eHealth Ontario

Adopter's Site Support Guide

Provincial Client Registry Services

Version: 1.0

Ontario
eHealth Ontario

Document Control

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

Approval History

APPROVER(S)	TITLE/DEPARTMENT	APPROVED DATE
eHealth Ontario	Privacy	2016-11-17
eHealth Ontario	Security	2016-11-17
eHealth Ontario	Product Management Registries	2017-01-17

Revision History

VERSION NO.	DATE	SUMMARY OF CHANGE	CHANGED BY
1.0	2017-01-17	Initial version published	eHealth Ontario

Document Sensitivity Level

Medium

Table of Contents

Glossary

Term	Definition
ADT	Admit, Discharge, Transfer
EHR	Electronic Health Record
HIC	Health Information Custodian
MOHLTC	Ministry of Health & Long Term Care
PCR	Provincial Client Registry
PHIPA	Personal Health Information Protection Act, 2004
PID	Patient Identifier Domain
RPDB	Registered Persons Data Base

About This Document

Background

The Provincial Client Registry (PCR) is the definitive source for a health care client's identity, facilitating the unique, accurate and reliable identification of individual clients and others who receive care in Ontario, across the disciplines in the health care sector. It contains demographic and identification cross-reference data for health care clients registered in one or more Patient Identifier Domains (PID) for which eHealth Ontario, as a result of policy/program/IT decisions, has established a data sharing agreement with the respective organizations.

The PCR is fed by multiple data sources, including the Ministry of Health and Long Term Care (MOHLTC, or ministry) Registered Persons Data Base (RPDB), hospital sites tracking Admissions, Discharges, and Transfers (ADT), and other systems that participate in health care services (e.g. Wait Times Information System (WTIS), Cardiac Care Network (CCN)) and independent health facilities (e.g. True North Imaging). The PCR includes the functionality of an Enterprise Master Patient Index (EMPI) to match records from different sources referring to a single health care client, addressing the need for positive client identification across Ontario's Electronic Health Record (EHR).

Examples of PCR services include:

- Validating health care client identity information
- Searching and resolving information from multiple sources that refer to the same health care client identity
- Obtaining summary and detailed demographic information about a health care client
- Adding and updating a health care client record
- Merging and unmerging health care client records (because they either do, or do not, refer to the same individual)
- Reconciling duplicates

Document Approach and Scope

This document describes the functions and associated benefits provided by the PCR and the related privacy and security requirements health care providers and organizations using the PCR must adhere to.

Audience

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 PCR service. The guide provides information regarding support and maintenance as well as privacy and security procedures and obligations.

1 Introduction

The Provincial Client Registry (PCR) Adopter's Site Support Guide is a comprehensive document outlining various processes which were created to assist organizations acting as service providers to eHealth Ontario when connecting new sites to the PCR. The guide provides information regarding support and maintenance as well as privacy and security procedures and obligations.

Related Documents

The PCR Site Support Guide should be read in conjunction with the following:

- eHealth Ontario Acceptable Use Policy
- eHealth Ontario Personal Health Information Privacy Policy
- Information Security Policy
- Acceptable Use of Information and Information Technology Policy
- Personal Health Information Protection Act, 2004

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 PCR 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 hours 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
☐	Name
☐	Site location
☐	Contact information, including backup contacts where applicable
☐	eHealth Ontario service
☐	eHealth Ontario service environment affected (e.g. production or conformance testing)
☐	Description of issue (include date and time the issue occurred and the number of users impacted if known)
☐	Steps to reproduce issue and troubleshooting diagnostic steps taken

1.1.4 Service Request Initiation & Escalation

#	Step	Description
1	Service Request	• Adopter contacts eHealth Ontario to open a service request. • Adopter chooses service desk option from phone prompt.
2	Engagement with frontline service desk team	• 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	• 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

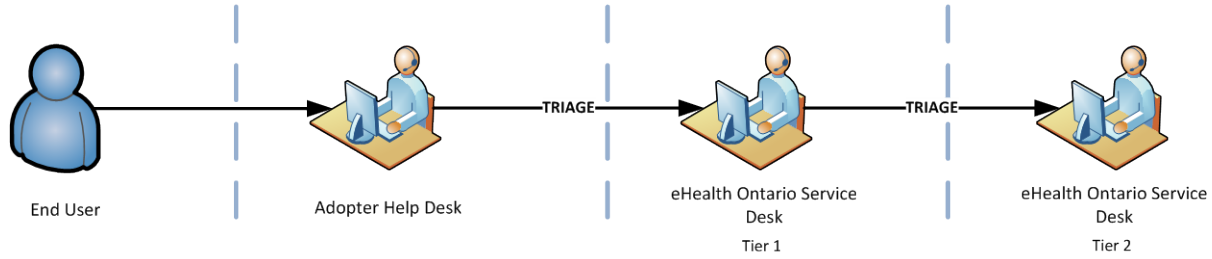
eHealth Ontario Service Desk values and promotes adopter satisfaction. We welcome adopter feedback and encourage adopters to get involved through the following channels:

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

1.2.1 High Level Depiction of the PCR Support Model



1.2.2 Adopter Help Desk Accountabilities

When any issues with the interface used to access PCR 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

1.2.3 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 PCR related interface issues
- Reporting a PCR application error
- Reporting a privacy or security incident or breach

Or, when requesting information from eHealth Ontario regarding:

- PCR functionality;
- Privacy and security of PCR personal health information.

Note: End users should always contact their local site help desk for assistance with PCR 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.

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

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

- For requesting additional information to fulfill PCR privacy request;
- For incident or breach management purposes.

2 Operational Responsibilities for PCR Data

2.1 Audit Logs

According to our agreements with relevant organizations who contribute data to eHealth Ontario's PCR, as well as agreements signed with participating Adopter organizations, eHealth Ontario is responsible for keeping an electronic record of all accesses to PCR 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 PCR Data

HICs must retain personal health information in accordance with applicable legislation and health regulatory requirements. In addition, the EHR Retention *Policy* places certain retention obligations on HICs as detailed below:

Information Type	**Retention Period**
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.
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.
Assurance-related documents	10 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/en/initiatives/resources.

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/security.

3 Privacy and Security

3.1 Access Requests

Under PHIPA, individuals or their substitute decision makers have a right to access data held by a HIC. If an individual requests access his or her records that an organization has collected, created and / or contributed to the PCR, that organization must follow Part V of PHIPA as well as its related internal policies, procedures and practices before responding.

If an individual would like to request a copy of what personal health information of theirs is in PCR, please direct the individual to contact eHealth Ontario at 1-866-250-1554, or through http://www.ehealthontario.on.ca/en/contact.

3.2 Audit Log Requests

When a health care provider receives a request for access directly from an individual related to audit logs (e.g. who has looked at my information) for records stored in PCR, the HIC is required to:

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

Health care providers may request audit logs of their facility's access to PCR data directly from eHealth Ontario by calling eHealth Ontario's Service Desk at 1-866-250-1554. Note that this request should come from the privacy office at the participating organization. If the organization does not have a privacy office, the health care provider may contact eHealth Ontario directly.

3.3 Correction Requests

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

At the request of the individual, when a correction request is fulfilled, the HIC must notify eHealth Ontario of the correction and request an audit report of who has accessed the individual's personal health information, in the event that the individual would like to inform other HICs who may have accessed his /her personal health information. The HIC must then notify relevant sites that have viewed the individual's personal health information of the correction.

Where a HIC receives a request for correction directly from an individual related to personal health information that was created by another or more than one HIC, he /she must respond no later than two days upon receiving the request by:

- Notifying the individual that the request for correction involves personal health information not within their custody or control, and
- Directing the individual to contact eHealth Ontario at 1-866-250-1554 or through http://www.ehealthontario.on.ca/en/contact.

3.4 Privacy Complaints and Inquiries

If an Adopter organization directly receives a privacy inquiry or complaint related solely to that organization's records in PCR, or his / her agents and / or service providers, the HIC is required to follow his / her own internal policies, procedures, and practices.

If the organization receives a privacy complaint or inquiry from an individual relating to eHealth Ontario or the agency's privacy policies and procedures, the individual 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.

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

3.5 Privacy and Security Training

Adopting organizations are required to provide privacy and security training to their agents and electronic service providers prior to their access to EHR system. The training should ensure that agents and electronic service providers are aware of their duties under applicable privacy legislative, 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 access to the EHR. 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/en/initiatives/resources. All end users must be in receipt of the applicable privacy training before accessing the system.

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.

3.6 Privacy and Security Incident and 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 personal information or personal health information 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 PCR 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 personal information or personal health information that is in contravention of applicable privacy law.
- Any other circumstances where there is unauthorized or inappropriate collection, use or disclosure, copying, modification, retention or disposal or 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.

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 and security incidents/breaches involving the PCR data accessed by that site in accordance with the steps contained in this document.

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 information to PCR.

Instructions for Health Care Providers

Reporting a privacy or security incident or breach to eHealth Ontario is required when a HIC becomes aware of an actual or suspected incident or breach caused or contributed by:

- Another HIC or the agents or electronic service providers of another HIC,
- More than one HIC or the agents or electronic service providers of more than one HIC,

- eHealth Ontario or its agents or electronic service providers, or
- Any other unauthorized persons who are not agents or electronic service providers of eHealth Ontario or any other HIC.

If you become aware of, or suspect, a privacy or security incident or breach of PCR data by you or any of your employees, agents, or service providers, you must immediately report the incident or breach to your organization's privacy office. If you do not have a privacy office or you are unable to reach your privacy office or support team to report a breach, please contact the Service Desk at 1-866-250-1554 and open a breach or incident ticket no later than the end of the following business day.

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.

You are expected to cooperate in any incident or breach containment activities or with any investigation undertaken. During the investigation, 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.

In instances where a breach was solely caused by a HIC that did not solely create and contribute the personal health information to PCR, the HIC, in consultation with the other HICs who contributed data and eHealth Ontario, shall identify the individual to investigate the breach. The specific roles for each party involved in the privacy breach are noted in the *EHR Privacy Breach Management Policy* at http://www.ehealthontario.on.ca/en/initiatives/resources.

Instructions for Privacy Officers

If you become aware of, or suspect, an incident or breach related to PCR data by any of your organization's staff members, including employees, agents or service providers, you must immediately report the incident or breach to the eHealth Ontario Service Desk 1-866-250-1554 to open an incident or breach 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 or breach, please have the following information ready:

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

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