eHealth Ontario
It's working for you

Site Support Guide

Digital Health Drug Repository

Reference Guide & Privacy and Security Procedures and Obligations

Version: V3.1

Ontario
eHealth Ontario

Copyright Notice

All rights reserved

Trademarks

Table of Contents

Glossary

Term	Definition
CDPS	Comprehensive Drug Profile Strategy
DHDR	Digital Health Drug Repository
EHR	Electronic Health Record
HIC	Health Information Custodian as defined by PHIPA
MOHLTC or ministry	Ministry of Health and Long-Term Care
NMS	Narcotics Monitoring System
NSAA	*Narcotics Safety and Awareness Act, 2010*
PHIPA	*Personal Health Information Protection Act, 2004*
ODB	Ontario Drug Benefit
SDM	Substitute Decision Maker

1 General Information

1.1 Purpose and Scope

This document describes the functions and associated benefits provided by the Digital Health Drug Repository (DHDR) and the related privacy and security requirements health care providers and organizations using the DHDR must adhere to.

The site support guide is intended for organizations that have signed or will sign the appropriate eHealth Ontario Electronic Health Record (EHR) interface agreement, acting as a service provider to eHealth Ontario when connecting new users and sites to the DHDR service. The guide provides information regarding support and maintenance as well as privacy and security procedures and obligations.

1.2 Related Documents

This guide should be read in conjunction with the following related documents:

- eHealth Ontario Privacy and Data Protection Policy
- eHealth Ontario Personal Health Information Privacy Policy
- eHealth Ontario Personal Information Privacy Policy
- eHealth Ontario Privacy Complaints and Inquiries Policy and Procedure
- eHealth Ontario Privacy Incident and Breach Management Policy
- eHealth Ontario Privacy Policy on the Responsibilities of Third Party Service Providers
- eHealth Ontario Acceptable Use Policy
- ONE ID Registrant Reference Guide
- Information Security Policy
- Acceptable Use of Information and Information Technology Policy Federation Identity Provider Standard
- Personal Health Information Protection Act, 2004
- eHealth Ontario Service Interaction Guide

EHR Security Policies

- Acceptable Use of Information and Information Technology Policy
- Access Control and Identity Management Policy for System Level Access
- Business Continuity Policy
- Cryptography Policy
- Electronic Service Provider Policy
- Information Security Incident Management Policy
- Information and Asset Management Policy
- Information Security Policy
- Local Registration Authority Practices Policy
- Security Logging and Monitoring Policy
- Network and Operations Policy
- Physical Security Policy
- System Development Lifecycle Policy
- Threat Risk Management Policy

EHR Privacy Policies

- EHR Assurance Policy
- EHR Logging and Auditing Policy

- EHR Privacy and Security Training Policy
- EHR Retention Policy
- EHR Access and Correction Policy
- EHR Consent Management Policy
- EHR Inquiries and Complaints Policy
- EHR Privacy Breach Management Policy

The EHR privacy and security policies and related documents can be found at http://ehealthontario.on.ca/en/about-us/our-privacy-commitment/ and http://ehealthontario.on.ca/en/about-us/security

The Federation Identity Provider Standard can be found at:
http://www.ehealthontario.on.ca/images/uploads/support/eHealth_Ontario_Federation_Identity_Provider_Standard_EN.pdf

2 Service Description

Medication-related problems, such as drug interactions and adverse drug events, continue to present a burden on healthcare and have been identified by health care providers as contributors to morbidity and mortality and patients' use of the health system.

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

The DHDR is designed with capacity to accommodate medication information for "All Drugs, All People" in Ontario and it offers web services for integration (e.g., through clinical viewers) to connected systems supporting Electronic Health Records (EHR) in the province. The objective is to facilitate incremental access to dispensed drug events and pharmacy service information. These include ministry drug data holdings (e.g., Ontario Drug Benefit (ODB) and Narcotics Monitoring System (NMS) data) and over time, the DHDR will expand further to include pharmacy data holdings for drugs paid for directly by patients or by private insurance.

As part of the roadmap under the CDPS, plans will continue to develop to integrate the DHDR with other Point of Service systems such as Pharmacy Management Systems, Electronic Medical Records and Hospital Information Systems for prescribed drug events, drug utilization and medication reconciliation.

The DHDR supports the long-term CDPS vision of 'All Drugs, All People' and contributes to the broader goal of a connected Ontario health care system.

More information regarding the ministry's provision of access to information about publicly funded drugs and pharmacy services, as well as monitored drugs, including a "Questions and Answers" document for health care providers, can be found at: www.ontario.ca/mydruginfo

3 DHDR Data

3.1 Contents of the Data:

Health care providers (e.g. physicians, nurse practitioners and pharmacists) are able to access information about publicly funded drugs and pharmacy services, as well as all monitored drugs (regardless of payor), for the purpose of providing health care to an individual.

For more information, please refer to the link: Information Available to Health Care Providers through the Digital Health Drug Repository.

For drugs, health care providers are able to view the dispensed date, name, strength, dosage form, quantity and estimated days' supply of the drugs which have been dispensed to a patient. In addition, prescriber and pharmacy information is displayed.

For pharmacy services, providers will see the service date, a description of the service and the pharmacy information. In some instances, prescriber information will be available, which may be the name of the pharmacist that provided the pharmacy service. Quantity and days' supply default to a value of 1.

3.2 Limitations of the Data:

DHDR data is limited to:

- Information that the ministry has the authority to disclose under the terms of the *Personal Health Information Protection Act, 2004* (PHIPA) and the *Narcotics Safety and Awareness Act, 2010* (NSAA);
- Information that has been submitted to the Ontario Public Drug Programs claims adjudication system or Narcotics Monitoring System to date in respect of the drug and pharmacy service data described in section 3.1.

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

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

Drug products that are not provided under the conditions described in section 3.1 – including unmonitored drugs paid for directly by patients or by private insurance, over-the-counter medications, or herbal products – are not part of the information being made accessible to providers.

If a patient has blocked access to their information in the DHDR, providers will only be able to access this information with the express consent of the patient, as described in section 6.2.3 of this document. It is important that health care providers discuss the information available through the DHDR with their patients to confirm their complete list of medications to develop the Best Possible Medication History.

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

4 Support

eHealth Ontario will provide service provider organizations with support in various forms as outlined below.

Note: Within the domain of the DHDR, 'client' refers to the eHealth Ontario DHDR Service providers.

4.1 Contacting the Service Desk for Support

4.1.1 Client site helpdesk and application interface support group accountabilities

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

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

4.1.2 When should you call eHealth Ontario Service Desk?

Contact the eHealth Ontario Service Desk when you are:

- Requesting assistance with troubleshooting DHDR public key infrastructure PKI certificate issues
- Requesting assistance with troubleshooting service related interface issues
- Reporting a DHDR application error
- Reporting missing results in DHDR
- Reporting data quality issues in DHDR
- Reporting a privacy and security breach
- Inquiring about DHDR functionality
- Inquiring or reporting about the privacy and security of personal health information

4.1.3 Reporting an incident or creating a service request

Phone 1-866-250-1554
- The fastest way to report a high severity issue/incident (e.g. production is down or environment is severely degraded) is to contact eHealth Ontario Service Desk via telephone to open an incident or service request ticket.

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

4.1.4 Checklist to help expedite your ticket

Be ready with the following details:

- Your name
- Your site location
- Your contact information, include backup contacts where applicable <phone #> <email address>

- Indicate the eHealth Ontario service environment affected <e.g. production or testing>
- Description of issue <include date and time the issue occurred, the number of users impacted if known>
- Steps to reproduce issue and troubleshooting diagnostic steps taken

4.1.5 When does eHealth Ontario Service Desk contact you?

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

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

- For requesting additional information to fulfill DHDR audit reports and patient access requests
- For incident management purposes

4.1.7 Data quality assurance

The accuracy of data within DHDR is important to eHealth Ontario. Should you find missing results or incorrect data, please notify us by contacting the eHealth Ontario Service Desk.
The following information should be supplied to assist us with the investigation for missing or incorrect data:

- Your contact information <name> <phone #> <email address>
- The name of your organization or the organization that you are reporting on behalf of (e.g. physician's office, hospital, department)
- The name of the organization that submitted the data
- The information that is missing (if reporting a single missing result)
- If the DHDR information is incorrect, provide details around why this is so without including PI or PHI to the eHealth Ontario Service Desk

The eHealth Ontario Service Desk is the single point of contact for end users and service providers for opening tickets for DHDR related issues (refer to section 6.5 Correction Requests on in this guide for additional details).

4.1.8 Clinical Viewer Issues

Issues related to the interface (e.g. regional clinical viewer) used to connect to the DHDR services should be directed to their associated Help Desks.

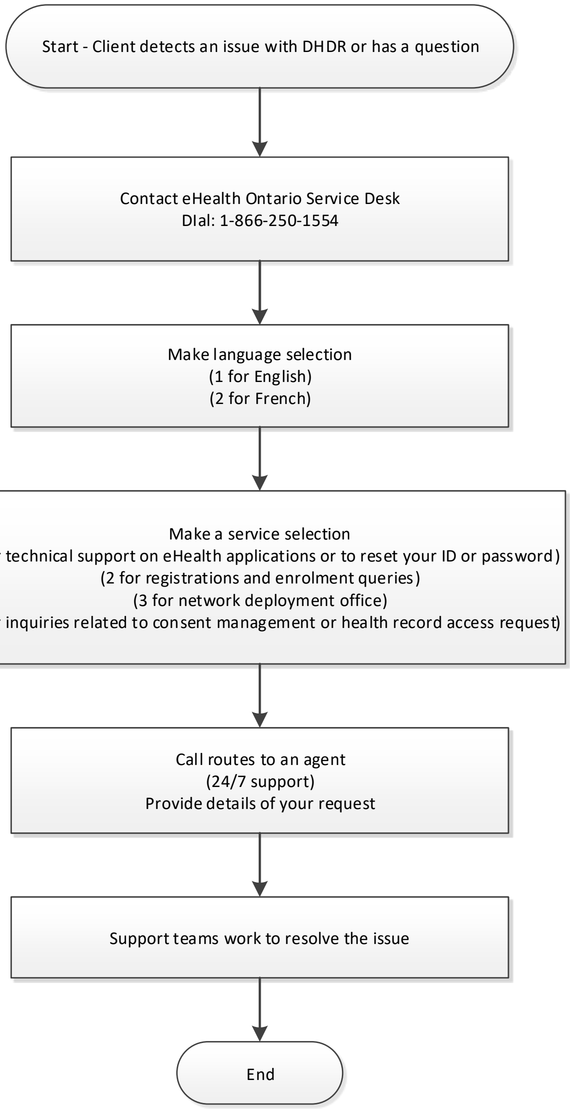
4.1.9 How to reach eHealth Ontario Service Desk

The eHealth Ontario Service Desk contact information is:

Contact Information	Phone: 1-866-250-1554 Fax: 416-586-4040 (Please phone the eHealth Ontario Service Desk to notify them when faxing any information related to an incident or service request.)

	Email: servicedesk@ehealthontario.on.ca *Note: Phone is the primary method of contact for the eHealth Ontario Service Desk. There is currently no service level agreement for incidents or service requests via email.*
Hours of Operation	**Service Desk**: 7/24/365 to call to report all incidents or create service requests

Incident Management Support Flow


Start - Client detects an issue with DHDR or has a question
Contact eHealth Ontario Service Desk
DIal: 1-866-250-1554
Make language selection
(1 for English)
(2 for French)
Make a service selection
(1 for technical support on eHealth applications or to reset your ID or password)
(2 for registrations and enrolment queries)
(3 for network deployment office)
(4 for inquiries related to consent management or health record access request)
Call routes to an agent
(24/7 support)
Provide details of your request
Support teams work to resolve the issue
End

4.1.10 Incident ticket escalation process

Step 1 Open ticket	- Contact eHealth Ontario to open a ticket at 1-866-250-1554 - Choose “technical support” 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 Support Team as necessary - The support agent may request additional information from you to assist in troubleshooting or service request fulfillment process - Once all action items have been completed, if the Service Desk agent cannot resolve the problem or fulfill the service request, it will be escalated to eHealth Ontario’s and other next level support teams
Step 3 Issue escalated to eHealth Ontario’s and other next level support teams	- Incident ticket is assigned to the next level of support - Assigned next level of support contacts you - The next level of support reviews incident or service request and continues troubleshooting or service request activities where required, other support teams are engaged

4.1.11 Progress of your incident ticket

Updates - Automated updates are provided as the incident ticket is escalated among teams. Feel free to review the progress of your incident ticket by contacting the eHealth Ontario Service Desk anytime.

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

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

4.1.12 Client satisfaction

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

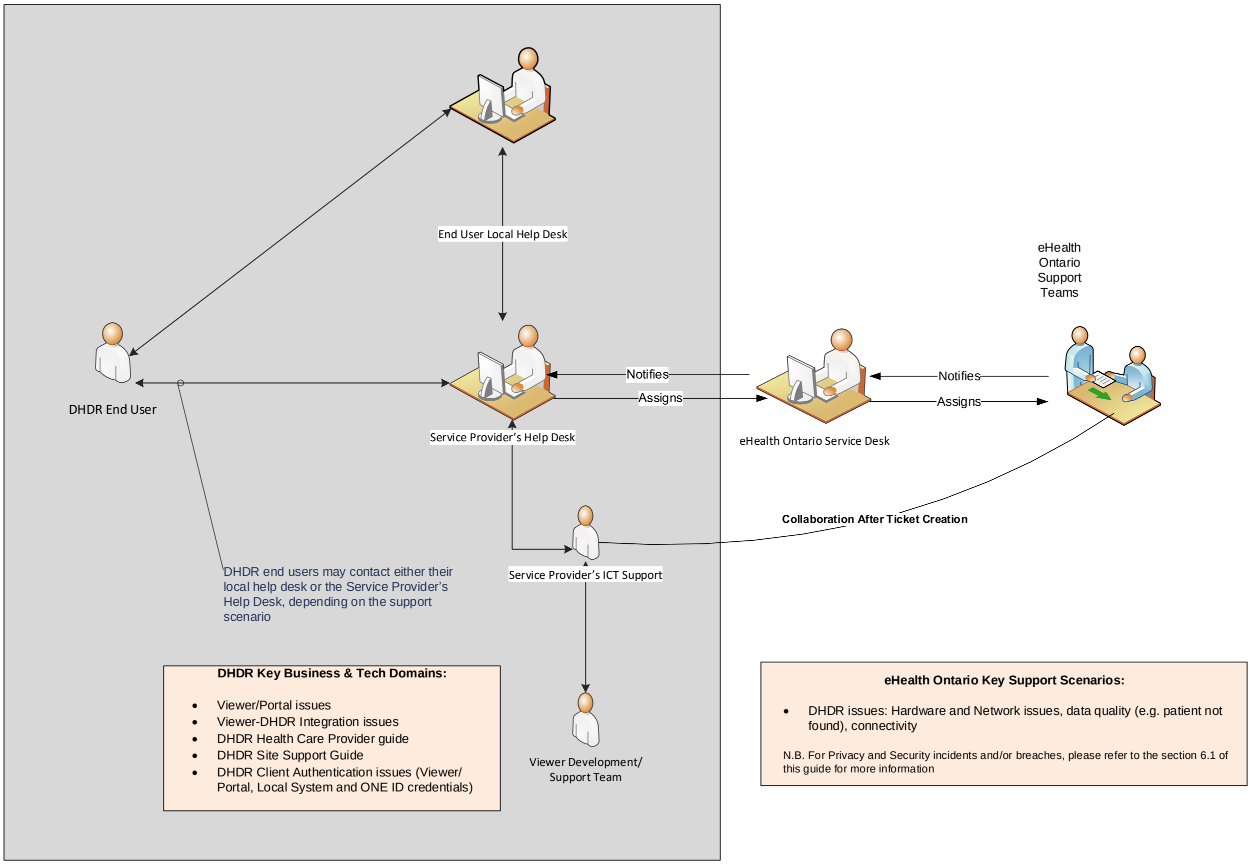
Client satisfaction survey

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

General feedback

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

4.2 Support Processes



DHDR end users may contact either their local help desk or the Service Provider's Help Desk, depending on the support scenario

DHDR Key Business & Tech Domains:

- Viewer/Portal issues
- Viewer-DHDR Integration issues
- DHDR Health Care Provider guide
- DHDR Site Support Guide
- DHDR Client Authentication issues (Viewer/ Portal, Local System and ONE ID credentials)

eHealth Ontario Key Support Scenarios:

- DHDR issues: Hardware and Network issues, data quality (e.g. patient not found), connectivity

N.B. For Privacy and Security incidents and/or breaches, please refer to the section 6.1 of this guide for more information

5 Operational Responsibilities for DHDR Data

5.1 Temporary Unblocking of Access Reporting

DHDR permits health care providers to access a patient's blocked DHDR data with express consent from the patient or the patient's substitute decision-maker (SDM). When this occurs, eHealth Ontario will coordinate with ServiceOntario to send a letter directly to the patient with details of the temporary unblocking of access event. Additionally, eHealth Ontario will provide a report of all temporary unblocking of access actions performed on DHDR data within an organization to the Privacy Officer of that organization.

5.2 Audit Logs and Reports

Under the *Personal Health Information Protection Act, 2004* (PHIPA), eHealth Ontario is responsible for keeping an electronic record of all accesses to DHDR data whether held in an eHealth Ontario system or a third party system. Due to this legislative requirement, eHealth Ontario must have access to a copy of the audit logs. eHealth Ontario may be asked to provide an audit report on these access logs.
At this time, the following audit reports are available to participating health care organizations:

1. DHDR System User Activity Report (or 'organization request'): A report of all users in a particular organization who have accessed DHDR data in the timeframe set out in the request.
2. DHDR Particular User Activity Report (or 'user request'): a report of all accesses to DHDR data by a particular user at an organization in the timeframe set out in the request.
3. DHDR Patient Report (or 'patient request'): a report of all users in an organization who have accessed a particular patient's DHDR data (note: this report is only available by request of the patient).
4. Temporary Unblocking of Access Report.

5.3 Patient Access Requests

Patients may request access to their personal health information in DHDR or request reports on who has accessed their personal health information in DHDR or request their consent directive history. Depending on the type of request (see section 6.3 of this guide), the request is fulfilled by MOHLTC or by the organization (HIC) that received the request.

6 Privacy and Security

6.1 Privacy and Security Obligations

As health information custodians (HICs) of patient personal health information, health care providers have obligations under PHIPA and Ontario Regulation 329/04 (O.Reg. 329/04).

In accordance with PHIPA, health care providers may only access the DHDR to collect drug and pharmacy service information for the purpose of providing health care, or assisting in the provision of health care, to his / her patients. HICs and their agents are NOT permitted to access the service to collect DHDR data for any other purpose, including, but not limited to, research.

When collecting, using, or disclosing DHDR data, each health care provider is responsible for ensuring that he or she and his or her employees, agents and service providers handling personal health information on the provider’s behalf are in compliance with their obligations set out in:

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

A useful overview of security best practices for small medical offices (for example, family health teams) and larger, more complex organizations (for example, hospitals) can be found on the eHealth Ontario website at http://www.ehealthontario.on.ca/about-us/security/guides.

6.2 Patient Consent

6.2.1 Consent Management

Quick Tip

The DHDR gives patients, or their substitute decision maker (SDM), the option to exercise a consent directive by blocking or unblocking access to their patient data. If a patient wishes to block access to his / her information in the DHDR, or wishes to unblock access (remove the restriction), he / she can call ServiceOntario INFOline toll-free at 1-800-291-1405 (TTY 1-800-387-5559).

The DHDR gives patients or their SDM the option to block access to the patient data that is available within the service. If a patient blocks access to his/her data, health care providers querying the DHDR will not be able to access any patient information unless the health care provider performs a temporary unblocking of access based on express consent from the patient or the patient's SDM at the point of care. Please refer to Appendix B for more details.

6.2.2 Blocking and Unblocking Access

If a patient wishes to block access to his/her information in the DHDR, or wishes to unblock access (remove the restriction), he/she can call ServiceOntario INFOline toll-free at 1-800-291-1405 (TTY 1-800-387-5559) or obtain the appropriate form by downloading them from the ministry's website at www.ontario.ca/mydruginfo. For sample forms please refer to Appendix C.

6.2.3 Temporary Unblocking of Access

Quick Tip

DHDR permits health care providers to access a patient's blocked information with express consent from the patient or the patient's SDM. This will allow all health care providers within the organization access to a patient's drug and pharmacy service information for a period up to four (4) hours.

The DHDR permits health care providers to temporarily access a patient's blocked information only with express consent from the patient or the patient's SDM. The DHDR does not permit 'risk of harm' overrides on a patient's decision to block access; the ministry is the health information custodian (HIC) for the DHDR, but it is not considered to be within the patient's circle of care. Therefore, express consent is required.

All temporary unblock permissions will last for four (4) hours, after which time, access will once again be blocked. The health care provider must obtain and complete a "Temporary Unblocking of Access to Your Drug and Pharmacy Service Information" form, which is available in the clinical viewer. For a sample form please refer to Appendix D. If the patient's SDM is providing consent, the type of relationship with the patient must be included on the form. The health care provider must obtain the patient's / SDM's authorization and signature on the form and keep the form securely on file for audit purposes.

Temporary unblocking of access actions are logged in the system, along with the identity of the health care provider who obtained consent. The DHDR logs all accesses to data, and an audit of this information can be requested. In addition, a notification letter will be sent to the patient by ServiceOntario informing them of the temporary unblocking of access event(s).

6.3 Patient Access Requests

Patients may be aware that their information is being made available by the ministry, but may not be specifically aware that the “DHDR” is the technology that makes this information available. As a result, it may be necessary to clarify a patient’s request to ensure that they are provided with the appropriate response. For example, providers may need to differentiate between hospital pharmacy records accessible through ClinicalConnect and the publicly funded drug, monitored drug and pharmacy service information accessible via the DHDR.

The following types of questions correspond to the different requests that a patient may make:

Question 1: **An individual asks a provider at a particular organization: “Who from that organization has accessed my drug and/or pharmacy service information [from the DHDR]?”**
You may provide this log of access in accordance with your internal access policies and procedures. If it is not possible for you to respond to this request, forward the request to your privacy office for your privacy office to follow the steps below. If you do not have a privacy office, you may follow the steps below:

1. Contact the eHealth Ontario Service Desk at 1-866-250-1554 and request an audit report by patient. The eHealth Ontario Service Desk will open a ticket on your behalf.
2. eHealth Ontario Service Desk will provide the requestor with a blank report request form.
3. Requestor fills out form and encrypts form[1]. Encrypted form should be sent to dhdr@ehealthontario.on.ca.
4. An eHealth Ontario representative will contact the requestor for the password for the encrypted file.
5. The eHealth Ontario representative will encrypt the report and send it to you via email.
6. The eHealth Ontario representative will provide you with the password.
7. You must notify the eHealth Ontario representative if the encrypted report received cannot be opened.

Question 2: An individual asks, “Which health care providers across Ontario have accessed my drug and/or pharmacy service information [in the DHDR]?”
Should an individual wish to make a request to find out who in Ontario has accessed their drug and pharmacy service information via the DHDR in a given timeframe, please direct the individual to ServiceOntario INFOline at 1-800-291-1405 (TTY: 1-800-387-5559).

Question 3: An individual would like to know what drug and/or pharmacy service information about them is being disclosed by the ministry.
If you receive a request from an individual regarding what drug and pharmacy service information about them the MOHLTC makes available through the DHDR, please refer the individual to ServiceOntario INFOline at 1-800-291-1405 (TTY: 1-800-387-5559).

[1] For instructions on how to encrypt forms containing personal health information, see Appendix A.

Question 4: An individual would like to request the consent directive history of blocking/unblocking the access of their drug and pharmacy service information.
Should an individual wish to make a request to inquire about their consent directive history related to access to their drug and pharmacy service information via the DHDR, please direct the individual to ServiceOntario INFOline at 1-800-291-1405 (TTY: 1-800-387-5559).

6.4 Requests for DHDR Audit Reports

HICs may require a record of who from their organization accessed DHDR data via your clinical viewer system. In the event that you are unable to fulfill this requirement using your own internal system logs, you may request an access report from eHealth Ontario. eHealth Ontario is able to provide you with the following types of audit reports:

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

b. By user request: eHealth Ontario will provide a report of all accesses to DHDR data by a particular user from your organization in the timeframe set out in the request.

Note that these requests should come from the privacy office at your organization. If you do not have a privacy office, you may contact eHealth Ontario directly by following the steps below.

To request DHDR audit reports:

1. Contact the eHealth Ontario Service Desk at 1-866-250-1554 and request an audit report by user or audit report by organization. The eHealth Ontario Service Desk will open a ticket on your behalf.
2. eHealth Ontario Service Desk will provide the requestor with a blank report request form.
3. Requestor fills out form and encrypts form[2]. Encrypted form should be sent to dhdr@ehealthontario.on.ca.
4. An eHealth Ontario representative will contact the requestor for the password for the encrypted file.
5. The eHealth Ontario representative will encrypt the report and send it to you via email.
6. The eHealth Ontario representative will provide you with the password.
7. You must notify the eHealth Ontario representative if the encrypted report received cannot be opened.

6.5 Correction Requests

Patient Correction Requests
Should your patients wish to request corrections to their drug and pharmacy service information in the DHDR (e.g., incorrect or missing medications and/or pharmacy services, or corrections to patient demographic information), direct the patient to contact the ServiceOntario INFOline toll-free at 1-800-291-1405 (TTY: 1-800-387-5559).

[2] For instructions on how to encrypt forms containing personal health information, see Appendix A.

Prescriber/Pharmacy Correction Requests
If a health care provider would like to request a correction to their provider information associated with a DHDR record (e.g. missing or incorrect prescriber / pharmacy information), they should contact the eHealth Ontario Service Desk at 1-866-250-1554.

Note: Do not include any personal information or personal health information in the notification to the eHealth Ontario Service Desk.

6.6 Privacy Complaints and Inquiries

If you receive a privacy-related inquiry or complaint from a patient relating to the DHDR or his/her drug and pharmacy services information in the DHDR, the patient can contact the ServiceOntario INFOline toll-free at 1-800-291-1405 (TTY: 1-800-387-5559).

If you receive a complaint or inquiry from a patient relating to eHealth Ontario or the agency's privacy policies and procedures, the patient can submit their complaint, concern or inquiry by telephone, email, fax or mail to the eHealth Ontario Privacy Office:

eHealth Ontario Privacy Office
P.O. Box 148
Toronto, ON M5G 2C8
T: 416-946-4767
Fax: 416-586-6598
privacy@ehealthontario.on.ca

Individuals may submit anonymous complaints and inquiries; however, in order to receive a response, complaints and inquiries must include the sender's name, address, telephone number, or email address. Personal health information should not be submitted with the complaint or inquiry.

6.7 Retention

Quick Tip

HICs must retain records in accordance with their internal retention guidelines. If you have any retention questions, please consult your Privacy Officer or Health Records Department.

PHIPA requires HICs to ensure that its records are retained for a specified period, and transferred and disposed of in a secure manner. In addition, the *EHR Retention Policy* places certain retention obligations on HICs as detailed below:

Information Type	Retention Period
Personal health information in the EHR system	The longer of the following time periods: • As long as the HIC that created and contributed the personal health information to the EHR retains the PHI in its local systems; • In accordance with the retention schedule of the HIC that created and contributed the PHI to the EHR; or • 30 years after the most recent instance of personal health information being used for the purpose of providing health care; or 10 years after the patient has expired and in accordance with any applicable court order or court action or other legal requirement.
Audit logs and audit reports that contain personal health information:	30 years or when personal health information is removed from EHRs – whichever is longer.
Backups of personal health information in the EHR system and audit logs and audit reports containing PHI	Retained no longer than 2 years.
Information collected to respond to individuals related to their: ○ Request for Access or Request for Correction under PHIPA; ○ Request to make, modify, or withdraw a Consent Directive under PHIPA or ○ Inquiries or Complaints under PHIPA.	2 years after the request was made. For complaints, retain for 2 years after the complaint has been closed by the HIC, eHealth Ontario, or the IPC, whichever is longer.
Information created about an individual as part of an investigation of privacy breaches and/or security incidents.	2 years after the privacy breach has been closed by the HIC, eHealth Ontario or the Information and Privacy Commissioner of Ontario, whichever is longer.
Information used for identity provider registration that contains personal information	7 years after last use.
System-level logs, tracking logs, reports and related documents for privacy and security tasks that do not contain personal health information	For a minimum of 2 years.
Templates or resources developed by eHealth Ontario in respect of the EHR	For a minimum of 2 years.
Assurance-related documents	10 years.

Information Type	Retention Period
eHealth Ontario business documentation	For a minimum of 7 years.

Specific types of personal health information included in each of the information types can be found in the *EHR Retention Policy* at http://www.ehealthontario.on.ca/images/uploads/support/EHR_Privacy_Policies_EN.pdf.

In addition, HICs must ensure records are protected and disposed of in accordance with the *Information Security Policy* at: http://www.ehealthontario.on.ca/en/about-us/security/.

6.8 Privacy and Security Training

HICs are required to provide privacy and security training to their agents and electronic service providers prior to accessing the DHDR. The training should ensure that agents and electronic service providers are aware of their duties under applicable privacy legislation, such as PHIPA, as well as relevant privacy and security policies and procedures in respect of the EHR system. Training should be completed prior to being provisioned an account for accessing the DHDR. eHealth Ontario has developed role-based training materials to facilitate this training requirement. For information on what to include in privacy and security training, please see the *EHR Privacy and Security Training Policy* at http://www.ehealthontario.on.ca/images/uploads/support/EHR_Privacy_Policies_EN.pdf.

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

6.9 Privacy-Related Questions

If a service provider or health care provider has any questions regarding the privacy-related processes described above and incident/breach management processes, contact eHealth Ontario at 1-866-250-1554.

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

6.10 Security

Health care providers should ensure that their employees, agents and service providers handling personal health information on the provider's behalf are in compliance with the provider's obligations, and are aware of, and comply with, any specific obligations under PHIPA or the regulation applicable to the provider's employees, agents or service providers.

A useful overview of security best practices for small medical offices (for example, family health teams) and larger, more complex organizations (for example, hospitals) can be found on the eHealth Ontario website: http://www.ehealthontario.on.ca/about-us/security/guides

6.11 Privacy and Security Incident and Breach Management

Quick Tip

Service providers and HICs shall report an actual or suspected privacy or security breach or incident to eHealth Ontario by calling the 24/7 Service Desk at 1-866-250-1554 as soon as possible.

A privacy incident is:

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

A privacy breach is:

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

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

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

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

6.11.1 Instructions for Health Care Providers

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

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

It is expected that you will cooperate with any investigations conducted by eHealth Ontario in respect of any privacy or security incidents or breaches in relation to DHDR data. During an investigation by eHealth Ontario you may be required to provide additional information which may include personal health information or personal information, in order to contain or resolve the incident or breach. Any personal health information or personal information that is requested by eHealth Ontario should be sent as an encrypted document via email; this procedure is noted in Appendix A.

For a DHDR related privacy or security incident or breach, please do not contact any patient or SDM directly unless expressly directed to do so by eHealth Ontario, in writing.

6.11.2 Instructions for Privacy / Security Officers

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

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

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

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

Once a call has been logged with the Service Desk, the incident response lead will be engaged to deal with the situation. A remediation plan will be developed in consultation with the requestor.

Appendix A: Procedures for Communicating Sensitive Files via email

Overview

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

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

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

Authorized uses

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

If sending sensitive information over non secure email is an ongoing business process, considerations should be made to automate the process and use an enterprise mechanism to securely transfer the information.
eHealth Ontario's limit on email attachments is 10 MB per email.

For further assistance please contact the eHealth Ontario Service Desk at 1-866-250-1554.

Instructions to file encryption and password creation
Use of WinZip encryption software

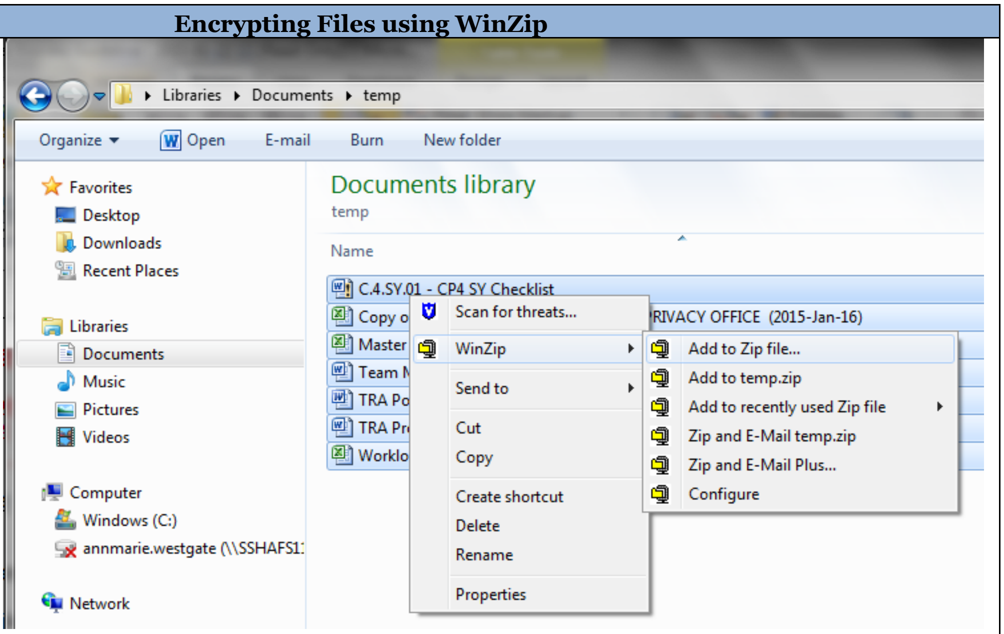
WinZip 16.0 standard versions are eHealth Ontario's suggested encryption tool.

Encrypting Files using WinZip

Step 1. Create Archive
Open the file location.

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

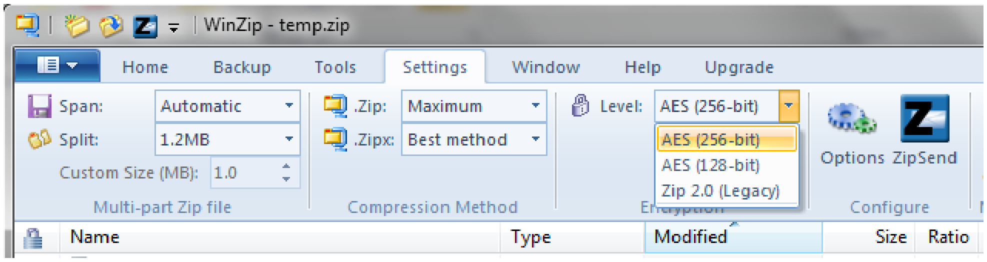
Assign the file name you wish to use.



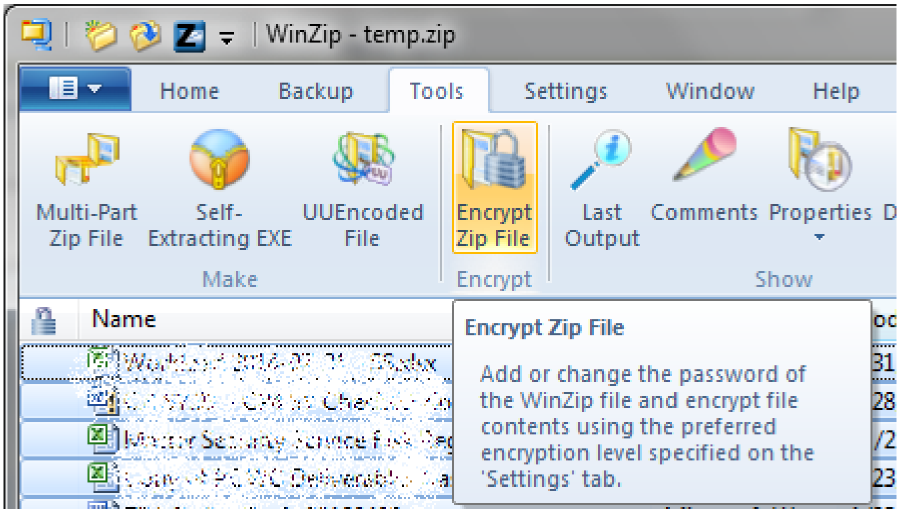
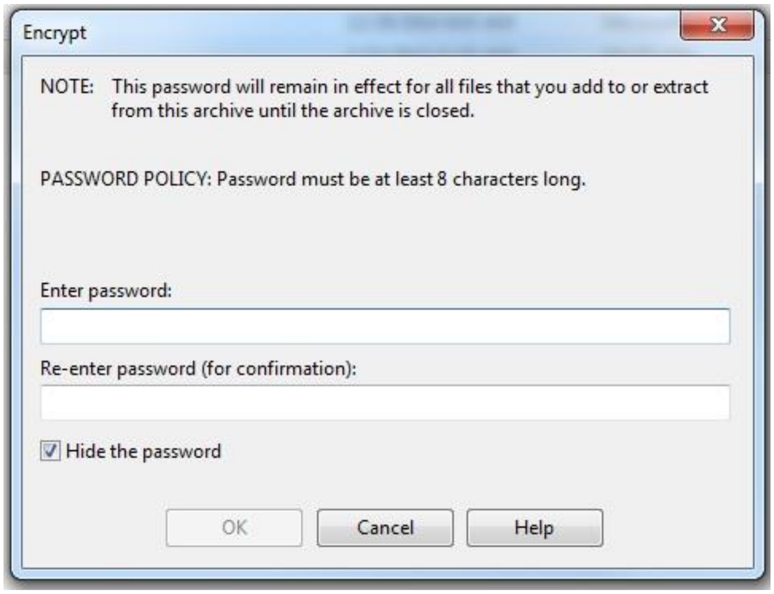
Step 1. Add files to an archive

Step 2. Open the Archive:
Double click on the zip file to open the archive.

Step 3. Choose a stronger encryption mechanism
Use AES 256-bit encryption. In the **Settings** tab, ensure the encryption level selected is **AES (256-bit)**.



Step 3 Choose an encryption mechanism

Encrypting Files using WinZip	
Step 4. Encrypt the entire file From the Tools menu, click on **Encrypt Zip File**	 WinZip - temp.zip Home Backup Tools Settings Window Help Multi-Part Zip File Self-Extracting EXE UUEncoded File Make Encrypt Zip File Encrypt Last Output Comments Properties Show Name Encrypt Zip File Add or change the password of the WinZip file and encrypt file contents using the preferred encryption level specified on the 'Settings' tab. **Step 4.** Encrypt the Zip File
Step 5. Create a strong password Enter a password and then confirm it. See below, for how to create a strong password.	 Encrypt NOTE: This password will remain in effect for all files that you add to or extract from this archive until the archive is closed. PASSWORD POLICY: Password must be at least 8 characters long. Enter password: Re-enter password (for confirmation): ☑ Hide the password **Fig.4** Create a strong password

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

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

File transfer, and sharing
Once the file has been encrypted and password protected it is temporarily saved to the network share or local hard drive share. The password should be communicated by phone to the file recipient or by using an "out of band" method (e.g. if emailing the document, send password by phone, fax or mail). In other words, the password should not be sent at the same time using the same method as the encrypted file.

The following requirements apply to password management:

Password creation

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

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

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

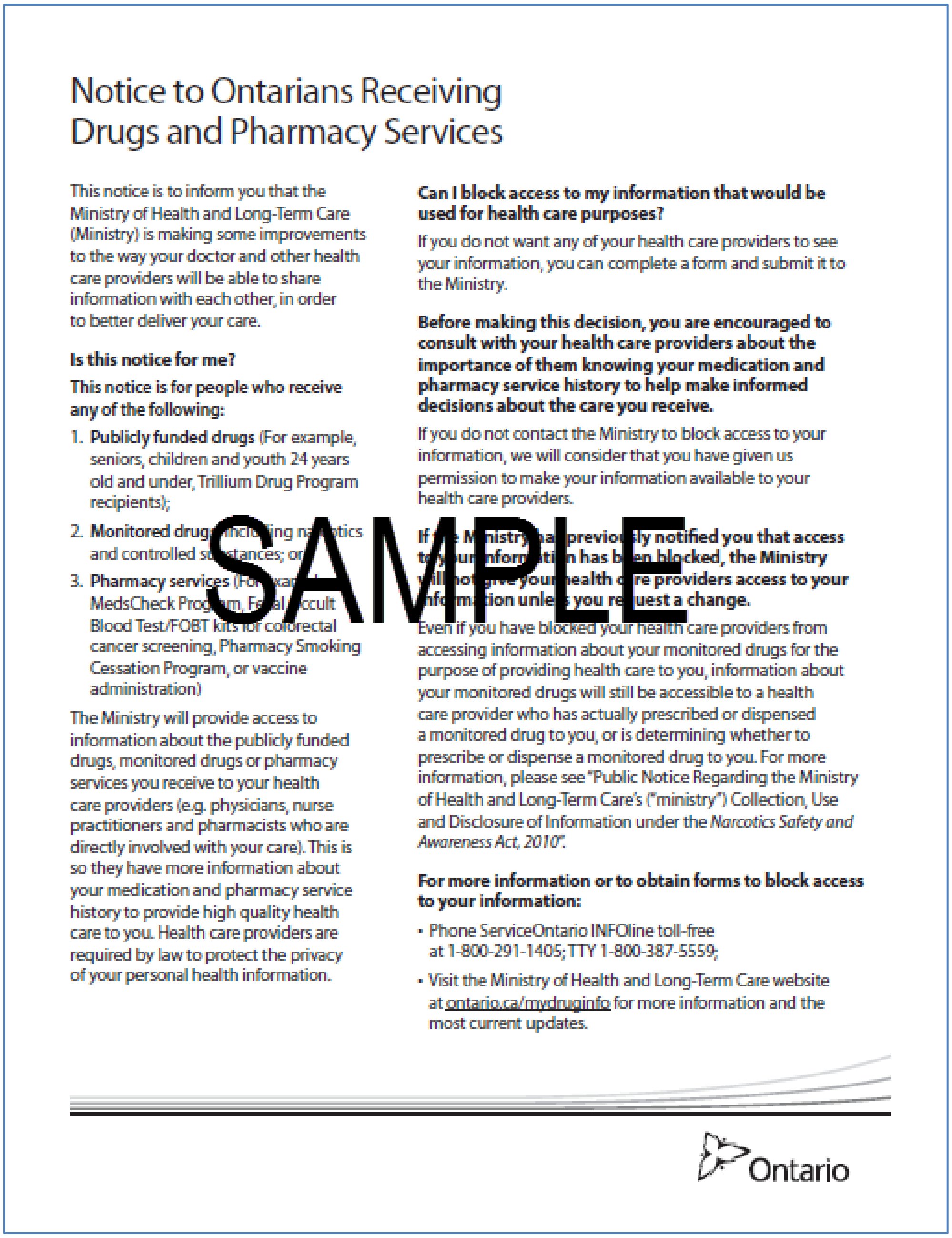
- Determine the authorized recipient of the information
- Make the encrypted file available to the recipient using agreed process (e.g. SFTP, email)
- The requestor calls the sender by phone
- The sender verbally verifies the recipient's identity:
    - name
    - title, business unit, organization
    - name of received / retrieved encrypted file
- Verbally provide the verified recipient with the password to open the encrypted file
- Request and obtain verbal confirmation that the recipient has been able to extract the file(s)
- The sender securely destroys the written copy (if any) of the password and deletes any copies of the file from any local or network drives

Password recovery
WinZip does not provide a mechanism for password recovery. Therefore, in the case of long term storage of encrypted files, a method of password recovery must be in place to access these files (e.g. if an employee leaves and their files need to be accessed).
An example of a password recovery method is storing the password in a sealed envelope which can only be accessed by upper management and will only be accessed for password recovery purposes.

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

Appendix B: Notice to Ontarians Receiving Drugs and Pharmacy Services

A sample of the document is provided below. Please refer to the link Notice to Ontarians Receiving Drugs and Pharmacy Services for the latest version of the document.



Notice to Ontarians Receiving Drugs and Pharmacy Services

This notice is to inform you that the Ministry of Health and Long-Term Care (Ministry) is making some improvements to the way your doctor and other health care providers will be able to share information with each other, in order to better deliver your care.

Is this notice for me?

This notice is for people who receive any of the following:

1. **Publicly funded drugs** (For example, seniors, children and youth 24 years old and under, Trillium Drug Program recipients);
2. **Monitored drugs** (including narcotics and controlled substances; or
3. **Pharmacy services** (For example, MedsCheck Program, Fecal Occult Blood Test/FOBT kits for colorectal cancer screening, Pharmacy Smoking Cessation Program, or vaccine administration)

The Ministry will provide access to information about the publicly funded drugs, monitored drugs or pharmacy services you receive to your health care providers (e.g. physicians, nurse practitioners and pharmacists who are directly involved with your care). This is so they have more information about your medication and pharmacy service history to provide high quality health care to you. Health care providers are required by law to protect the privacy of your personal health information.

Can I block access to my information that would be used for health care purposes?

If you do not want any of your health care providers to see your information, you can complete a form and submit it to the Ministry.

Before making this decision, you are encouraged to consult with your health care providers about the importance of them knowing your medication and pharmacy service history to help make informed decisions about the care you receive.

If you do not contact the Ministry to block access to your information, we will consider that you have given us permission to make your information available to your health care providers.

If the Ministry has previously notified you that access to your information has been blocked, the Ministry will not give your health care providers access to your information unless you request a change.

Even if you have blocked your health care providers from accessing information about your monitored drugs for the purpose of providing health care to you, information about your monitored drugs will still be accessible to a health care provider who has actually prescribed or dispensed a monitored drug to you, or is determining whether to prescribe or dispense a monitored drug to you. For more information, please see "Public Notice Regarding the Ministry of Health and Long-Term Care's ("ministry") Collection, Use and Disclosure of Information under the *Narcotics Safety and Awareness Act, 2010*".

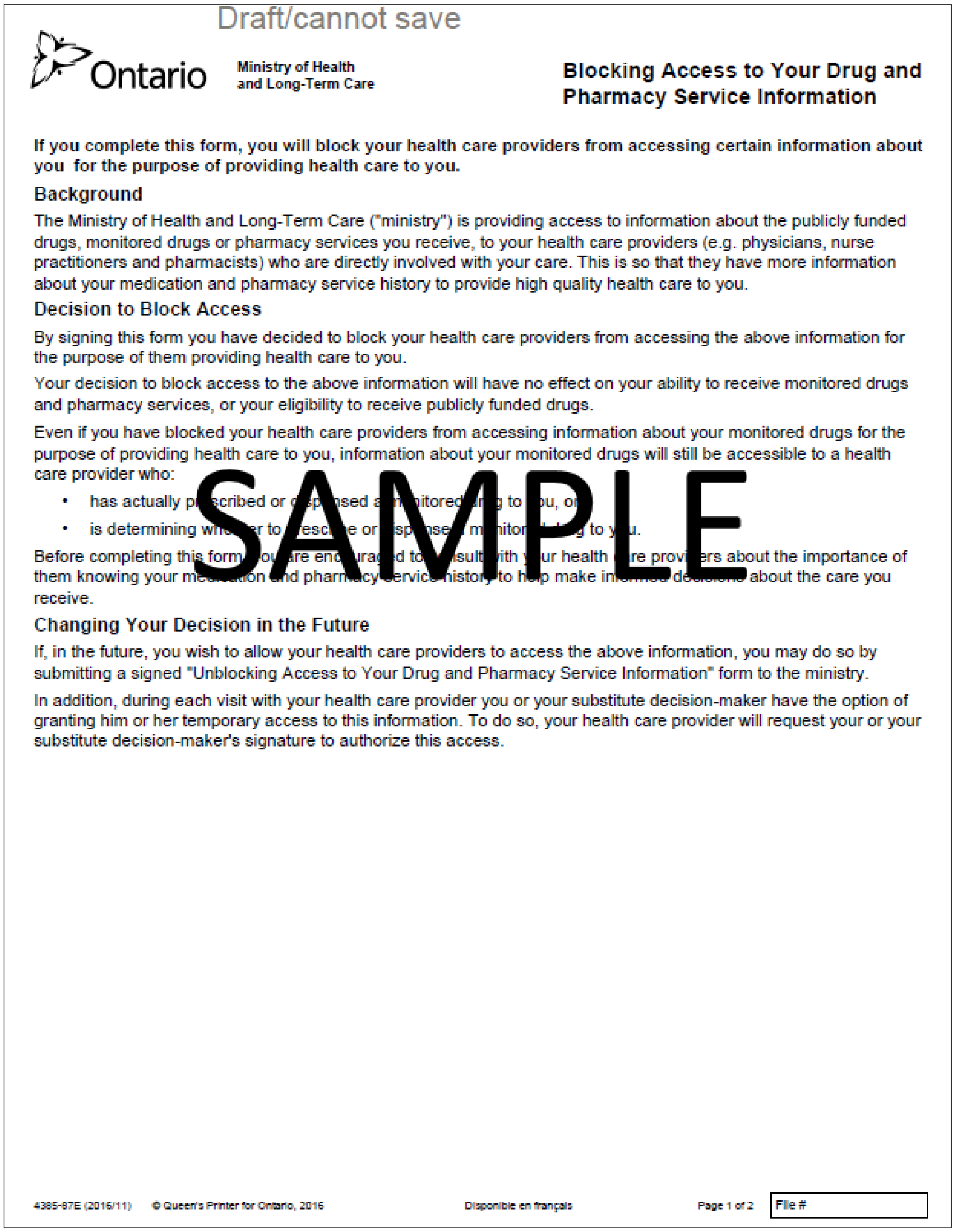
For more information or to obtain forms to block access to your information:

- Phone ServiceOntario INFOline toll-free at 1-800-291-1405; TTY 1-800-387-5559;
- Visit the Ministry of Health and Long-Term Care website at ontario.ca/mydruginfo for more information and the most current updates.

Ontario

Appendix C: Blocking and Unblocking Access Forms

Patients may register a consent directive to block or unblock access to their drug and pharmacy service information in DHDR by completing the appropriate form and submitting it to the ministry. Your patients can obtain these forms by calling ServiceOntario INFOline toll-free at 1-800-291-1405 (TTY 1-800-387-5559) or by downloading them from the ministry's web site at www.ontario.ca/mydruginfo.



Ontario Ministry of Health and Long-Term Care

Blocking Access to Your Drug and Pharmacy Service Information

If you complete this form, you will block your health care providers from accessing certain information about you for the purpose of providing health care to you.

Background

The Ministry of Health and Long-Term Care ("ministry") is providing access to information about the publicly funded drugs, monitored drugs or pharmacy services you receive, to your health care providers (e.g. physicians, nurse practitioners and pharmacists) who are directly involved with your care. This is so that they have more information about your medication and pharmacy service history to provide high quality health care to you.

Decision to Block Access

By signing this form you have decided to block your health care providers from accessing the above information for the purpose of them providing health care to you.

Your decision to block access to the above information will have no effect on your ability to receive monitored drugs and pharmacy services, or your eligibility to receive publicly funded drugs.

Even if you have blocked your health care providers from accessing information about your monitored drugs for the purpose of providing health care to you, information about your monitored drugs will still be accessible to a health care provider who:

- has actually prescribed or dispensed a monitored drug to you, or
- is determining whether to prescribe or dispense a monitored drug to you.

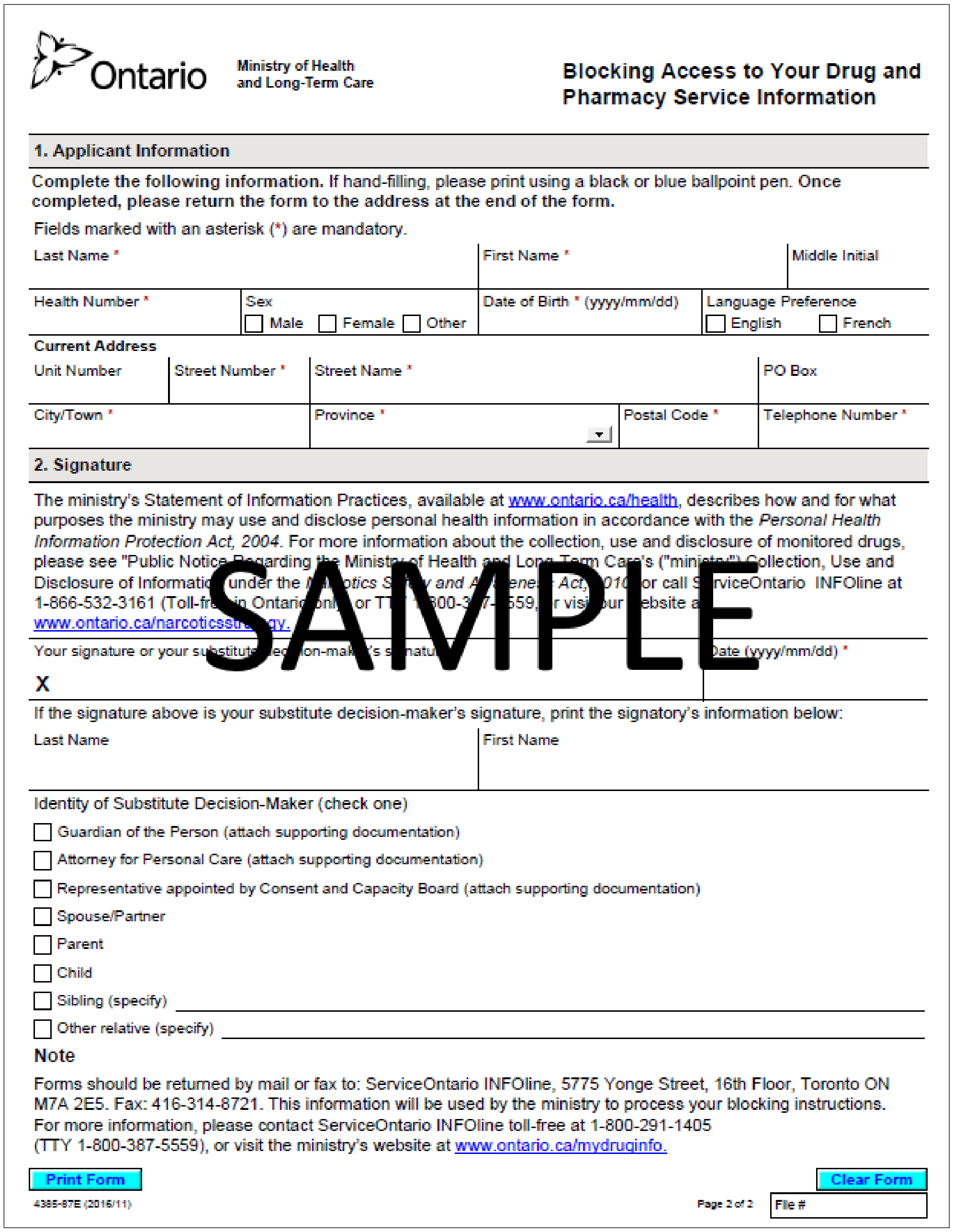
Before completing this form, you are encouraged to consult with your health care providers about the importance of them knowing your medication and pharmacy service history to help make informed decisions about the care you receive.

Changing Your Decision in the Future

If, in the future, you wish to allow your health care providers to access the above information, you may do so by submitting a signed "Unblocking Access to Your Drug and Pharmacy Service Information" form to the ministry.

In addition, during each visit with your health care provider you or your substitute decision-maker have the option of granting him or her temporary access to this information. To do so, your health care provider will request your or your substitute decision-maker's signature to authorize this access.

4385-87E (2016/11) © Queen's Printer for Ontario, 2016 Disponible en français Page 1 of 2 File #



Ontario Ministry of Health and Long-Term Care

Blocking Access to Your Drug and Pharmacy Service Information

1. Applicant Information

Complete the following information. If hand-filling, please print using a black or blue ballpoint pen. Once completed, please return the form to the address at the end of the form.

Fields marked with an asterisk (*) are mandatory.

Last Name *		First Name *	Middle Initial
Health Number *	Sex □ Male □ Female □ Other	Date of Birth * (yyyy/mm/dd)	Language Preference □ English □ French

Current Address

Unit Number	Street Number *	Street Name *		PO Box
City/Town *		Province *	Postal Code *	Telephone Number *

2. Signature

The ministry's Statement of Information Practices, available at www.ontario.ca/health, describes how and for what purposes the ministry may use and disclose personal health information in accordance with the *Personal Health Information Protection Act, 2004*. For more information about the collection, use and disclosure of monitored drugs, please see "Public Notice Regarding the Ministry of Health and Long-Term Care's ("ministry") Collection, Use and Disclosure of Information under the *Narcotics Safety and Awareness Act, 2010* or call ServiceOntario INFOline at 1-866-532-3161 (Toll-free in Ontario only) or TTY 1-800-387-5559, or visit our website at www.ontario.ca/narcoticsstrategy.

Your signature or your substitute decision-maker's signature *

X

Date (yyyy/mm/dd) *

If the signature above is your substitute decision-maker's signature, print the signatory's information below:

Last Name

First Name

Identity of Substitute Decision-Maker (check one)

□ Guardian of the Person (attach supporting documentation)

□ Attorney for Personal Care (attach supporting documentation)

□ Representative appointed by Consent and Capacity Board (attach supporting documentation)

□ Spouse/Partner

□ Parent

□ Child

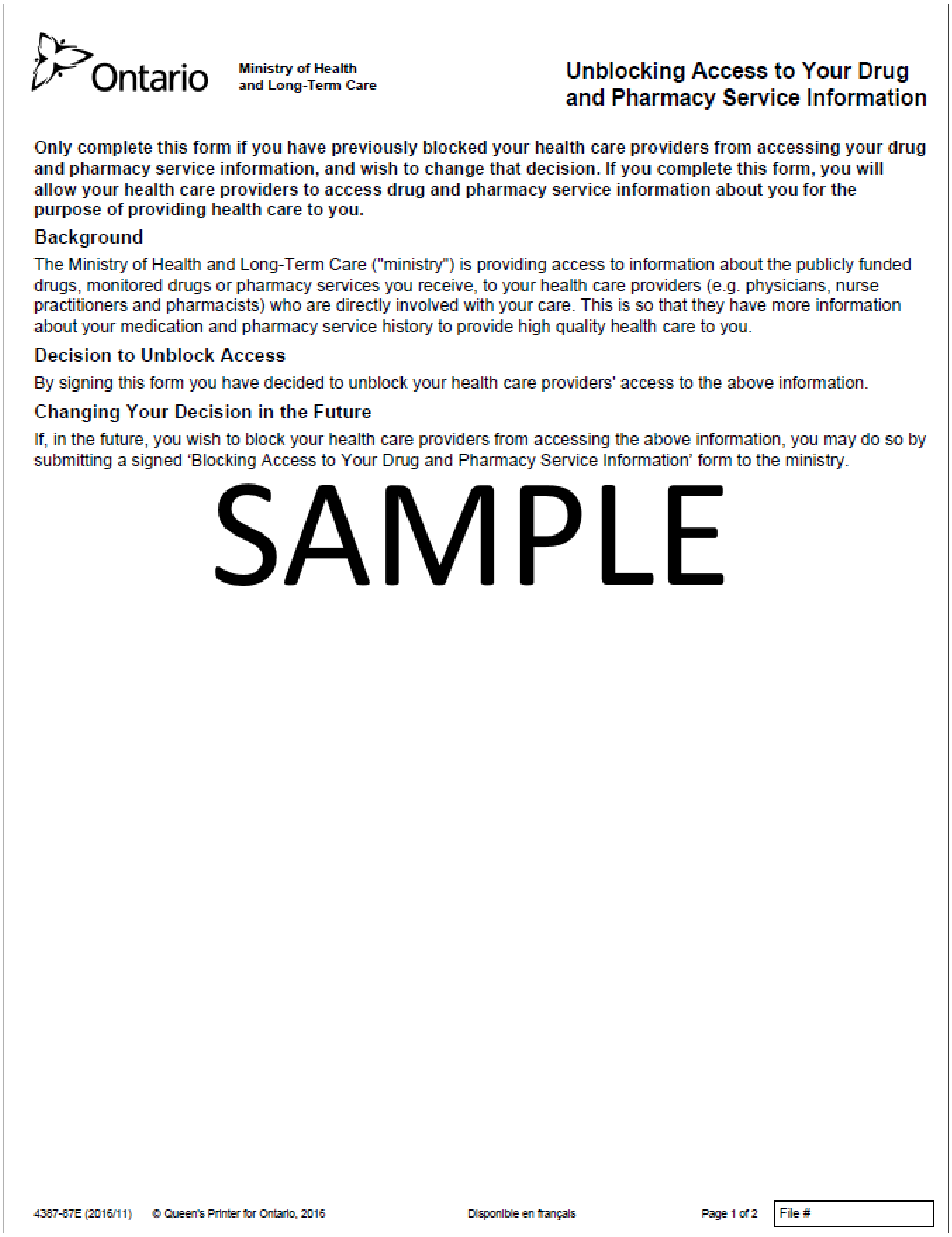
□ Sibling (specify) ____________________

□ Other relative (specify) ____________________

Note

Forms should be returned by mail or fax to: ServiceOntario INFOline, 5775 Yonge Street, 16th Floor, Toronto ON M7A 2E5. Fax: 416-314-8721. This information will be used by the ministry to process your blocking instructions. For more information, please contact ServiceOntario INFOline toll-free at 1-800-291-1405 (TTY 1-800-387-5559), or visit the ministry's website at www.ontario.ca/mydruginfo.

4385-87E (2016/11) Page 2 of 2 File #



Ontario Ministry of Health and Long-Term Care

Unblocking Access to Your Drug and Pharmacy Service Information

Only complete this form if you have previously blocked your health care providers from accessing your drug and pharmacy service information, and wish to change that decision. If you complete this form, you will allow your health care providers to access drug and pharmacy service information about you for the purpose of providing health care to you.

Background

The Ministry of Health and Long-Term Care ("ministry") is providing access to information about the publicly funded drugs, monitored drugs or pharmacy services you receive, to your health care providers (e.g. physicians, nurse practitioners and pharmacists) who are directly involved with your care. This is so that they have more information about your medication and pharmacy service history to provide high quality health care to you.

Decision to Unblock Access

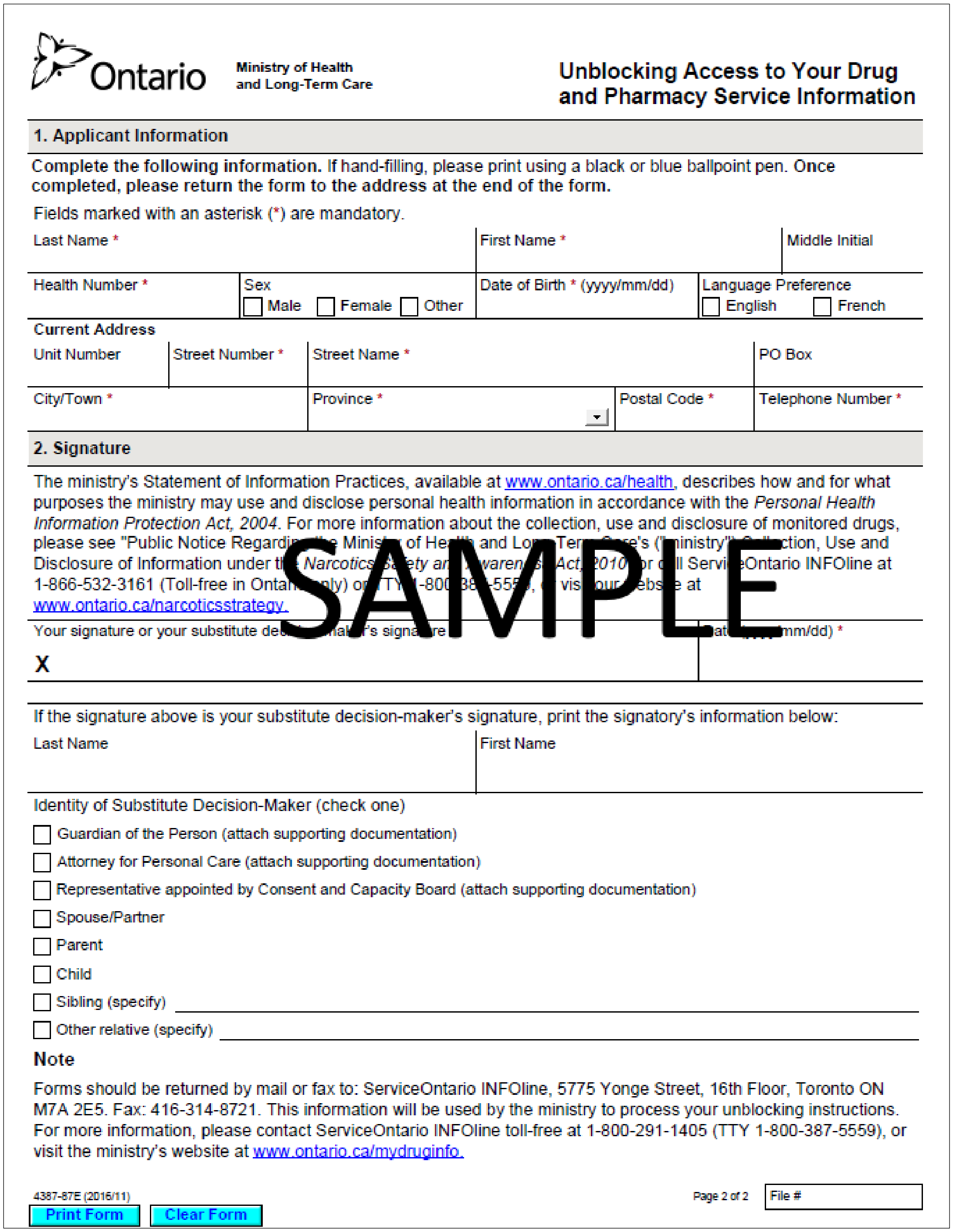
By signing this form you have decided to unblock your health care providers' access to the above information.

Changing Your Decision in the Future

If, in the future, you wish to block your health care providers from accessing the above information, you may do so by submitting a signed 'Blocking Access to Your Drug and Pharmacy Service Information' form to the ministry.

Disponible en français

File #



Ontario Ministry of Health and Long-Term Care

Unblocking Access to Your Drug and Pharmacy Service Information

1. Applicant Information

Complete the following information. If hand-filling, please print using a black or blue ballpoint pen. **Once completed, please return the form to the address at the end of the form.**

Fields marked with an asterisk (*) are mandatory.

Last Name * | First Name * | Middle Initial

Health Number * | Sex □ Male □ Female □ Other | Date of Birth * (yyyy/mm/dd) | Language Preference □ English □ French

Current Address

Unit Number | Street Number * | Street Name * | PO Box

City/Town * | Province * | Postal Code * | Telephone Number *

2. Signature

The ministry's Statement of Information Practices, available at www.ontario.ca/health, describes how and for what purposes the ministry may use and disclose personal health information in accordance with the *Personal Health Information Protection Act, 2004*. For more information about the collection, use and disclosure of monitored drugs, please see "Public Notice Regarding the Ministry of Health and Long-Term Care's ("ministry") Collection, Use and Disclosure of Information under the *Narcotics Safety and Awareness Act, 2010*" or call ServiceOntario INFOline at 1-866-532-3161 (Toll-free in Ontario only) or TTY 1-800-387-5559, or visit our website at www.ontario.ca/narcoticsstrategy.

Your signature or your substitute decision-maker's signature | Date (yyyy/mm/dd) *

X

If the signature above is your substitute decision-maker's signature, print the signatory's information below:

Last Name | First Name

Identity of Substitute Decision-Maker (check one)

□ Guardian of the Person (attach supporting documentation)

□ Attorney for Personal Care (attach supporting documentation)

□ Representative appointed by Consent and Capacity Board (attach supporting documentation)

□ Spouse/Partner

□ Parent

□ Child

□ Sibling (specify) ____________________

□ Other relative (specify) ____________________

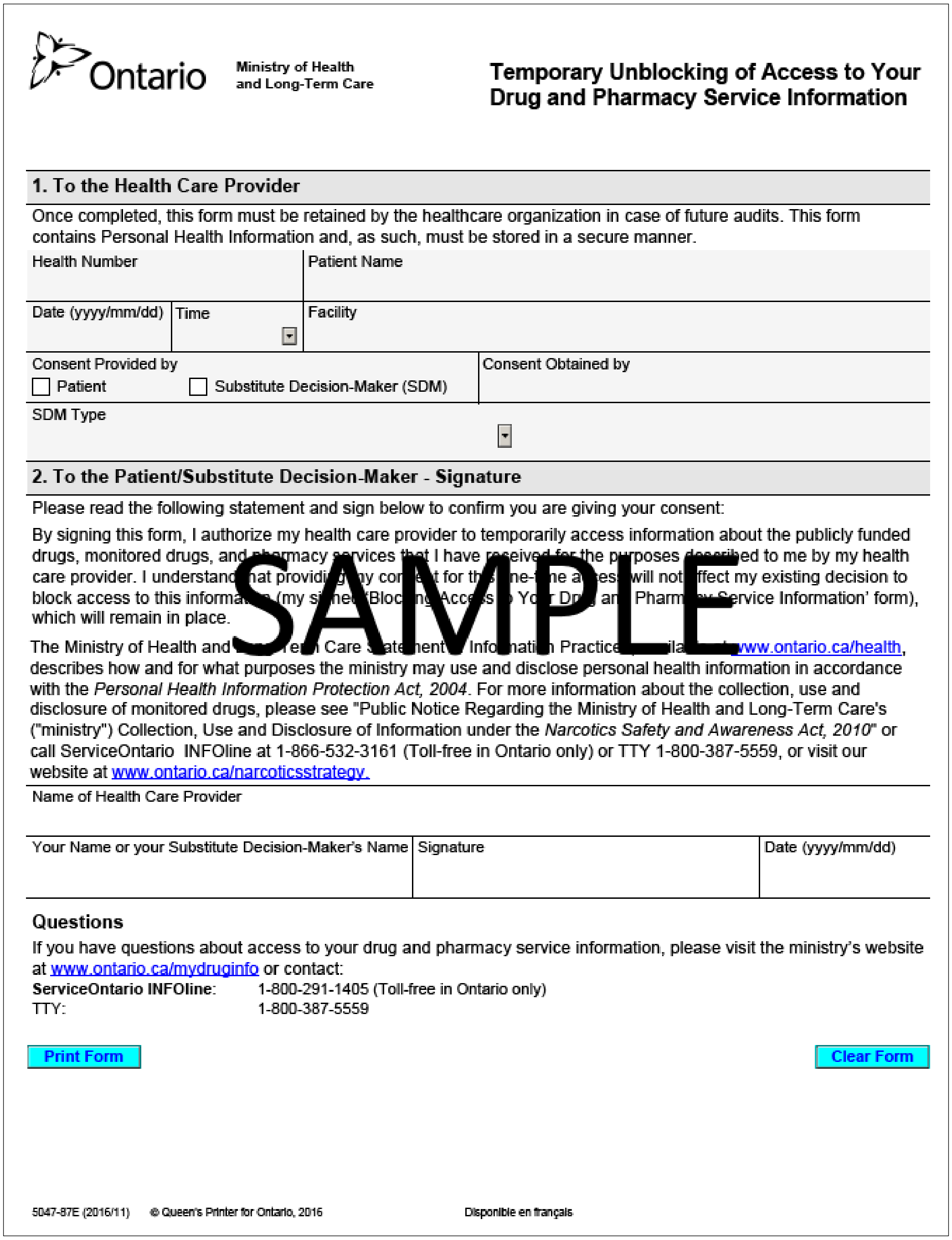
Note

Forms should be returned by mail or fax to: ServiceOntario INFOline, 5775 Yonge Street, 16th Floor, Toronto ON M7A 2E5. Fax: 416-314-8721. This information will be used by the ministry to process your unblocking instructions. For more information, please contact ServiceOntario INFOline toll-free at 1-800-291-1405 (TTY 1-800-387-5559), or visit the ministry's website at www.ontario.ca/mydruginfo.

4387-87E (2016/11) Page 2 of 2 File #

Appendix D: Temporary Unblocking of Access Form

The DHDR permits health care providers to temporarily access a patient's blocked information only with express consent from the patient or the patient's SDM. The health care provider must print and complete a "Temporary Unblocking of Access to Your Drug and Pharmacy Service Information" form, which is available in the clinical viewer. A sample of the document is provided below. Please refer to the link Temporary Unblocking of Access Form for the latest version of the document.



Ontario Ministry of Health and Long-Term Care

Temporary Unblocking of Access to Your Drug and Pharmacy Service Information

1. To the Health Care Provider

Once completed, this form must be retained by the healthcare organization in case of future audits. This form contains Personal Health Information and, as such, must be stored in a secure manner.

Health Number

Patient Name

Date (yyyy/mm/dd)

Time

Facility

Consent Provided by

□ Patient □ Substitute Decision-Maker (SDM)

Consent Obtained by

SDM Type

2. To the Patient/Substitute Decision-Maker - Signature

Please read the following statement and sign below to confirm you are giving your consent:

By signing this form, I authorize my health care provider to temporarily access information about the publicly funded drugs, monitored drugs, and pharmacy services that I have received for the purposes described to me by my health care provider. I understand that providing my consent for this one-time access will not affect my existing decision to block access to this information (my signed 'Blocking Access to Your Drug and Pharmacy Service Information' form), which will remain in place.

The Ministry of Health and Long-Term Care Statement of Information Practices, available at www.ontario.ca/health, describes how and for what purposes the ministry may use and disclose personal health information in accordance with the *Personal Health Information Protection Act, 2004*. For more information about the collection, use and disclosure of monitored drugs, please see "Public Notice Regarding the Ministry of Health and Long-Term Care's ("ministry") Collection, Use and Disclosure of Information under the *Narcotics Safety and Awareness Act, 2010*" or call ServiceOntario INFOline at 1-866-532-3161 (Toll-free in Ontario only) or TTY 1-800-387-5559, or visit our website at www.ontario.ca/narcoticsstrategy.

Name of Health Care Provider

Your Name or your Substitute Decision-Maker's Name

Signature

Date (yyyy/mm/dd)

Questions

If you have questions about access to your drug and pharmacy service information, please visit the ministry's website at www.ontario.ca/mydruginfo or contact:

ServiceOntario INFOline:	1-800-291-1405 (Toll-free in Ontario only)
TTY:	1-800-387-5559

Print Form

Clear Form

5047-87E (2016/11)

Disponible en français