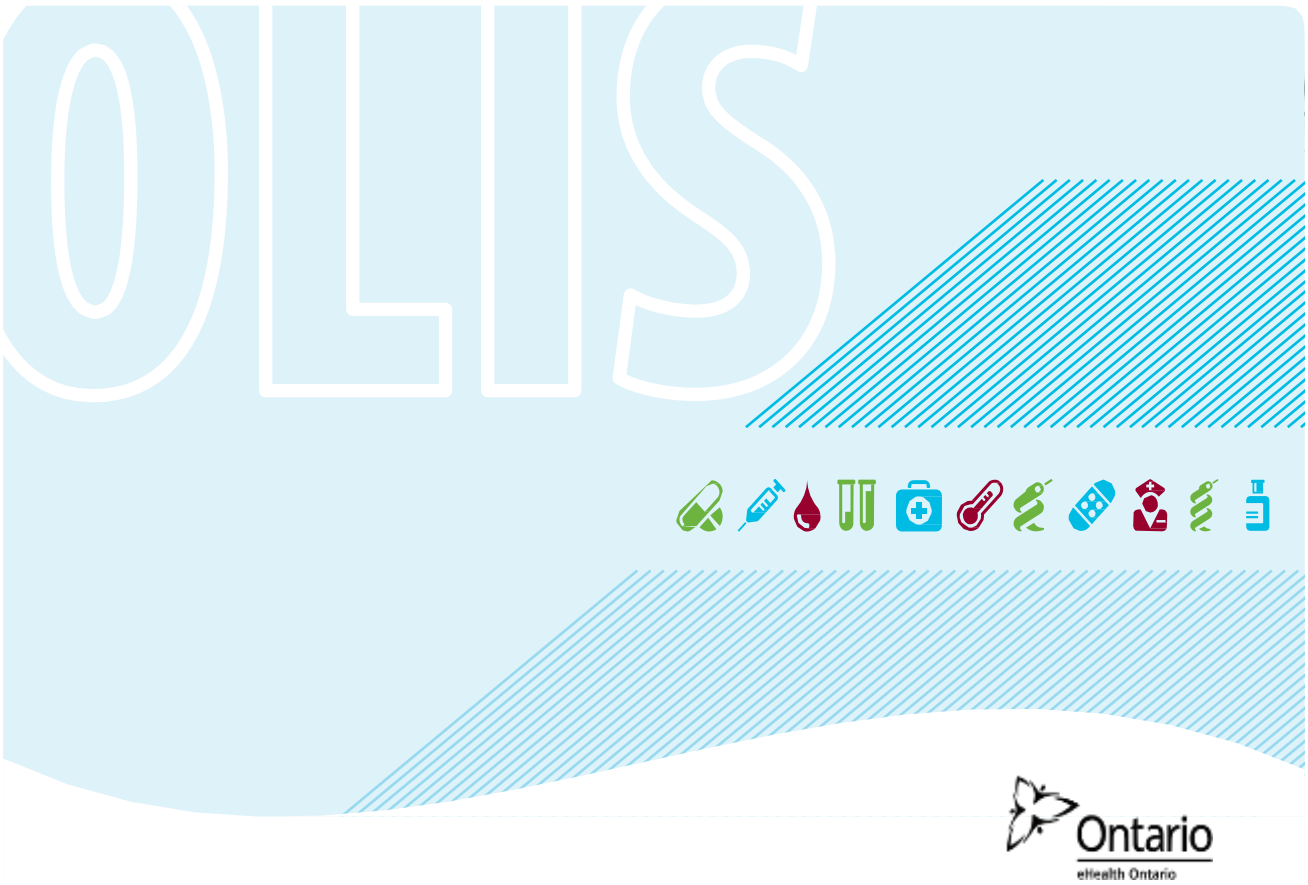


eHealth Ontario Site Support Guide

Version 8.0

Reference Guide

This guide will assist the electronic Child Health Network with information around processes and contacting eHealth Ontario for support.

www.eHealthOntario.on.ca

Version	Date	By	Comments
1.0	06/07/12	Marcia Bailey	Draft
2.0	25/07/12	Marcia Bailey	Added updates for Service Ontario contact numbers from MOHLTC
3.0	26/7/12	Arshia Raafat	Revised, re-structured and edited document and incorporated feedback from Privacy and Security.
4.0	15/10/12	Arshia Raafat	Incorporated changes based on discussions amongst eHealth Ontario, eCHN and SickKids
5.0	30/05/13	Marcia Bailey	Added the client profile form at the end
6.0	30/10/13	Arshia Raafat and Carla Murphy	Incorporated input and updates from eHealth Privacy and Security and OLIS Business
7.0	27-11-13	John Kellenberger	Incorporated updates from eCHN
7.1	02-12-13	John Kellenberger	Minor updates incorporated
7.2	05-12-13	John Kellenberger	Minor updates incorporated
7.4	12-12-13	John Kellenberger	Minor wording updates
8.0	19-12-13	John Kellenberger	Minor wording updates

Contents

NOTICE AND DISCLAIMER

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 the electronic Child Health Network (eCHN) with facilitating access to the Ontario laboratories information system (OLIS). The guide provides information regarding support and maintenance as well as privacy and security procedures and obligations.

The guide includes information for eCHN as well as information to be shared with eCHN users and sites and has been structured accordingly.

A. electronic Child Health Network (eCHN)

1. Support

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

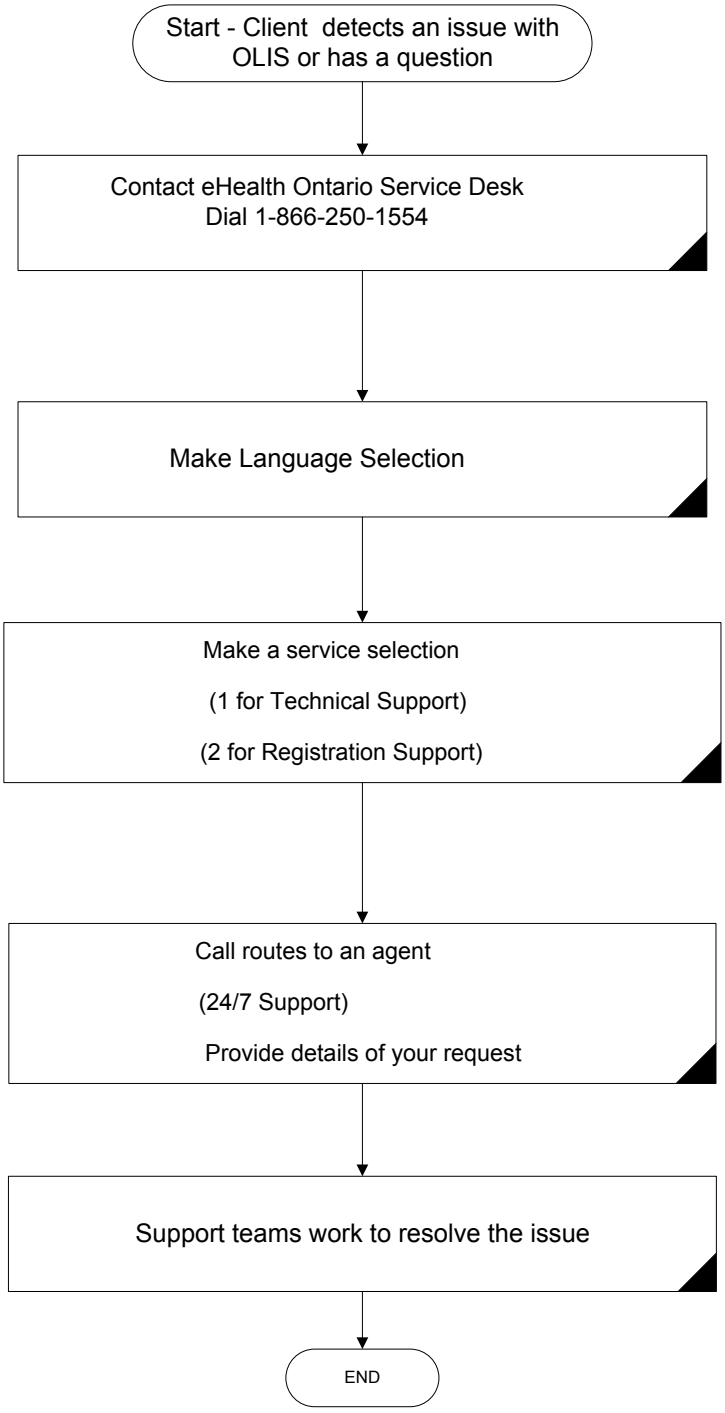
1.1 Contacting the Service Desk for Support

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
Tel: (905) 826 – 5551
Toll Free: 1-866-250-1554
Option 1 – Technical Support
Option 2 – Registration Support
Email: servicedesk@ehealthontario.on.ca
Email: registration.agents@ehealthontario.on.ca
For a list of other contact numbers within eHealth Ontario, please visit
http://www.ehealthontario.on.ca/en/contact

7/24 hr service request support flow



1.1.2 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 the phone.

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 issues 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 transferred to eHealth Ontario's next level of support team

Step 3	Incident is assigned to the next level of support
Issue transferred to eHealth Ontario next level of support team	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 fifteen (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 (3) attempts to contact you. During this time, you will receive three (3) 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

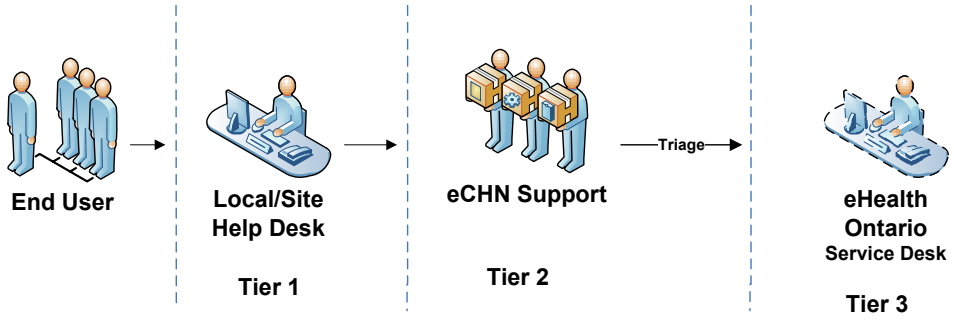
Upon closing a service request, eHealth Ontario randomly selects incidents to be surveyed. For that reason you might receive a request to fill in an online questionnaire. We would very much appreciate it if you would help us ensure the quality of our service by taking a short, five (5)-minute survey.

General feedback

If you wish to provide us your comments or suggestions, please contact the eHealth Ontario service desk by email servicedesk@ehealthontario.on.ca.

1.2 Support Processes

1.2.1 High level depiction of the service desk model



1.2.2 eCHN support accountabilities

When any issues with the eCHN interface are detected, eCHN provides support for sites and users and will assist in:

- troubleshooting the issues;
- providing a resolution where possible;
- determining potential impact of the issues; and
- escalating to the appropriate eCHN 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 PKI certificate issues
- Requesting assistance with troubleshooting OLIS related interface issues
- 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 around our release dates and application improvement activities

1.2.5 When does the eHealth Ontario privacy office contact you?

- For requesting additional information and/or data audit logs 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 eCHN 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 <hospital, lab, department>
- The name of the lab that submitted the result
- The lab report #
- 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)**

2. eCHN Operational Responsibilities for OLIS Data

2.1 Submitting Data Audit Logs to eHealth Ontario

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 such as eCHN's. Due to this legislative requirement, eHealth Ontario must obtain a copy of the OLIS audit logs from eCHN on a weekly basis. eHealth Ontario may require additional information from eCHN to interpret the logs.

2.1.1 Content

At a minimum the log must include:

- the user ID (first name, last name, regulatory college licence number, if applicable)
- location (organization ID)
- audit event time of access
- audit event date of access
- Patient ID (including name, health card number or medical record number, date of birth, and gender)
- audit event ID (from eCHN's WebChart logs)
- event type (e.g. view doc)
- application (e.g. WebChart)
- document name (name of lab result accessed)
- document facility (e.g. lifelabs)
- document (i.e. lab result) date & time
- additional info (from eCHN's audit logs)
- if delegate access is permitted (future state), the user on whose behalf the query is submitted

Additionally, eHealth requires logs showing consent overrides that have been implemented in eCHN's system for OLIS data, including:

- the user ID (first name, last name, regulatory college licence number)
- location (organization ID)
- time of access (i.e. time consent was overridden)
- audit event date of access (i.e. date consent was overridden)
- Patient ID (including name, health card number or medical record number, date of birth, and gender)
- audit event ID (from eCHN's WebChart logs)
- application (this should always be WebChart)
- event type (e.g. override of consent directive)
- type of override (should always be express consent from the patient on a temporary basis 'Z')
- if substitute decision maker (SDM) provided express consent for the override, then SDM name and relationship to patient must be provided
- if applicable, document facility from which document came
- if applicable, document (i.e. lab result) date & time

In addition to the above, eCHN is to provide eHealth Ontario with any paper or electronic documents that are required to translate an identifier (ID) used in the audit logs to a real-world ID. For example, if an organization ID is used in the audit logs to identify an eCHN site, then

eCHN is to provide eHealth Ontario with the organization ID in the logs, along with the full name and location of the organization from which the user accessed the information.

2.1.2 Timeline

For every weekly log transfer, eCHN should include the period of the report (e.g. April 1, 2012 to April 7, 2012), and the date the report was created.

2.1.3 Process

- eCHN to supply OLIS Access logs weekly to the OLIS Business Support Delivery (BSD) team every Friday by 2 pm, by email to : OLISBusinessHelp@ehealthontario.on.ca
- OLIS BSD team will communicate with the eCHN identified contact to obtain the password to decrypt the file
- OLIS BSD will store files under OLIS consent folder in the eCHN Audit Log folder

Please refer to Appendix B for instructions on how to encrypt files and securely transfer them to eHealth Ontario.

2.2 OLIS Data in eCHN - Retention Schedule

eHealth Ontario is responsible for establishing the retention schedule for OLIS data as well as for any copies of the data which remain in its control, such as the eCHN sub-copy of the OLIS data and log data.

Additionally, as eCHN will be acting as a PHIPA Sub-Agent of eHealth Ontario for the purpose of consent management and producing reports to respond to Individual Access Requests, any personal health information (PHI), or related information, created or received by eCHN in its Sub-Agent role will have to follow the retention schedule set out by the Ministry of Health and Long Term Care (MOHLTC).

The retention schedule for all OLIS data, including OLIS-related logs, as well as PHI held by eHealth Ontario as Sub-Agent is included in Appendix A. Under agreement with eHealth Ontario, eCHN is required to follow this retention schedule for the OLIS data and related documentation. eCHN must adhere to the retention schedule in Appendix A in respect of the following:

- OLIS data in eCHN's data repository;
- OLIS-related audit logs including SDM information;
- Any paper or electronic documents that are required to translate an identifier (ID) used in the audit logs to a real-world ID; and

- TPAS (tactical privacy audit solution) reports, the consent override reports, incident management reports, and any other reports or related documentation produced by eCHN in its Sub-Agent role.

eCHN has advised that it retains the PHI in its data repository until the Health Information Custodian (HIC) advises the PHI to be removed. Appendix A of this guide sets out the retention period for each type of OLIS data and related documentation. For any type of OLIS-related documentation excluded from this retention schedule the retention period is indefinite unless otherwise notified in writing by eHealth Ontario.

2.3 Logical Deletion of OLIS Data in eCHN

eHealth Ontario has the ability to logically delete corrupted lab records. Each time this occurs, eHealth Ontario will provide to eCHN 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 inserted into OLIS
- Include or exclude flag
- Deletion date

eCHN will identify the OLIS logically deleted record, based on information provided by eHealth Ontario, and logically delete the record from the eCHN repository within five (5) business days

2.4 Consent Override Reporting Process

Patients have the option to restrict access to their data in OLIS through consent directives (see section 3.1 below). eCHN users can only override a patient's consent directive with the express consent of the patient or their substitute decision maker. 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.

To facilitate the process, eCHN will send reports to eHealth Ontario at OLISBusinessHelp@ehealthontario.on.ca on a weekly basis. The reports will detail patient express consent overrides to OLIS data within its system. The legal agreements signed by both organizations include details on this activity and highlight the following data elements that are to be shared with eHealth Ontario. eCHN to share for any patient whose OLIS consent directive was overridden:

- date and time consent was overridden (YYYY/MM/DD);

- action performed (i.e. consent override with express consent);
- last, first name and middle name if available or substitute decision maker name and the relationship to the patient;
- Ontario health card number and version code and/or medical record number;
- gender;
- date of birth (YYYY/MM/DD);
- language preference; and
- mailing address of patient including street name, suite or apt. number, city, province or equivalent, postal code or equivalent

The consent override report will be produced by eCHN via an automated process that will run on a weekly basis. The output of the automated process will be a list of patient IDs and types that have had an override on their blocked OLIS data. The output will also include the health care provider that initiated the override along with the date and time of each override. This output file will be used by eHealth Ontario to generate individual patient reports that will be embedded in a letter addressed to the patient, explaining the purpose of the report.

2.5 Responding to Access Requests (Tactical Privacy Audit Solution Reports)

eHealth Ontario will require eCHN to produce OLIS logs to assist eHealth Ontario in fulfilling access requests. There are two forms of access request with respect to OLIS:

- Access requests from individuals to the MOHLTC as the HIC of OLIS (discussed at section 3.2.1); and
- Access request from HIC organizations connected to OLIS (discussed at 3.2.2)

eCHN is not to respond directly to access requests but will assist eHealth Ontario in accordance with the process described below. The eHealth Ontario Privacy Office will contact the eCHN Help Desk to request logs and eCHN will provide the logs requested within two (2) business days.

2.5.1 Processing of access requests

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. If the processing of a patient or HIC access request requires logs from eCHN, the eHealth Ontario privacy office will contact the eCHN help desk at 416-813-7998 from Monday through Friday from nine (9) to five (5) and at 416-904-6484 at all other times to request logs.

- eCHN is to provide the TPAS logs requested by eHealth within **two (2)** business days.
- eCHN business help desk will encrypt the TPAS logs with WinZip as noted in **Appendix B** and send the logs to the email address provided by eHealth Ontario privacy office at the time of placing the request for logs.

- eCHN to provide mapping of organization IDs noted in the logs as well as provide data field definitions as noted in the TPAS logs.
- eHealth Ontario privacy office is to notify eCHN when request is closed.
- eCHN is to retain the COPY (i.e. excerpt) of the TPAS logs produced for eHealth to respond to the access request until they are successfully transferred to eHealth Ontario.
- As described in Appendix A of this document, eCHN is to permanently delete the TPAS report/logs transferred to eHealth Ontario after confirmation from eHealth Ontario is received by eCHN that the transfer of the report(s) to eHealth was successful.

2.5.2 Types of logs

eCHN will be required to provide the following types of TPAS logs to assist eHealth Ontario in fulfilling access requests.

- Access to patient Y's OLIS records by all eCHN users
    - This log should include information on access to a particular patient's ("patient Y") OLIS records by all eCHN users.
    - This log should include the following information: Patient ID (including name, HCN or MRN, date of birth), date of access, access type, OLIS data accessed, the organization the individual accessed the record from, the user who accessed the information and the time period during which the access occurred.
- Access at a particular facility to patient Y's OLIS records
    - This log should include information on access to patient Y's OLIS records by eCHN users at a particular eCHN site ("facility X"). The log should include the following information: Patient ID, date of access, OLIS data accessed, access type, the user who accessed the information, the facility where access occurred and the time period during which the access occurred.
- Access by user A, at facility X, to OLIS records of patients
    - This log should contain information on access by user A at facility X of record of patients. The log should contain information on the date of access, access type, OLIS data accessed, patients whose information was accessed (Patient ID), the facility where access occurred and the time period during which the access occurred.
- Access to OLIS data by all users at Facility X
    - This log should contain information on access to OLIS data by all users at facility X. The log should contain information on the date of access, access type, patients whose information was accessed (Patient ID), users who accessed the information, OLIS data accessed, the facility where access occurred and the time period during which the access occurred.

3. Privacy and Security

3.1 Patient Consent

3.1.1 Background

As custodians of patient PHI, eCHN sites and health care providers working at sites have obligations under the PHIPA and Ontario Regulation 329/04. The site obligations are set out in the Health Care Provider Guide embedded in section B.2.

eCHN, for the OLIS-eCHN initiative is acting as a PHIPA Sub-Agent to eHealth Ontario, as well as a service provider to eHealth Ontario. This means that eCHN has certain obligations in respect of consent management for OLIS data in eCHN's system.

Patient Consent Model for OLIS-eCHN

OLIS data in eCHN has a consent directive capability, which gives patients or their substitute decision maker(s) 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 eCHN for OLIS data will not be able to access any patient information that has been, or will be, submitted into OLIS. When an eCHN user queries OLIS lab results for this patient, the eCHN WebChart will notify him/her that the result is blocked when returning the results of a patient query.

3.1.2 Overriding a consent directive from within the eCHN WebChart

In special cases (with consent from the patient or the patient's SDM) the consent directive restricting access to OLIS data can be overridden by a provider, from within the eCHN WebChart.

Such an override is logged in the eCHN Audit Manager, along with the identity of the overriding health care provider. As detailed in section 2.4, eCHN provides eHealth Ontario with a weekly report of the consent directive overrides, for OLIS data.

The eCHN WebChart application enables users to override a consent directive applied to data within eCHN's system where; (a) there is a clinical/emergency requirement; or (b) access has been granted directly by patient or the patient's SDM (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, eCHN's users are permitted to override a consent directive applied to OLIS data within eCHN's system 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. eCHN has modified its WebChart user interface to permit eCHN users to override the patient's consent directive, for OLIS data, only with the express consent of the patient or SDM, and not for reasons of clinical emergency (eCHN has technically disabled the clinical/emergency override option for OLIS data). Overriding a patient's consent directive for OLIS data without express consent from the patient or the patient's SDM constitutes a breach of the user's (or eCHN site's) agreement with eHealth Ontario, and will be subject to the remedies available under the agreement.

If a user inquires to eCHN about the consent management features of OLIS, including the consent override function, please advise the user to contact eHealth Ontario's privacy office at privacy@ehealthontario.on.ca. Please advise the user to indicate in the e-mail that they are an eCHN user.

3.1.3 Applying consent directives to OLIS data

If a patient contacts eCHN and wishes to place a restriction on access to his/her information in OLIS, or wishes to reinstate access (remove the restriction), eCHN is not permitted to access OLIS data for this purpose. eCHN is to advise 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 Health Information Custodian (HIC or custodian) 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 (including the OLIS data in eCHN's system), only the MOHLTC can respond to an individual's access request. As stated in the agreement between eHealth Ontario and eCHN, eCHN is not to provide OLIS data or OLIS audit logs directly to patients.

Instead, if a patient requests OLIS data from eCHN, or inquires as to who has viewed the patient's OLIS data in eCHN, then eCHN is to 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

If eHealth Ontario determines that it requires eCHN's assistance in fulfilling an individual's access request for OLIS data, then eHealth Ontario will contact eCHN and the parties will follow the process set out in section 2.5 above.

3.2.2 Requests from eCHN sites for OLIS audit logs (for their site)

eCHN sites (lead physician or privacy officer at an eCHN site) may require a record of who from their organization accessed OLIS data via eCHN's WebChart. 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 eCHN 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 eCHN site, within the timeframe set out in the request.

If eCHN receives a request from an eCHN site for OLIS audit logs, eCHN is to advise the site to contact eHealth Ontario's service desk at 1-866-250-1554 to make the request for the audit logs for the eCHN site.

The eHealth Ontario service desk will open a ticket to fulfill the request. A representative from eHealth Ontario's privacy office will call the contact person listed on the OLIS-eCHN Site Profile Form to confirm the type of report requested. eHealth Ontario will then contact eCHN to assist with fulfilling the site's request for OLIS audit logs, in accordance with the log/report transfer processes described in section 2.5 above.

eCHN is not to release OLIS audit logs to eCHN sites directly, unless expressly permitted by eHealth Ontario in writing. However, eCHN may make available to a site the online audit tool via the eCHN Audit Reporter to review access to its patients' records.

3.3 Inquiries and Complaints Received by eCHN in Respect of eHealth Ontario or OLIS Data

If eCHN receives any complaints or inquiries from users or patients with respect to OLIS data in eCHN's system, eCHN 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 how eCHN manages the OLIS data on behalf of eHealth Ontario.

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

Tel. 1-866-250-1554
Email: servicedesk@ehealthontario.on.ca

If eCHN receives a complaint or inquiry relating to eHealth Ontario in general (i.e. not related to OLIS data in eCHN's system), or related to eHealth Ontario's privacy policies and procedures, eCHN 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 eCHN

If eCHN has any questions regarding the privacy-related processes described above, including how to respond to individual access requests, retention periods, consent obligations of eCHN 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

A joint eHealth Ontario/eCHN privacy and security incident management process was created for this initiative. The process describes the responsibilities of eCHN in the event that a privacy or security incident as defined in the embedded document below is discovered by eCHN or is reported by a patient or a site. The sites' privacy and security incident management responsibilities are detailed in the Health Care Provider Guide which is referenced in section B.2.

eCHN eHealth
Privacy Breach Manag

4. Legal Agreements and Access to OLIS

eHealth Ontario and eCHN have entered into a legal partnership for the purpose of providing authorised eCHN users with access to OLIS data. The agreements structure for the project has been defined in the document embedded below. eHealth Ontario, in addition to entering into agreements with eCHN, will be directly signing legal agreements with eCHN sites including hospitals, CCACs and practitioner offices.

4.1 Who can access OLIS data and for what purpose

eCHN must only provide OLIS access to users that are Ontario regulated health professionals for which eCHN records in its audit logs the name and Regulatory College # of the user.

eCHN must only provide access to OLIS to eCHN users for the purpose of providing health care or assisting in the provision of health care to patients. eCHN must not use or allow the use of OLIS or OLIS data for any research purposes or any other secondary uses unless authorised to do so in writing by the MOHLTC, a copy of which authorisation is to be provided to eHealth Ontario prior to any such use.

In addition, eCHN must ensure that it will only provide access to OLIS data to those users that have signed the applicable agreements as outlined in the agreements structure embedded below.

4.2 Agreements Structure

OLIS eCHN Final
Agreements Structure

4.3 Agreements Tracking

As agreed upon by eCHN and eHealth Ontario, eHealth Ontario is to facilitate the signing of agreements between eHealth Ontario and eCHN sites. eHealth Ontario will be distributing the agreements to eCHN sites and users and monitoring the agreement execution progress by recording the progress and sharing with eCHN on a weekly basis (every Friday).

4.4 Additional Information

In addition to the legal agreements, eHealth Ontario will distribute the following documents to each site and all users:

- Health Care Provider Guide (included in section B.2)
- Client Site Profile Form (included in section B.1). Instructions for completing the form are also included in this section.

B. eCHN Users and Sites

1. OLIS Setup Requirements

A privacy officer/contact person will be assigned by each eCHN site that has access to OLIS data, to liaise with eHealth Ontario for incident management purposes. eHealth Ontario will be distributing the Client Site Profile Form, referenced in Appendix D, to each site.

1. All sites provisioned to access OLIS must fill out a Client Site Profile Form and send it to the eHealth Ontario service desk through e-mail 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. eHealth Ontario will distribute the Client Site Profile form to each site and advise the contact person at the site to complete the form and e-mail it to the eHealth Ontario service desk at the e-mail address included above.
2. The privacy officer/contact person at eCHN and preferably 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 B of this guide.

2. Health Care Provider Guide

The Health Care Provider Guide was developed to inform users and sites of all processes related to the use of OLIS data via eCHN's WebChart. eHealth Ontario will distribute this guide to each site (physician offices, hospitals, CCACs, …) that is registered to access OLIS via eCHN. Each eCHN user and the privacy officer at each site should be provided with a copy of the guide. The Health Care Provider Guide to be distributed is embedded below.

eCHN Health Care Provider Guide.pdf

Appendix A: Retention Schedule for OLIS Data

Category of Data	Description	Retention Period	Notes
OLIS data in eCHN's data repository	"OLIS data" means any personal health information (as defined in s.4 of PHIPA) about Patients in OLIS, including name, health number, laboratory test result history and related personal information of a patient. OLIS data does not include OLIS access and system logs, or information about consent directive overrides for OLIS data, including substitute decision maker (SDM) information. **File Format:** Electronic	Indefinitely, unless otherwise instructed by eHealth Ontario in writing.	eCHN to permanently destroy the relevant OLIS data when instructed by eHealth Ontario in writing in accordance with the definition of 'destroy' in the PHIPA Sub-Agent Agreement entered into between eHealth Ontario and eCHN. The definition of 'destroy' is reproduced below this table. Upon secure destruction of the OLIS data, eCHN will provide eHealth Ontario with a certificate of destruction if directed to do so by eHealth Ontario.
OLIS-related audit logs and supporting materials	This Category includes OLIS access and system logs in eCHN's system which detail, for each OLIS record accessed, the name/ID of the user that has accessed the OLIS data, location of access (Organization ID), time/date of access, patient ID and the user on whose behalf the query is submitted. This Category of data also includes records of consent overrides for OLIS data performed by eCHN users, including, where applicable, the name of the substitute decision maker (SDM) that provided express consent and relationship of the SDM to the patient. This category additionally includes supporting materials such as any paper or electronic documentation that is required to translate an identifier (ID) used in the audit logs into a real-world ID (for example, if a	Indefinitely, unless otherwise instructed by eHealth Ontario in writing.	eCHN to transfer to eHealth Ontario on a weekly basis a copy of the OLIS-related audit logs and supporting materials. Please see section A.2.1 for more information on the transfer process.

	form is required to identify an user or organization by name/licence number/location rather than by the ID used in the logs, then eCHN to retain such forms). **File Format:** electronic/paper		
Consent override reports	Weekly reports provided by eCHN to eHealth Ontario with details of overrides performed in eCHN's system on blocked OLIS data. These reports may include information about the SDM and the relationship to the patient. **File Format:** paper/electronic	**Up to 5 days** - eCHN to permanently delete the consent override report(s), immediately or no later than 5 calendar days, once confirmation from eHealth Ontario is received that the transfer of the report(s) to eHealth Ontario was successful.	eCHN to permanently destroy the relevant consent override reports, at the expiry of the retention period in accordance with the definition of 'destroy' in the PHIPA Sub-Agent Agreement entered into between eHealth Ontario and eCHN. The definition of 'destroy' is reproduced in the Appendix of this document for reference. Upon secure destruction of the consent override reports, eCHN will provide eHealth Ontario with a certificate of destruction if directed to do so by eHealth Ontario.
Privacy and Security Incident Management Investigation Reports and related documentation	This category includes any privacy or security incident investigation materials that contain personal information or personal health information, including investigation notes, copies of logs to support incident investigation, investigation reports and other incident management documentation, that eCHN produces for eHealth Ontario to assist eHealth Ontario with Incident management or investigation. **File Format:** electronic/paper	**Up to 5 days** - eCHN to permanently delete the report(s), immediately or no later than 5 calendar days, once confirmation from eHealth Ontario is received that the transfer of the report(s) to eHealth Ontario was successful.	eCHN to permanently destroy the relevant incident management documentation, at the expiry of the retention period in accordance with the definition of 'destroy' in the PHIPA Sub-Agent Agreement entered into between eHealth Ontario and eCHN. The definition of 'destroy' is reproduced below this table for reference. Upon secure destruction of the incident management documentation, eCHN will provide eHealth Ontario with a certificate of destruction if directed to do so by eHealth Ontario
TPAS reports	Tactical Privacy Audit Solution (TPAS) reports include copies of logs/reports produced by eCHN to assist eHealth Ontario in responding to patient and health care provider requests regarding access to OLIS patient health records in eCHN's system.	**Up to 5 days** - eCHN to permanently delete the report(s), immediately or no later than 5 calendar days, once confirmation from eHealth Ontario is received that the transfer of the report(s) to	eCHN to permanently destroy the relevant TPAS documentation, at the expiry of the retention period in accordance with the definition of 'destroy' in the PHIPA Sub-Agent Agreement entered into between eHealth Ontario and eCHN. The definition of 'destroy' is reproduced below

	This includes any paper or electronic documents that are received or produced by eCHN (such as access request forms with patient identification information, copies of access logs about a particular patient or provider) to assist eHealth Ontario in responding to an access request. **File Format**: electronic/paper	eHealth Ontario was successful.	this table for reference. Upon secure destruction of the TPAS documentation, eCHN will provide eHealth Ontario with a certificate of destruction if directed to do so by eHealth Ontario

"Destroy" means, with respect to the Relevant PHI in the possession or control of the Contracting PHIPA Agent or of any PHIPA Sub-Agent, to:

(a) physically destroy all print and other hard copies of it;

(b) erase, scrub, or otherwise remove all electronic, digital or other versions of it from every item of equipment and all media (including disks, tapes, computers, servers, and related peripheral equipment such as disk arrays, tapes or disk backup units) that it has been installed, downloaded, or otherwise put, onto; and

(c) otherwise obliterate it,

or to ensure that the foregoing is done, and **"Destroying" and "Destroyed"** have corresponding meaning.

"Return" means for eCHN to return the data (paper or electronic) to eHealth Ontario, using secure means as directed by eHealth Ontario, when the retention period is complete.

Appendix B: Procedures for Communicating Sensitive Files Over email

Overview

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

This document provides the 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 could 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 as part of 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.

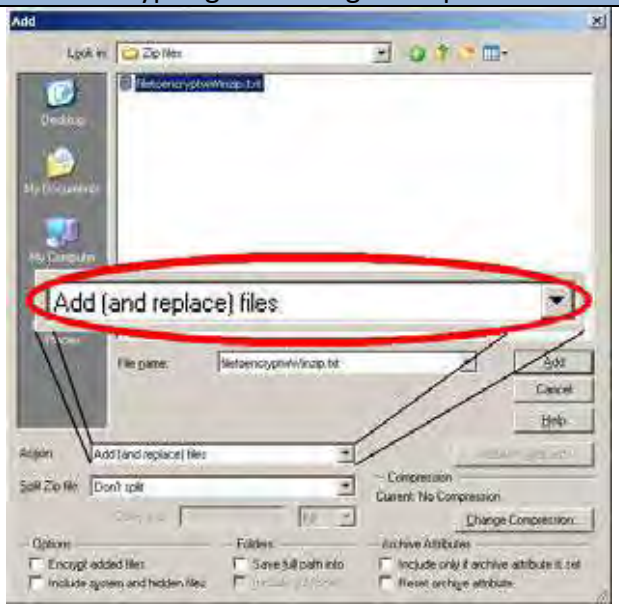
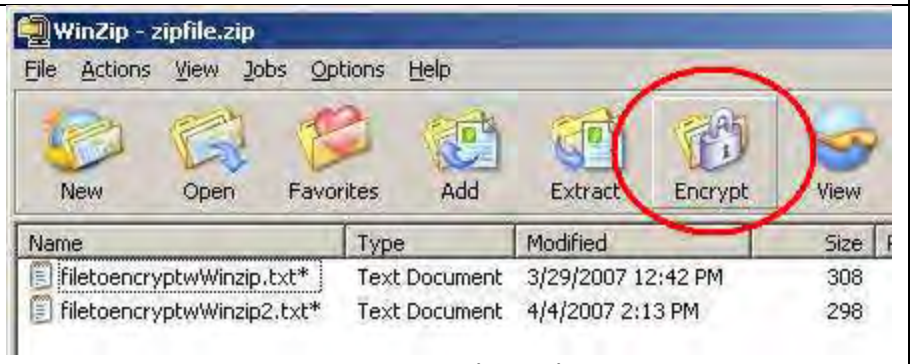
The limit on email attachments has been predetermined at 10 MB per email at eHealth Ontario.

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.	 **Fig.1** Add files to an archive
Step 2. <u>Encrypt the entire archive:</u> Encrypt the entire archive after all files have been added. Click on the "Encrypt" icon.	 **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.

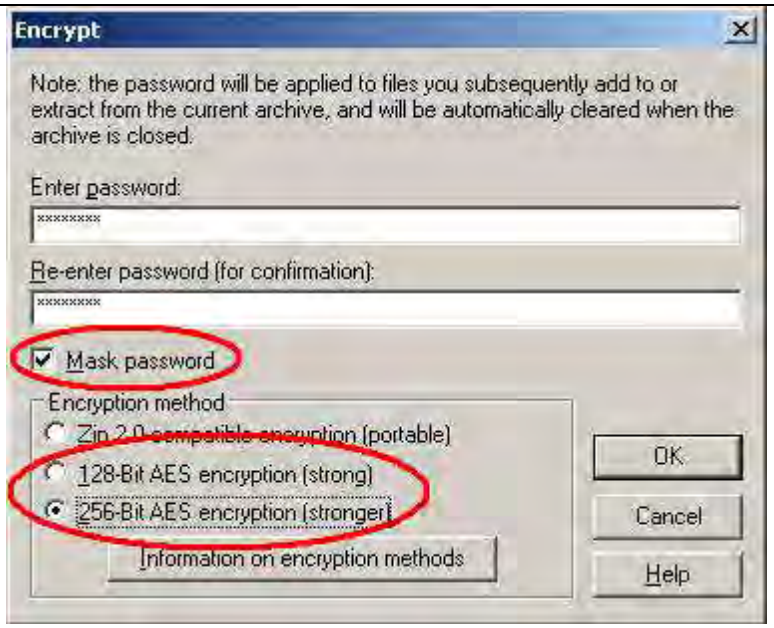


Fig.3 Choose an encryption mechanism

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 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 for the business' needs).

An example of a password recovery method is storing the password in a sealed envelope to which only upper management have access to 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 C: 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

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

Internal Communications

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

Part IV – Investigation

11. Breach investigation

Investigation Summary	•
Outocme 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 ongoing 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 D: Client Site Profile Form

eHealth Ontario Client Site Profile Form

Form Completion Instructions

1. This form must be completed with all contacts that eHealth Ontario will use to provide ongoing support.
2. All fields must be completed as specified. Mandatory fields are marked with an asterisk. Indicate "N/A" if a field is not applicable.
3. **E-mail completed form to the eHealth Ontario Service desk at** registration.agents@ehealthontario.on.ca.

1A – Practice Group Information (*Please provide information about the Practice Group)*

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

Other Locations - If site has other locations please indicate them here

Location Name		Location Name	
Business Telephone		Business Telephone	

1B – Helpdesk Support Contact Information (*Please provide information for the lead contact at the Practice)*

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*

1C – Privacy Officer Contact *(Please provide the name of a privacy contact who provides support for this service at the Practice Location, where different from above)*

Salutation ☐ Dr. ☐ Mr. ☐ Miss ☐ Mrs. ☐ Ms.	First Name *	Last Name *	
Business Telephone * *(incl. Extension)*	Is voicemail available (Yes/No)	Alternate telephone number	Business E-mail

1D – Notification Contact *(Please provide the name of a contact who provides support for this service at the Practice Location, where different from above)*

Salutation ☐ Dr. ☐ Mr. ☐ Miss ☐ Mrs. ☐ Ms.	First Name *	Last Name *	
Business Telephone * *(incl. Extension)*	Is voicemail available (Yes/No)	Alternate telephone number	Business E-mail

1E – System Security Contact *(Please provide the name of a technical contact who provides support for this service at the Practice Location, where different from above)*

Salutation ☐ Dr. ☐ Mr. ☐ Miss ☐ Mrs. ☐ Ms.	First Name *	Last Name *	
Business Telephone * *(incl. Extension)*	Is voicemail available (Yes/No)	Alternate telephone number	Business E-mail

Part 1 – Practice Information	
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.
Business Telephone (including Extension)*	Enter the business telephone number and extension where the helpdesk support contact can be reached.
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.