

eHealth Ontario

Adopter's Site Support Guide

Provider Registry Services

Version: 1.0

January 2016

Copyright Notice

Copyright © 2016, eHealth Ontario

All rights reserved

No part of this document may be reproduced in any form, including photocopying or transmission electronically to any computer, without prior written consent of eHealth Ontario. The information contained in this document is proprietary to eHealth Ontario and may not be used or disclosed except as expressly authorized in writing by eHealth Ontario.

Trademarks

Other product names mentioned in this document may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Document Control

The electronic version of this document is recognized as the only valid version.

Approval History

APPROVER(S)	TITLE/DEPARTMENT	APPROVED DATE
Samara Strub	Privacy Analyst, Privacy	2015-11-17
Suchun Wu	Senior IT Security Consultant, Security	2015-11-17
Michael Conde	Manager, Provincial Registries	2016-01-07
Cynthia Zhang	Relationship Manager, Identity, Access and Privacy	2016-01-07

Revision History

VERSION NO.	DATE	SUMMARY OF CHANGE	CHANGED BY
1.0	2016-01-11	Initial version published	Identity, Access and Privacy

Document Sensitivity Level

Medium

Table of Contents

About This Document	2
Background.....	2
Document Approach and Scope.....	2
Audience	2
1 Introduction.....	3
1.1 Support	3
1.2 Support Processes	5
2 Operational Responsibilities for PR Data	6
2.1 Audit Logs	6
2.2 Retention and Disposal of PR Data	6
3 Privacy and Security	6
3.1 Data Inquiries.....	6
3.2 Process Inquiries	6
3.3 Incident/Breach Management.....	7
4 Appendix.....	10
4.1 PR Error Codes.....	10

About This Document

Background

The Provider Registry (PR) is the authoritative source of information for health profession data and health care service delivery locations for use by all Electronic Health Record (EHR) solutions. It facilitates the unique and accurate identification of regulated provider persons and organizations that provide health services in Ontario, or who participates in the collection, use, or disclosure of Personal Health Information (PHI) across the continuum of care. The PR contains authoritative information about regulated health professionals and organizations in Ontario that fall within the definition of Health Information Custodian (HIC) or operator of a HIC pursuant to the Personal Health Information Protection Act (PHIPA). The PR is fed by regulatory colleges, Ministry of Health and Long-Term Care databases, hospitals, and other organizations, and is managed by eHealth Ontario.

The PR is designed to:

- Positively identify regulated provider persons;
- Provide information on providers (e.g. licensing status, practice locations).

Examples of services provided by the PR include:

- Searching and resolving a provider person's identity;
- Searching and resolving provider organization data and locations.

Document Approach and Scope

The purpose of this document is to provide post-go live site support information and guidelines for adopter organizations that use the PR. This document clearly defines the processes required for receiving support from eHealth Ontario for any PR-related issues, and assists adopters in the transition to operations.

Audience

The intended audience for this document includes any users at the adopter organization who will be interacting with the PR.

1 Introduction

The Provider Registry (PR) Adopter's Site Support Guide is a comprehensive document outlining various processes which were created to assist adopter organizations when connecting new sites to the PR. The guide provides information regarding support and maintenance as well as privacy and security procedures and obligations.

1.1 Support

The eHealth Ontario Service Desk is the primary support mechanism for all adopters of eHealth Ontario services. A description of how to engage the Service Desk, and its associated processes, is provided below.

1.1.1 Contacting the Service Desk for Support

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

How to reach eHealth Ontario Service Desk:

Service Desk – open 7 days per week, 24 hrs per day

Local: (905) 826-5551
Toll Free: 1-866-250-1554
Option 1 – Technical support (existing Adopter)
Option 2 – Registration support (new Adopter)
Email: servicedesk@ehealthontario.on.ca

For a list of other contacts within eHealth Ontario, visit: <http://www.ehealthontario.on.ca/en/contact>

1.1.2 Creating a Service Request

Telephone – Suggested method to create a high severity issue/incident (e.g. production is down or environment is severely degraded).

Email – Suggested method to create a medium or low severity issue is to contact eHealth Ontario Service Desk via email.

1.1.3 Checklist to Help Expedite Service Request

✓	Activity
<input type="checkbox"/>	Name
<input type="checkbox"/>	Site location
<input type="checkbox"/>	Contact information, including backup contacts where applicable
<input type="checkbox"/>	eHealth Ontario service
<input type="checkbox"/>	eHealth Ontario service environment affected (e.g. production or conformance testing)
<input type="checkbox"/>	Description of issue (include date and time the issue occurred and the number of users impacted if known)
<input type="checkbox"/>	Steps to reproduce issue and troubleshooting diagnostic steps taken

1.1.4 Service Request Initiation & Escalation

#	Step	Description
1	Service Request	<ul style="list-style-type: none">• Adopter contacts eHealth Ontario to open a service request.• Adopter chooses service desk option from phone prompt.
2	Engagement with frontline service desk team	<ul style="list-style-type: none">• eHealth Ontario Service Desk agent works with the Adopter to identify issue(s) and commences troubleshooting steps.• eHealth Ontario's Service Desk agent may engage with an eHealth Ontario Technical Lead as necessary.• Service Desk agent may request additional information from the Adopter to assist in the troubleshooting process.• Once all action items have been completed, if the Service Desk agent cannot resolve the problem and no progress is being made on the incident, it may be escalated to eHealth Ontario's next level support team.
3	Issue escalated to eHealth Ontario next level support team	<ul style="list-style-type: none">• Issue is assigned to the next level of support.• Assigned next level of support contacts the Adopter.• Next level of support reviews the issue and continues troubleshooting activities where required.• Additional support teams are engaged to continue efforts to resolve the issue where applicable.

1.1.5 Service Request Resolution

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

Service request priority - Incident priority is determined mutually by the support agent and the Adopter.

Service request closure - A service request will be closed 15 days after the service request ticket is resolved, no further troubleshooting is possible, or the Adopter authorizes the eHealth Ontario support team to close the request. The request will alternatively be closed if no feedback has been received after three attempts to contact the Adopter. During this time, the Adopter will receive three reminders with the final reminder stating that the request will be closed the next day.

1.1.6 Adopter Satisfaction

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

Adopter satisfaction survey -

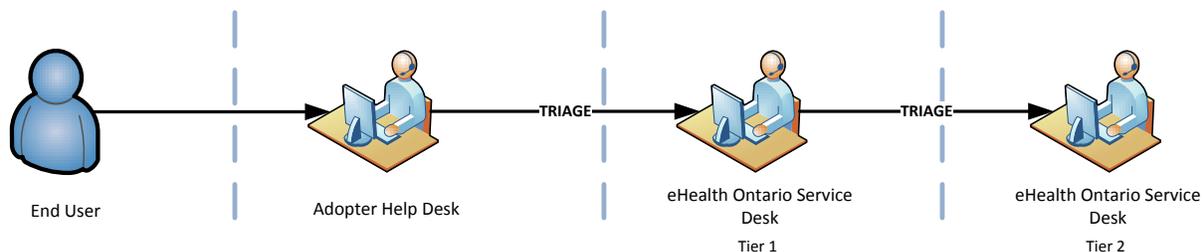
Upon closing a service request, eHealth Ontario randomly selects incidents to be surveyed. An Adopter may receive a request to fill in an online questionnaire. We appreciate adopters helping us ensure the quality of our service by completing a brief five minute survey.

General feedback -

Please email servicedesk@ehealthontario.on.ca to provide any comments or suggestions.

1.2 Support Processes

1.1.7 High Level Depiction of the PR Support Model



1.1.8 Adopter Help Desk Accountabilities

When any issues with the interface used to access PR data are detected, the Adopter help desk at each site provides support for its sites users and will assist in:

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

1.1.9 When Should an Adopter Call the eHealth Ontario Service Desk?

Contact the eHealth Ontario Service Desk when you have information on/questions regarding the following issues:

- Requesting assistance with troubleshooting PR related interface issues
- Reporting a PR application error (See [Appendix PR Error Codes Table](#))
- Reporting a privacy breach

Or, when requesting information from eHealth Ontario regarding:

- PR functionality;
- Privacy and security of PR personal information.

Note: End users should always contact their local site help desk for assistance with PR related issues. The local site help desk will then triage the issue to the eHealth Ontario Service Desk if necessary. End users **should not** contact the eHealth Ontario Service Desk without consulting their local site help desk first.

1.1.10 When does the eHealth Ontario Service Desk contact the Adopter?

- 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 PR interface; and
- To provide information regarding our release dates and application improvement activities.

1.1.11 When does the eHealth Ontario Privacy Office contact the Adopter?

- For requesting additional information to fulfill PR access requests;
- For incident management purposes.

2 Operational Responsibilities for PR Data

2.1 Audit Logs

According to our agreements with relevant regulatory colleges who contribute data to eHealth Ontario's PR, as well as agreements signed with participating Adopter organizations, eHealth Ontario is responsible for keeping an electronic record of all accesses to PR data held in an eHealth Ontario system. Due to this requirement, eHealth Ontario must have access to a copy of the Adopter organization's audit logs. eHealth Ontario may be asked to provide an audit report on these audit logs.

2.2 Retention and Disposal of PR Data

Data that is collected from the PR for use at the Adopter site should only be retained for as long as the site requires the data to carry out the permitted purposes set out in the relevant agreements. After this period, PR data should be securely disposed.

3 Privacy and Security

3.1 Data Inquiries

If an Adopter organization receives any complaints or inquiries from users or providers with respect to PR data, the site must report the inquiry or complaint to eHealth Ontario's Service Desk as soon as reasonably possible after receipt, and work with eHealth Ontario to investigate and respond to complaints that arise with respect to PR data.

3.2 Process Inquiries

If an Adopter organization receives a complaint or inquiry relating to eHealth Ontario in general (i.e. not related to PR data), or related to eHealth Ontario's privacy policies and procedures (including how to respond to individual access requests, and incident/breach management processes), the site should advise the individual to submit their complaint, concerns or inquiry by telephone, email, fax or mail to the director of privacy:

eHealth Ontario Privacy Office

P.O. Box 148

777 Bay Street, Suite 701

Toronto, ON M5G 2C8

Tel: (416) 946-4767

Fax: (416) 586-6598

Email: privacy@ehealthontario.on.ca

Note: *It is extremely important that no patient personal health information and/or personal information is disclosed in any emails to eHealth Ontario.*

3.3 Incident/Breach Management

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

- i) Incidents or breaches detected by help desk contacts at an Adopter organization;
- ii) Incidents or breaches detected by users at Adopter organizations; and
- iii) Incidents or breaches detected by eHealth Ontario which have an impact on Adopter organizations.

A privacy incident is:

- A contravention of the privacy policies, procedures or practices implemented by an Adopter organization and eHealth Ontario, where this contravention does not result in unauthorized collection, use, disclosure and destruction of PI or does not result in non-compliance with applicable privacy law.
- A contravention by an Adopter organization of any agreements entered into between eHealth Ontario and that Adopter organization, where the contravention does not constitute non-compliance with applicable privacy law.
- A contravention of agreements entered into between eHealth Ontario and an Adopter organization accessing the PR via that site's application interface, where the contravention does not constitute non-compliance with applicable privacy laws.
- A suspected privacy breach.

A privacy breach is:

- The collection, use or disclosure of PI that is not in compliance with FIPPA and its regulations.
- Circumstances where PI is stolen, lost or subject to unauthorized or inappropriate collection, use or disclosure, copying, modification, retention or disposal.

A security incident is:

- A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.
- Categorized as: malicious code, probe and scan, denial of service, unauthorized access, and inappropriate use.

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

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

Privacy or security incidents/breaches detected by an Adopter organization or its users:

1. Upon detecting a privacy or security incident/breach the users must immediately contact their local help desk and /or in-house Privacy and/or Security Lead.
2. Adopter organization designated contact(s) (authorized site contact, help desk contact and/or site Privacy/Security Lead), "the contact", connects with the eHealth Ontario service desk by telephone at 1-866-250-1554, immediately upon becoming aware of an actual or suspected privacy/security incident involving

or potentially impacting PR data; the Adopter organization's help desk or privacy officer in cooperation with eHealth Ontario is responsible for containing such privacy/security incidents and documenting any containment and/or remediation activities undertaken. No PI/PHI should be included in this documentation.

3. For a PR related privacy or security incident/breach, the contact is not to contact any provider, patient or substitute decision maker directly, unless expressly directed to do so by eHealth Ontario, in writing.
4. The service desk will open a Security Incidence Response (SIR) or a Privacy Breach Management (PBM) ticket and assign it to the corresponding team.
5. The eHealth Ontario SIR or PBM team will engage the contact to receive an update on the investigation by their site.
6. If required, the SIR or PBM lead will request a copy of any related information from the client site to assist in eHealth Ontario's own incident management activities. The logs and/or any other sensitive information should be sent to eHealth Ontario as an encrypted document via an email.
7. Adopter organization must complete all remediation activities as directed by eHealth Ontario and implement preventative measures to avoid recurrence of the incident and ensure the privacy and security of the PR data.
8. The contact may be asked to provide eHealth Ontario with a copy of the incident report upon closure of the privacy or security incident/breach.
9. The contact is expected to destroy the incident investigation materials, after the incident investigation report is sent to eHealth Ontario, and after eHealth Ontario has communicated back to them that the actual or suspected incident/breach is closed.

Privacy or security incidents/breaches detected by an Adopter organization and reported directly to eHealth Ontario:

1. The Adopter organizations users contact eHealth Ontario directly to report a suspected or actual privacy or security incident/breach.
2. The service desk will open a SIR or PBM ticket and assign it to the corresponding team.
3. The SIR or PBM lead will connect with the contact to inform them of the suspected or actual incident/breach.
4. The contact will assist the SIR or PBM lead in containing and investigating a suspected or actual privacy or security incident/breach.
5. If required, the SIR or PBM lead will request a copy of any required documentation from the client's site to assist in investigation and/or communication.
6. The logs and/or any other sensitive information should be sent to eHealth Ontario as an encrypted document via an email.
7. The contact must complete all remediation activities as directed by eHealth Ontario to prevent recurrence of the incident or to ensure the privacy and security of the PR data. The site may be asked to provide eHealth Ontario with a copy of the incident report upon closure of the privacy or security incident/breach.
8. The contact is expected to destroy the incident investigation materials, after the incident investigation report is sent to eHealth Ontario, and after eHealth Ontario has communicated back to them that the incident is closed.

eHealth Ontario detected privacy/security breach/incident:

1. A privacy or security incident/breach is detected by eHealth Ontario.
2. The service desk is notified of the incident.
3. The service desk opens a SIR or PBM ticket and assigns it to the corresponding team.

4. SIR or PBM investigates the incident. If during the investigation it is determined that that the privacy/security incident has an impact on any adopter organization, privacy or security notifies the contact of the incident.
5. The contact assists privacy or security in containing, investigating and resolving the incident.

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

What to provide eHealth Ontario's Service Desk when reporting a privacy/security breach:

When reporting a confirmed or suspected privacy or security incident/ breach to eHealth Ontario, the following information should be provided by the contact:

1. Description of the situation and condition that led to the incident.
2. Who is calling and who was involved (name and role)?
3. Where did the incident happen?
4. When and at what time was the incident noticed?
5. Describe how the incident was detected.
6. If possible, provide information on the situation and condition that lead to the incident - for example:
 - o Human error
 - o Negligence
 - o Technical failure, caused by failure of an application or system to maintain privacy
 - o Process failure, caused by not following a process
 - o Willful wrongdoing
 - o Act of nature
7. What information was involved and in what format (i.e. paper or electronic)?
8. What system(s) was involved?
9. If possible, list measures taken to contain the PI/PHI as a result of the incident
10. If possible, list any corrective measures taken or additional controls applied.

Note: *It is extremely important that no patient personal health information and/or personal information is disclosed to the eHealth Ontario Service Desk Agent when reporting a suspected or actual incident/breach.*

4 Appendix

4.1 PR Error Codes

	Code	Display Name	Description
1.	NS200	unsupported interaction	The interaction (or: this version of the interaction) is not supported.
2.	NS202	unsupported processing id	The Processing ID is not supported.
3.	NS203	Unsupported version id	The Version ID is not supported.
4.	NS250	Unsupported processing Mode	The processing mode is not supported.
5.	NS260	Unknown sender	The Device.id of the sender is unknown.
6.	INTERR	Internal system error	An internal software component (database, application, queue mechanism, etc.) has failed, leading to inability to process the message.
7.	NOSTORE	No storage space for message.	Rejection: The message can't be stored by the receiver due to an unspecified internal application issue. The message was neither processed nor stored by the receiving application.
8.	RTEDEST	Message routing error, destination unreachable.	Error: The destination of this message is known to the receiving application. Messages have been successfully routed to that destination in the past. The link to the destination application or an intermediate application is unavailable.
9.	RTUDEST	Error: message routing error, unknown destination.	The destination of this message is unknown to the receiving application. The receiving application in the message does not match the application which received the message. The message was neither routed, processed nor stored by the receiving application.
10.	RTWDEST	Message routing warning, destination unreachable.	Warning: The destination of this message is known to the receiving application. Messages have been successfully routed to that destination in the past. The link to the destination application or an intermediate application is (temporarily) unavailable. The receiving application will forward the message as soon as the destination can be reached again.
11.	SYN	Syntax error.	Reflects errors in the syntax or structure of the communication.
12.	NS200	unsupported interaction	The interaction (or: this version of the interaction) is not supported.