eHealth Ontario
www.ehealthontario.on.ca

Health Care Provider Guide

Provincial Registries

Version: 1.0

Ontario
eHealth Ontario

Contents

Glossary 3

General Information **4**

Purpose and Scope 4
Audience 4
Related Documents 4

Service Description **5**

Overview 5
Benefits 6
To You 6
To Your Patients 6

Privacy and Security **7**

Access Requests 7
Access Requests for Provincial Registries data 7
Requests for Audit Logs 7
Correction Requests 8
Privacy Complaints and Inquiries 8
Retention 9
Privacy and Security Training 10
Privacy-Related Questions from Health Care Provider Sites 10
Privacy and Security Incident and Breach Management 10
A privacy incident is: 10
A privacy breach is: 11
A security incident is an unwanted or unexpected situation that results in: 11
Instructions for Health Care Providers 11
Instructions for Privacy Officers 12

Summary of Security Safeguards in Place at eHealth Ontario **13**

Administrative Safeguards 13
Technical Safeguards 14
Physical Safeguards 15

Glossary

Term	Definition
EHR	Electronic Health Record
HIC	Health Information Custodian
ONE® ID	Set of systems and processes for assigning and managing electronic identities to allow secure access to eHealth Ontario services
PCR	Provincial Client Registry
PHIPA	*Personal Health Information Protection Act, 2004*
PR	Provider Registry
RA	Registration Authority

General Information

Purpose and Scope

This guide describes the functions and associated benefits provided by eHealth Ontario's Provincial Client Registry and Provider Registry application as well as the privacy and security procedures and obligations health care providers and organizations using the Provincial Client Registry and Provider Registry must adhere to.

Audience

The primary audience for this document includes health care providers across Ontario's health care sector who may be an organization or a person, who has signed or will sign the appropriate eHealth Ontario access agreement(s) and use the Provincial Client Registry (PCR) and Provider Registry (PR) applications to assist with the provision of health care to their patients.

Related Documents

The PCR and PR health care provider guide should be read in conjunction with the following:

- eHealth Ontario Acceptable Use Policy
- ONE ID Registrant Reference Guide
- eHealth Ontario Personal Health Information Privacy Policy
- Information Security Policy
- Acceptable Use of Information and Information Technology Policy
- *Personal Health Information Protection Act, 2004*

In addition, the following Privacy policies can be found at http://www.ehealthontario.on.ca/en/initiatives/resources

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

Service Description

Overview

The Provincial Registries (Provincial Client Registry and Provider Registry) are repositories that form the backbone of the Electronic Health Record (EHR). They are the “source of truth” for patient information as well as regulated provider information.

Provincial Client Registry
The Provincial Client Registry (PCR) allows identity records issued by multiple disparate health information systems to be associated with one another through a single identifier. Currently it sources demographic data to identify clients from the Ministry of Health and Long-Term Care (MOHLTC) Registered Persons Database (RPDB) as well as 196 participating health sites across the province. PCR represents approximately 98% of Ontario’s population (via RPDB) and 86% of Ontario’s hospitals (including 196 sites, 64 sources, the Wait Time Information System and Cardiac Care Network , Independent Health Facility (IHF) and Community Care Access Centre (CCAC)). PCR correlates and links individual records from disparate systems to create a client’s ‘golden record’ using proprietary technology (Enterprise Master Patient Index). The registry also encourages ongoing data quality of source systems by providing contributors with reports and tools to remediate data quality issues. The data is updated through daily reports (delta basis) received from the MOHTLC and in near real-time from hospital sources.

Provider Registry (PR)
The Provider Registry (PR) is the authoritative source of information for health profession data and health care service delivery locations for use by all EHR solutions. It facilitates the unique and accurate identification of regulated provider persons and organizations that provide health services in Ontario, or who participate in the collection, use, or disclosure of personal health information 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) 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.

Benefits

To You

- Facilitate the sharing of clinical information by establishing a common patient identity across all points of service;
- Improve data quality and clinical workflow efficiency;
- Positively identify regulated provider persons;
- Provide information on providers (e.g. licensing status, practice locations).

To Your Patients

- Improve patient safety associated with patient misidentification;
- Enable the creation of an integrated longitudinal EHR;
- Reduce manual efforts related to maintaining and searching for provider information;
- Decrease time for clients to see providers (referrals, consults).

Privacy and Security

Access Requests

Access Requests for Provincial Registries data

Under PHIPA, individuals or their substitute decision makers have a right to access personal health information held by a HIC. As a health care provider, if you receive a request from an individual to access his or her records that you have collected, created and / or contributed, you must follow Part V of PHIPA as well as your related internal policies, procedures and practices before responding.

Where a HIC receives a request for correction directly from an individual related to records that were created and contributed to PCR by another or more than one HIC, the HIC must respond no later than two days after receiving the request for correction by:

- Notifying the individual that the request for correction involves PHI 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.

As a health care provider, if you would like a copy of your information stored in the PR, please contact your respective Regulatory College to make this request.

Requests for Audit Logs

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 they are 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.

As a provider, you may request audit logs of your 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 your organization. If you do not have a privacy office, you may contact eHealth Ontario directly at 1-866-250-1554.

If you would like an audit report of who has accessed your information in PR, contact the eHealth Ontario Service Desk at 1-866-250-1554.

Correction Requests

If you receive a request for correction directly from an individual related to personal health information that was created and contributed to PCR solely by your organization, you are required to follow Part V of PHIPA and your organization's 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, they 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.

To request a correction to your provider information in the PR, contact your respective regulatory college. eHealth Ontario receives regular updates to information in the PR from the contributing regulatory colleges.

Privacy Complaints and Inquiries

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

If a HIC receives a privacy inquire or complaint 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*

Retention

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**
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

Privacy and Security Training

HICs 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.

Privacy-Related Questions from Health Care Provider Sites

If a health care provider has any questions regarding the privacy-related processes described above, including how to respond to individual access requests, consent obligations or incident/breach management processes, 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.

Privacy and Security Incident and Breach Management

The *EHR Privacy Breach Management Policy* at http://www.ehealthontario.on.ca/en/initiatives/resources describes detailed steps to be taken in the event of a privacy breach/incident.

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.

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 and/or PR.

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 and/or PR 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 and/or PR, 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 or PR 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.

Summary of Security Safeguards in Place at eHealth Ontario

Administrative Safeguards

- eHealth Ontario's Chief Privacy Officer and the Chief Security Officer are accountable for privacy and security.

- eHealth Ontario has a comprehensive set of information security policies that align with its organizational goals, are regularly reviewed and enhanced. Staff members and contractors are required to familiarize themselves with the relevant policies and sign an attestation that they have read, understood and are committed to comply with them.

- All staff and contractors must sign confidentiality agreements and undergo criminal background checks prior to joining or providing services to eHealth Ontario. eHealth Ontario has a security screening policy that requires staff to have an appropriate level of clearance for the sensitivity of the information they may access.

- eHealth Ontario has mandatory privacy and security awareness and training programs.

- eHealth Ontario staff and contractors generally have no ability or permission to access personal health information. If access to personal health information is required in the course of providing eHealth Ontario services, individuals are prohibited from using or disclosing such information for any other purposes.

- eHealth Ontario ensures, through formal contracts and service level agreements, that any third party it retains to assist in providing services to eHealth Ontario or to health information custodians will comply with the restrictions and conditions necessary for eHealth Ontario to fulfil its legal responsibilities.

- eHealth Ontario staff, consultants, suppliers and clients must promptly report any privacy and security breaches to eHealth Ontario for investigation. An enterprise security and privacy incident management program is in place to ensure management of incidents and regular training and awareness for staff members involved in incident management.

- Security threat and risk assessments (TRAs) are conducted as part of both product/service development and client deployments. Security risk mitigation activities are established, assigned to a responsible individual, recorded and tracked as part of each assessment.

- eHealth Ontario provides a written copy of the results of privacy impact assessments and security threat and risk assessments to the affected health information custodians upon request.

- eHealth Ontario has established a formal risk management program which includes a policy and guidelines. A specialized management forum, the security leadership group, provides strategic direction and governance oversight for the security program, including regular review of risks and the corresponding risk treatment plans.

- Audit logs recording user activities, system administrator's activities, exceptions, and information security events must be produced and kept for a minimum of six months online and a minimum of 18 months in the archive, to assist in incident and problem management, future investigations and access control monitoring.

- eHealth Ontario keeps an electronic record of all accesses to all or part of the personal health information contained in the EHR and is in the process of developing solutions which ensure the record identifies the person who accessed the information and date.

- Log data required for litigation support must be kept until the disposition of the legal matter.

- All changes to the network are controlled by eHealth Ontario and subject to formal change management practices.

Technical Safeguards

- Strong passwords, secure tokens, and other authentication solutions are required for access to sensitive systems.

- Administrative access to all IT equipment and applications is provided on a need to know basis controlled via proper authorization and strong, two-factor authentication. All system and application access activities are logged.

- eHealth Ontario manages network traffic using security mechanisms such as routers, switches, network firewalls; and monitors network traffic using intrusion detection systems, and anti-virus programs.

- All sensitive data is encrypted in traffic between external sources and eHealth Ontario systems.

- All data stored on staff computers is encrypted. If laptops are lost or stolen, data confidentiality and integrity are not at risk.

- Data integrity controls are implemented as a quality assurance activity on the personal health information provided to eHealth Ontario by health information custodians.

- Independent vulnerability assessments of technical configurations and operational security practices are conducted periodically.

- A patch management process is in place to ensure that operating systems, databases and applications receive security patches and functional updates in a timely manner.

- Upon termination of employment or contracts, all accounts of former staff or consultants are deleted and access is disabled.

- Data and applications are backed up on a regular basis, and can be easily restored in case of operational incidents.

- A comprehensive disaster recovery and business continuity plan is in place and are tested and updated regularly.

Physical Safeguards

- The eHealth Ontario data centres are purpose-built facilities, with appropriate environmental controls and physically secured against unauthorized access. They are staffed and monitored continuously by trained security personnel.

- Specific physical security zones are implemented to separate and control access to public zone, delivery and loading area, office space, and computer rooms, with increasing physical security controls.

- Data centre physical security controls have been validated by an independent third party in accordance with federal government standards, and through internally conducted threat and risk assessments.

- Access to office areas is controlled with access badges, and traffic in the office areas is recorded by security cameras.

- Access to office areas where business processes require access to personal information or personal health information is physically restricted to only the staff members whose role involves handling of personal information or personal health information. Other staff members do not have physical or logical access to those areas.

- Visitors and third-party vendors to eHealth Ontario require visitor badges and are escorted at all times by full time staff members. Access badges expire automatically within 24 hours and cannot be reused.

- Decommissioned equipment that was used to process or store personal information or personal health information is securely disposed of, according to approved procedures.

- Procedures and appropriate equipment are in place for secure disposal of paper, CDs, or other media that may have sensitive information.