1-866-250-1554, immediately upon becoming aware of an actual or suspected privacy/security incident involving or potentially impacting OLIS data; the health care provider site’s helpdesk or privacy officer in cooperation with eHealth Ontario is responsible for containing such privacy/security incidents and documenting any containment and/or remediation activities undertaken. No PI/PHI should be included in this documentation.
3. For an OLIS related privacy or security incident/breach, the contact is not to contact any patient or substitute decision maker directly, unless expressly directed to do so by eHealth Ontario, in writing.
4. The eHealth Ontario service desk will open incident management ticket to track the progress of the investigation. eHealth Ontario will engage the contact to receive an update on the investigation by their site.
5. If required, eHealth Ontario will request a copy of any related information from the client site to assist in eHealth Ontario’s own incident management activities. The logs and/or any other sensitive information should be sent to eHealth Ontario as an encrypted document (WinZip) via an email. The procedure is noted in Appendix A.
6. Health care provider site must complete all remediation activities as directed by eHealth Ontario and implement preventative measures to avoid recurrence of the incident and ensure the privacy and security of the OLIS data.
7. The contact may be asked to provide eHealth Ontario with a copy of the incident report upon closure of the privacy or security incident/breach.
8. The contact is expected to destroy the incident investigation materials, after the incident investigation report is sent to eHealth Ontario, and after eHealth Ontario has communicated back to them that the incident/breach is closed.

3.5.5 Privacy or security incidents/breaches detected by a health care provider site and reported directly to eHealth Ontario

1. The health care provider site user contacts eHealth Ontario directly to report a suspected or actual privacy or security incident/breach.
2. The service desk will open and incident management ticket to track the progress of the investigation.

3. eHealth Ontario will engage the health care provider site contact to inform them of the suspected/actual incident/breach.
4. The health care provider site contact will assist eHealth Ontario in containing and investigating a suspected/actual privacy or security incident/breach.
5. If required, eHealth Ontario will request a copy of any required documentation from the client's site to assist in investigation and/or communication.
6. The logs and/or any other sensitive information should be sent to eHealth Ontario as an encrypted document (WinZip) via an email. The procedure is noted in Appendix A.
7. The health care provider site contact must complete all remediation activities as directed by eHealth Ontario to prevent recurrence of the incident or to ensure the privacy and security of the OLIS data. The site may be asked to provide eHealth Ontario with a copy of the incident report upon closure of the privacy or security incident/breach.
8. The health care provider site contact is expected to destroy the incident investigation materials, after the incident investigation report is sent to eHealth Ontario, and after eHealth Ontario has communicated back to them that the incident is closed.

3.5.6 eHealth Ontario detected privacy/security breach/incident

1. A privacy or security incident/breach is detected by eHealth Ontario.
2. The service desk is notified of the incident.
3. The service desk opens an incident management ticket to track the progress of the investigation.
4. eHealth Ontario contains and investigates the incident. If during the investigation it is determined that that the privacy/security incident has an impact on any health care provider site, eHealth Ontario notifies the health care provider site contact of the incident.
5. The health care provider site contact assists eHealth Ontario in containing and investigation and resolution of the incident.

The health care provider site contact must complete all remediation activities as directed by eHealth Ontario to prevent recurrence of the incident.

3.5.7 What to provide to eHealth Ontario's service desk when reporting a privacy/security incident?

When reporting a confirmed or suspected privacy or security incident/ breach to eHealth Ontario, the following information may be requested from the contact:

1. Description of the situation and condition that led to the incident.

Note: *It is extremely important that you do not disclose any patient personal health information and/or personal information to the eHealth Ontario service desk agent when reporting a suspected or confirmed privacy breach*.

2. Who was involved (name and role)?
3. Where did the incident happen?
4. When and at what time was the incident noticed?
5. If possible, describe how the incident was detected.
6. If possible, provide information on the most likely cause - for example:
    - Human error
    - Negligence
    - Technical failure, caused by failure of an application or system to maintain privacy
    - Process failure, caused by not following a process
    - Willful wrongdoing
    - Act of nature
7. Describe the type of personal information/personal health information involved in the incident.

Note: *It is extremely important that you do not disclose any patient personal health information and/or personal information to the eHealth Ontario Service Desk agent when reporting a suspected or confirmed privacy breach*.

8. If possible, list measures taken to contain the breach or any risks that could eventually result in a breach.
9. If possible, list any corrective measures taken or additional controls applied.

B. Site Support and Users

4. OLIS Setup Requirements

4.1 Registering site support contacts for service (Technical/Helpdesk Contacts/Privacy Officers)

A privacy officer/contact person will be assigned by each site with access to OLIS data, to liaise with eHealth Ontario for incident management purposes. The client site profile form, referenced below, can be used to submit contact information for each site that accesses OLIS.

1. All sites provisioned to access OLIS must fill out a client site profile form located in appendix C and send it to the eHealth Ontario service desk at: **registration.agents@ehealthontario.on.ca**
    a. The form captures contact information (i.e. name, site/organization, contact number/email) of the designated individual.
    b. Distribute the form to each site's helpdesk and advise the contact person at the site to complete the form and send it to the eHealth Ontario service desk at the email address provided above. This form can be used to capture updates to sites' support teams and authorized contacts when they change

2. The privacy officer/contact person at all sites will have WinZip installed to securely transfer sensitive information including PI/PHI via email to eHealth Ontario. Instructions for using WinZip are included in Appendix A of this guide.

4.2 Registering Users for Service

Users of the OLIS service access OLIS data using various interfaces. For some sites, access to the interfaces used to view data is managed locally; this includes login credentials assigned to users. eHealth Ontario has a web viewer to the OLIS data, users who access OLIS data via our OLIS web viewer will require a ONE ID login ID. To obtain a ONE ID, users can contact their Local Registration Authority (LRA) to complete a registration form. Registration forms can also be found at www.ehealthontario.ca/RA locate the form labelled OLIS – Individual Registration and Service Enrolment Form (HC Providers).

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 section four 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 (PI) and/or personal health information (PHI).

If sending sensitive information over email is an ongoing business process, considerations should be made to automate the process and use an enterprise mechanism to securely transfer the information other than outlined in this guide.

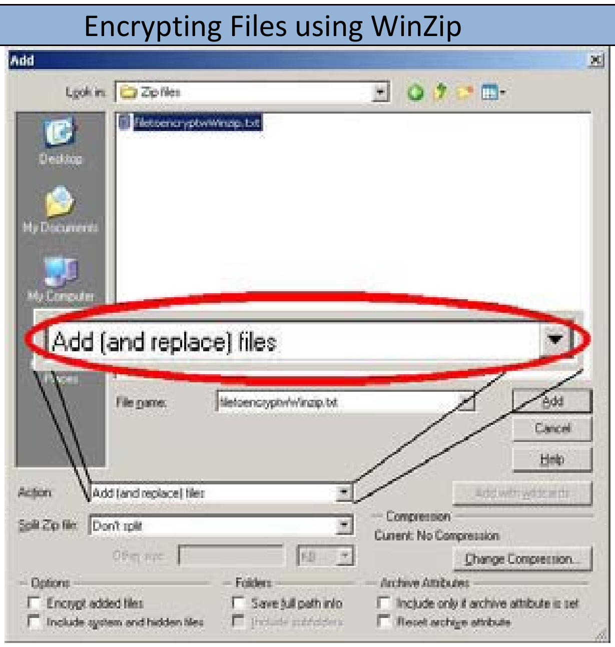
The limit on email attachments has been predetermined at 10 MB per email at eHealth Ontario.

For further assistance please contact eHealth Ontario security services.

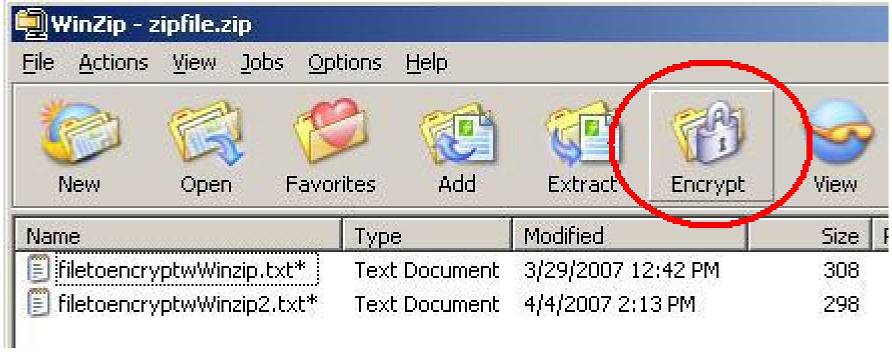
Instructions to file encryption and password creation

Use of WinZip encryption software

This guide has been written for ***WinZip 11.2*** standard versions and is the suggested encryption tool.

Encrypting Files using WinZip	
Step 1. Open the application. Create a new archive* and save in a working folder. <u>Add files to an archive:</u> Navigate to the folder where the sensitive files are. Choose to add files to an archive rather than move files to an encrypted archive. When a file is moved to an archive, it appears that the original copy of the file is deleted, but the contents of the file still exist in the computer's memory. Adding files to an archive is safer because this leaves the original file intact, making it obvious to the user that the contents of the plain file still exist on the computer. *An archive is a file document.	 Add Desktop My Documents My Computer Add Cancel Help Add with wildcards Change Compression... Options Folders Archive Attributes Look in: Zip files filetoencryptwWinzip.txt Add (and replace) files File name: filetoencryptwWinzip.txt Action: Add (and replace) files Split Zip file: Don't split Other size: KB Compression Current: No Compression ☐ Encrypt added files ☐ Include system and hidden files ☐ Save full path info ☐ Include subfolders ☐ Include only if archive attribute is set ☐ Reset archive attribute **Fig.1** Add files to an archive

Step 2. Encrypt the entire archive:
Encrypt the entire archive after all files have been added.
Click on the “Encrypt” icon.



Name	Type	Modified	Size
filetoencryptwWinzip.txt*	Text Document	3/29/2007 12:42 PM	308
filetoencryptwWinzip2.txt*	Text Document	4/4/2007 2:13 PM	298

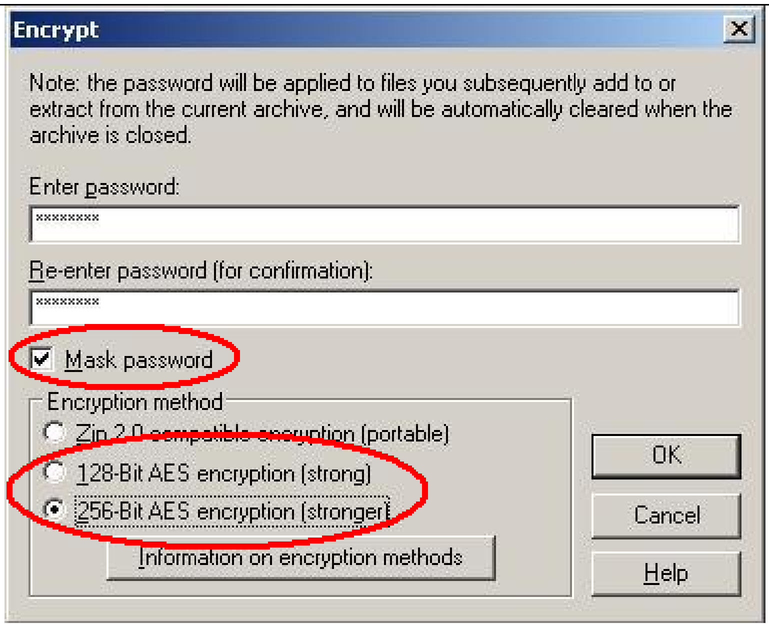
Fig.2 Encrypt the archive

Step 3. Choose a stronger encryption mechanism
Use 256-bit AES encryption. Do not use Zip 2.0 compatible encryption.

Step 4. Create a strong password (See section 4.1 below for details)
Enter a strong password when the **Encrypt** dialog displays and choose to mask the password as shown in Fig.3.

Step 5. Temporarily save the encrypted extract in a folder on your computer or a network share drive.

Note: Once the recipient confirms they are able to open the file, the local file can then be deleted.



Note: the password will be applied to files you subsequently add to or extract from the current archive, and will be automatically cleared when the archive is closed.

Enter password: ********

Re-enter password (for confirmation): ********

☑ Mask password

Encryption method
○ Zip 2.0 compatible encryption (portable)
○ 128-Bit AES encryption (strong)
● 256-Bit AES encryption (stronger)

Fig.3 Choose an encryption mechanism

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 problem of 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

- It is important to create a strong password with which 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. It is important to make sure that the email has been sent to the correct recipient. When the email is received, the requester should call the sender to acquire the password.

Password sharing

Passwords must be securely shared when being sent to eHealth Ontario from a health information custodian.

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 at their telephone number
- 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 Incident/Breach Management Report

Part I - Identification and Reporting

1. Background Information

Incident/Breach Summary	• Click here to enter text.
Name of reporting organization	Click here to enter text.
Point of contact and contact details	Click here to enter text.

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 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

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 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

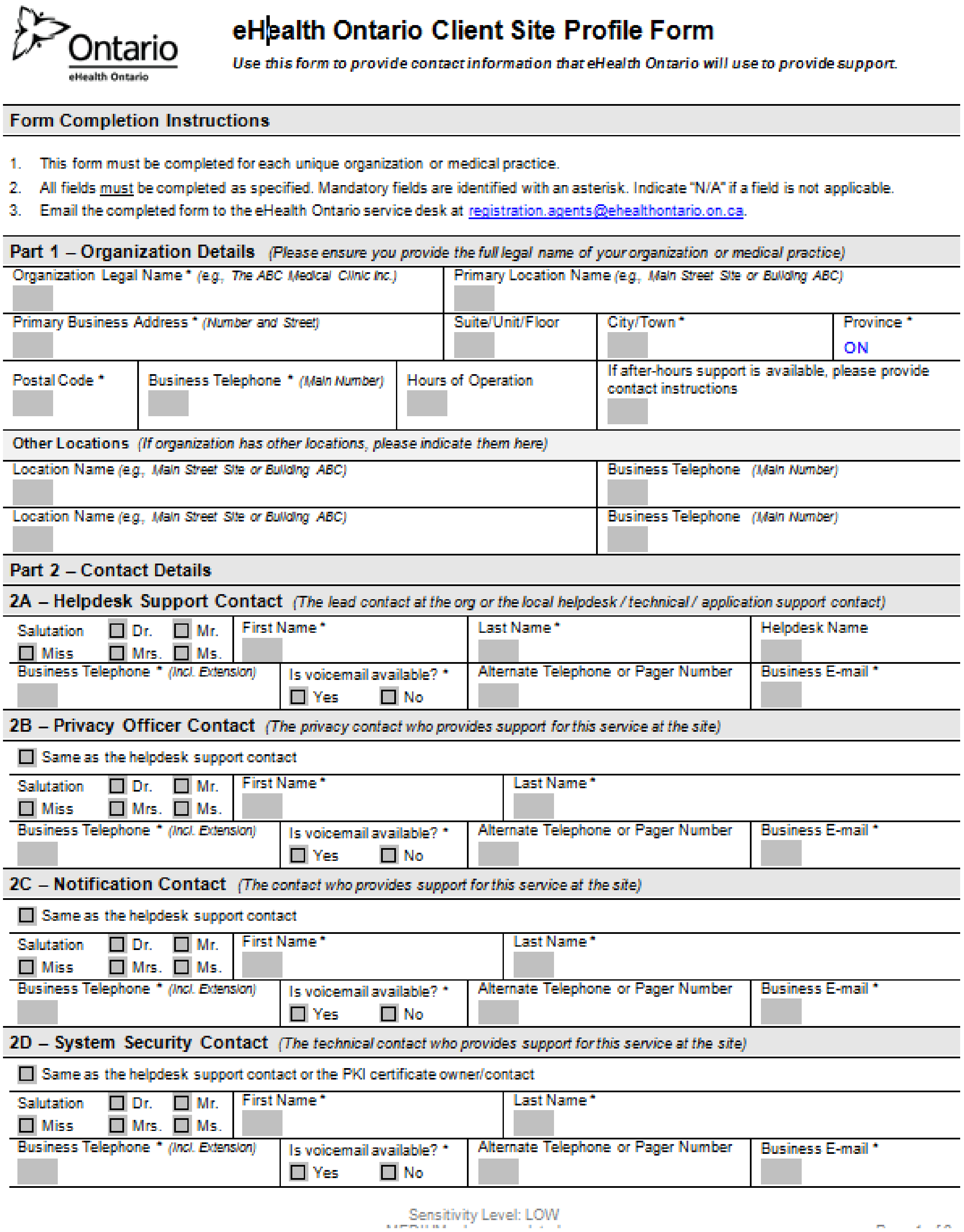
12. Please identify the remediation activities to prevent the incident from occurring again.

Remediation Recommendation	Schedule Date	Owner	Progress	Complete Date
Recommendations/ Actions items are captured in the attached document.			Click here to enter text.	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: Client Site Profile Form



Ontario
eHealth Ontario

eHealth Ontario Client Site Profile Form

Use this form to provide contact information that eHealth Ontario will use to provide support.

Form Completion Instructions

1. This form must be completed for each unique organization or medical practice.
2. All fields must be completed as specified. Mandatory fields are identified with an asterisk. Indicate "N/A" if a field is not applicable.
3. Email the completed form to the eHealth Ontario service desk at registration.agents@ehealthontario.on.ca.

Part 1 – Organization Details *(Please ensure you provide the full legal name of your organization or medical practice)*

Organization Legal Name * *(e.g., The ABC Medical Clinic Inc.)*		Primary Location Name *(e.g., Main Street Site or Building ABC)*	
Primary Business Address * *(Number and Street)*	Suite/Unit/Floor	City/Town *	Province * ON
Postal Code *	Business Telephone * *(Main Number)*	Hours of Operation	If after-hours support is available, please provide contact instructions

Other Locations *(If organization has other locations, please indicate them here)*

Location Name *(e.g., Main Street Site or Building ABC)*	Business Telephone *(Main Number)*
Location Name *(e.g., Main Street Site or Building ABC)*	Business Telephone *(Main Number)*

Part 2 – Contact Details

2A – Helpdesk Support Contact *(The lead contact at the org or the local helpdesk / technical / application support contact)*

Salutation □ Dr. □ Mr. □ Miss □ Mrs. □ Ms.	First Name *	Last Name *	Helpdesk Name
Business Telephone * *(Incl. Extension)*	Is voicemail available? * □ Yes □ No	Alternate Telephone or Pager Number	Business E-mail *

2B – Privacy Officer Contact *(The privacy contact who provides support for this service at the site)*

□ Same as the helpdesk support contact

Salutation □ Dr. □ Mr. □ Miss □ Mrs. □ Ms.	First Name *	Last Name *	
Business Telephone * *(Incl. Extension)*	Is voicemail available? * □ Yes □ No	Alternate Telephone or Pager Number	Business E-mail *

2C – Notification Contact *(The contact who provides support for this service at the site)*

□ Same as the helpdesk support contact

Salutation □ Dr. □ Mr. □ Miss □ Mrs. □ Ms.	First Name *	Last Name *	
Business Telephone * *(Incl. Extension)*	Is voicemail available? * □ Yes □ No	Alternate Telephone or Pager Number	Business E-mail *

2D – System Security Contact *(The technical contact who provides support for this service at the site)*

□ Same as the helpdesk support contact or the PKI certificate owner/contact

Salutation □ Dr. □ Mr. □ Miss □ Mrs. □ Ms.	First Name *	Last Name *	
Business Telephone * *(Incl. Extension)*	Is voicemail available? * □ Yes □ No	Alternate Telephone or Pager Number	Business E-mail *

Sensitivity Level: LOW

1A – Organization Details	
Organization Legal Name*	Indicate the legal name of the organization that is eligible for the service.
Primary Business Address*	Enter the address of the site identified in the Location Name field. Include the street number, street name, and street suffix (if any). For example, 123 Your Street North.
Suite/Unit/Floor	Enter the suite, unit, or floor number of the address identified in the Business Address field.
City/Town*	Enter the city or town associated with the address identified in the Business Address field.
Province*	This field always indicates Ontario and completion is therefore not necessary.
Postal Code*	Enter the postal code associated with the address identified in the Business Address field.
Business Telephone*	Enter the business main telephone number for the organization.
Hours of operation	Indicate your business hours in this field.
If after-hours support is available, please provide contact instructions	If your indicated contacts are available for contact outside of normal business hours indicate instructions around their availability.
Other Locations	Enter the names and addresses of any additional practice locations; you may use a separate sheet to capture additional sites as required.
1B – Helpdesk Support Contact Information	
Salutation	Enter title used before the surname or full name, or the professional title.
First Name*	Enter the contact's full first name.
Last Name*	Enter the contact's full last name.
Helpdesk Name	Enter the name of the Local Helpdesk
Business Telephone (including Extension)*	Enter the business telephone number and extension where the helpdesk support contact can be reached. In instances where there is a centralized helpdesk, a toll free number can be entered here
Alternate telephone or pager number	Enter any available alternate numbers where the contact can be reached.
Business E-mail	Enter the business e-mail address where the contact can be reached.
1C – Privacy Officer Contact	
Salutation	Enter title used before the surname or full name, or the professional title.
First Name*	Enter the service support contact's full first name.
Last Name*	Enter the service support contact's full last name.
Business Telephone (including Extension)*	Enter the business telephone number where the privacy officer t can be reached. Please list an extension number if applicable.
Alternate telephone or pager number	Enter any available alternate numbers where the contact can be reached.
Business E-mail	Enter the business e-mail address where the privacy officer can be reached. Please do not indicate personal e-mail addresses.
1D – Notification Contact	
Salutation	Enter title used before the surname or full name, or the professional title.
First Name*	Enter the service support contact's full first name.
Last Name*	Enter the service support contact's full last name.
Business Telephone (including Extension)*	Enter the business telephone number where the notification contact can be reached. Please list an extension number if applicable.
Business E-mail	Enter the business e-mail address where the notification contact can be reached. Please do not indicate personal e-mail addresses.
1E – System Security Contact	
Salutation	Enter title used before the surname or full name, or the professional title.
First Name*	Enter the service support contact's full first name.
Last Name*	Enter the service support contact's full last name.
Business Telephone (including Extension)*	Enter the business telephone number where the system security contact can be reached. Please list an extension number if applicable.
Business E-mail	Enter the business e-mail address where the system security contact can be reached. Please do not indicate personal e-mail addresses.

Appendix D: Glossary