ConnectingOntario

Health Care Provider Guide

ConnectingOntario

Version: 1.03

Document ID: Health Care Provider Guide

Document Owner: ConnectingOntario

Ontario
eHealth Ontario

Table of Contents

General Information

Purpose and Scope

The Health Care Provider Guide – ConnectingOntario (Guide) describes the functions and associated benefits provided by ConnectingOntario and the related privacy and security considerations, which health care providers and organizations using ConnectingOntario ClinicalViewer must adhere to.

Audience

This document is intended for health care providers across Ontario's health care sector that may be an organization or a person, who has signed or will sign the appropriate eHealth Ontario access agreement(s) and use the ConnectingOntario ClinicalViewer to view their patients'[1] records and results.

Related Documents

The Guide should be read in conjunction with the following information found at eHealthOntario.on.ca:

- eHealth Ontario Personal Health Information Privacy Policy
- 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
- eHealth Ontario Federation Identity Provider Policy and Standard
- EHR Security Policies
    - Acceptable Use of Information and Information Technology Policy

[1] For the purposes of this Guide, where the term 'patient' is used, it can denote client or individual accessing health care services.

    - 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
- OLIS Health Care Provider Guide – Lab

ConnectingOntario

Overview

ConnectingOntario enhances care for approximately 13.6 million Ontarians, by providing clinicians and care providers with clinical information in a safe secure electronic format that will improve patient outcomes. This seamless and secure system provides access to a majority of acute and community care data improving the timeliness of care decisions, reducing duplicate tests and procedures and better supporting care transition points. Three regional hubs, ConnectingOntario Greater Toronto Area, ConnectingOntario Northern and Eastern Region and Connecting South West Ontario are currently implementing ConnectingOntario to reach approximately 90,000 clinicians and care providers provincially.

Starting with clinician-identified priority data, the system leverages local, regional and provincial ehealth registries and repositories as data sources for:

- Clinical reports (CCAC, discharge summaries, emergency department, visits and encounters)
- Diagnostic imaging reports
- Drug information
- Lab results

With the support of information technology, ConnectingOntario:

- Identifies and collects priority data: a Clinical Data Repository (CDR) stores data from existing databases and registries
- Provides the ability to exchange information: a Health Integration Access Layer (HIAL) integrates and securely shares clinical data from multiple sources
- Provides access to information: access options, such as a provider portal and direct integration, allow clinicians to seamlessly access patient information online

ConnectingOntario transitioned from limited production release to full production release in summer 2015. ConnectingOntario benefits clinicians and care providers at more than 750 health care organizations, representing the following sectors:

- Acute care
- Community support services
- Complex continuing care
- Long-term care
- Mental health and addictions
- Primary care
- Rehabilitation

Benefits

Benefits to You

1. Enhanced care and experience
   - Reduce redundancy and frustration
   - Help improve interactions with point-of-care access to information
   - Improve transition between health care providers
2. Improved productivity and satisfaction
   - Improve efficiency of decision-making and the ability to monitor health outcomes
   - Provide electronic access to integrated health care information
   - Help improve inter-professional care and coordination of services
3. Improved organizational and system coordination and capacity
   - Accelerate the development and delivery of electronic health records
   - Provide significant cost-savings, enabling an integrated and sustainable approach to better manage, coordinate and plan care
   - Build foundational information technology (IT) elements that can be leveraged for other organizational, regional and provincial health initiatives

Benefit to Your Patients

- Patients receive better, more timely and more coordinated care

Responsibilities

eHealth Ontario Responsibilities

eHealth Ontario shall comply with the following obligations:

- Provide ConnectingOntario functionalities as described below, for registered health care providers 24/7
- Provide alternative ways to search for a patient of interest within the ConnectingOntario ClinicalViewer
- Enable access to the patient's health information that has been submitted by health care providers to the CDR and Ontario Laboratory Information System (OLIS)
- Do not provide access to any record contained within the CDR that has been restricted by one or more consent directives issued by the patient

- Temporarily reinstate access to a patient's health information contained within the CDR and OLIS that is restricted by consent directives when the health care provider indicates that the patient's or his/her substitute decision maker's approval (SDM) has been obtained, or for the purpose of reducing the risk of bodily harm to the patient or other persons
- Provide support for privacy-related inquiries/concerns about the data viewed in the solution
- Update the ConnectingOntario ClinicalViewer to expand and enhance the functionalities provided
- Conduct privacy and security assessments to ensure that the collection, storage, use and disclosure of personal information/personal health information (PH/PHI) via ConnectingOntario complies with legislative and privacy protection requirements
- Assist providers in meeting their legislative obligation for responding to a patient's access and correction requests

Contributor Responsibilities

Health care providers that contribute data to the CDR shall comply with the following obligations:

- Follow the supporting Electronic Health Record (EHR) security policies and EHR privacy policies when contributing to the CDR. See Related Documents for a complete listing of policies

Identity Provider Responsibilities

Identity providers who provide the identity management service shall comply with the following obligations:

- Follow the requirements of the eHealth Ontario *Identity Provider Policy* and Standard
- Follow the supporting EHR security policies when providing an identity management service. See Related Documents for a complete listing of policies.

Information Consumer Responsibilities

Health care providers who view the data displayed in the ConnectingOntario ClinicalViewer shall comply with the following obligations:

- Agree to follow the *EHR Information Security Policy* and the *EHR Acceptable Use of Information and Information Technology Policy* available at http://www.ehealthontario.on.ca/docs
- Review the reference information listed in Related Documents and learn how to protect privacy and security when using eHealth Ontario products
- Use the ConnectingOntario Clinical Viewer's functionalities only for approved clinical purposes
- Always indicate the person or the organization that the user represents when accessing patients' health information within the solution
- Obtain the patient's or the SDM consent prior to requesting temporary reinstatement of consent to access health information restricted by consent directives
- Implement and assist users to follow EHR privacy and security policies, where applicable

Privacy and Security Considerations

Quick Tip

ConnectingOntario gives patients or their SDM the option to allow or restrict access to patient data within the solution. Should a patient choose to place a consent directive in ConnectingOntario, he/she must fill out the EHR Consent Directive form, found at http://www.ehealthontario.on.ca, and send it to eHealth Ontario. Providers may help a patient fill out the form and forward it to eHealth Ontario on the patient's behalf.

Patient Consent

Consent Management

ConnectingOntario gives patients or their SDM the option to allow or restrict access to patient data within the ClinicalViewer. If a patient restricts access to his/her data, by applying a consent directive, providers querying the solution will be unable to access the information to which a consent directive has been applied.

Consent directives can be made, modified or removed to restrict or allow the following in the ConnectingOntario ClinicalViewer:

- All of a patient's records (Global Consent Directive)
- All of his/her reports from a particular provider (HIC-Record Consent Directive)
- All users from a particular organization (HIC-Agent Consent Directive)
- A particular provider (Agent Consent Directive)

Applying Consent Directives

If a patient contacts a health information custodian (HIC) and wishes to either place a restriction on access to his / her information, or wishes to reinstate access (remove the restriction), the HIC should:

- Capture the consent directive information on the EHR Consent Form at http://www.ehealthontario.on.ca, and
- Submit the consent directive information to eHealth Ontario by faxing it to 416-586-4397 or 1-866-831-0107.

eHealth Ontario will send the HIC a confirmation that the request has been fulfilled. The HIC should then provide notice to the patient that the consent directive has been successfully applied.

In instances where a patient requests to place a consent directive on or reinstate access to records contributed by more than one HIC, the patient should complete the EHR Consent Form or contact eHealth Ontario directly at 416-946-4767.

In all instances, eHealth Ontario will apply the consent directives within 7 days of verifying the identity of the patient making the request. The party who received the request for the consent directive then notifies the patient that his / her request has been fulfilled. If you cannot notify the patient, eHealth Ontario will notify him / her on your behalf on your direction.

Note that consent directive requests sent to eHealth Ontario on behalf of patients should come from the privacy office at your organization. If you do not have a privacy office, you may contact eHealth Ontario directly.

For OLIS consent directives, refer to the OLIS Health Care Provider Guide.

Overriding a Consent Directive

Quick Tip

ConnectingOntario permits a health care provider to temporarily override a patient's consent directive. If you perform a consent override, your privacy office will be notified by eHealth Ontario and asked to confirm the purpose of the override, and to subsequently notify the patient of the override occurrence. An override can be only performed at the express consent of the patient, or to reduce the risk of bodily harm to the patient or persons other than the patient. A consent directive override will be in effect for 24-hours for ConnectingOntario.

ConnectingOntario permits a health care provider in special cases to temporarily override a patient's consent directive.

Providers can temporarily override a consent directive under the following circumstances:

- With the express consent from the patient or the patient's SDM
- Believes on reasonable grounds that the override is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm to the patient to whom the personal health information (PHI) relates and where it is not reasonably possible to obtain the consent of the patient in a timely manner – or;
- Believes, on reasonable grounds, that the override is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm to a person other than the patient to whom the PHI relates or to a group of persons

A temporary consent override will be logged in the ConnectingOntario interface, along with the identity of the overriding health care provider. The override will be in effect for no more than 24-hours for ConnectingOntario.

eHealth Ontario will notify the HIC's privacy office if one of the HIC's agents overrides a consent directive. Once contacted by eHealth Ontario, it is the responsibility of the HIC's privacy office to:

1. Investigate the override to ensure it was for one of the reasons stated above, and
2. Notify the patient of the override at the first opportunity.[2]

If a consent directive override is applied for the purpose of eliminating or reducing a significant risk of serious bodily harm to a person other than the patient to whom the PHI relates or to a group of persons, the HIC should provide a written notice to the Information and Privacy Commissioner of Ontario (IPC) as soon as possible indicating that this type of override has occurred. For more information on what to include in this notice to the IPC, please see the *EHR Consent Management Policy*.

For OLIS, a consent directive override may only occur at the express consent of the patient or SDM. Refer to the OLIS Health Care Provider Guide for more details.

[2] For more information on what to include in this notice to the patient, please see the *EHR Consent Management Policy*. If you cannot notify the patient, contact eHealth Ontario, and eHealth Ontario will notify the patient on your behalf.

Access Requests

Quick Tip

When a patient requests to access or correct their data that your practice has contributed to ConnectingOntario, follow your internal procedures for allowing access or correction to that data. Make note of this request.

When a patient requests to access or correct their data that other HICs have contributed to ConnectingOntario, direct the patient to contact eHealth Ontario at 416-946-4767 as soon as possible to make the request.

Access Requests Made by Patients

Under PHIPA, patients or their SDM have a right to access data held by a HIC about the patient. When a provider receives a request for records collected, created and contributed by the provider to ConnectingOntario, the provider must follow Part V of PHIPA as well as all any related internal policies, procedures and practices to respond directly to the patient.

In instances where requests for access involves information contributed by another HIC or by multiple HICs, the provider is required to:

- Notify the patient that the request for access involves PHI not within the custody or control of the HIC that received the request for access, and
- Direct the patient to contact eHealth Ontario at 1-866-250-1554 or

As per the *EHR Access and Correction Policy*, eHealth Ontario may seek assistance from the HIC when responding directly to a request for access.

Requests for Audit Logs

When a provider receives a request for access directly from a patient related to audit logs for records stored in ConnectingOntario, the HIC is required to:

- Notify the patient that the HIC is unable to process the request for access, and
- Direct the patient to contact eHealth Ontario at 1-866-250-1554 or

Note that access requests and audit log requests should come from the privacy office at your organization. If you do not have a privacy office, you may contact eHealth Ontario directly.

For OLIS access requests, refer to the OLIS Health Care Provider Guide.

Correction Requests

When a HIC receives a request for correction directly from a patient related to health records that were created and contributed to ConnectingOntario solely by that HIC, the HIC is required to follow Part V of PHIPA and its internal policies, procedures and practices to respond directly to the patient in respect of the request for correction.

- At the request of the patient, 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 patient's record, in the event that the patient would like to inform other HICs who may have accessed their record. The HIC must then notify relevant sites that have viewed the patient's record of the correction.

Where a HIC receives a request for correction directly from a patient related to records that were created and contributed to ConnectingOntario 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 patient that the request for correction involves PHI not within their custody or control, and
- Directing the patient to contact eHealth Ontario at 1-866-250-1554 or

eHealth Ontario will coordinate the response to this request, and may seek assistance from the HIC(s) when responding to the patient.

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

For OLIS correction requests, refer to the OLIS Health Care Provider Guide.

Privacy Complaints and Inquiries

Quick Tip

When a person submits an inquiry or complaint related to ConnectingOntario, direct him / her to contact eHealth Ontario with their inquiry or complaint.

When a HIC directly receives an inquiry/complaint related solely to that HIC's records in ConnectingOntario, or related to the HIC and its agents and service providers, the HIC is required to follow its own internal policies, procedures, and practices to address the inquiry.

When a HIC directly receives an inquiry/complaint related solely to ConnectingOntario or to eHealth Ontario's agents or electronic service providers that it is unable to address, the HIC must:

- Notify the person that the HIC is unable to respond to the inquiry/complaint, and

- Direct the patient to contact eHealth Ontario at 1-866-250-1554 or

eHealth Ontario may seek assistance from the HIC(s) when responding directly to inquiries or complaints received by eHealth Ontario.

Retention

Quick Tip

HICs must retain records containing PHI for specified periods of time. Any information collected to respond to access and correction requests, inquiries, complaints, and information pertaining to consent directives must be retained for two years after the request was made.

PHIPA requires HICs to ensure that its records are retained for a specified period, and transferred and disposed of in a secure manner. HICs must ensure records are protected and disposed of in accordance with the *Information Security Policy*.

HICs will retain records containing the following information for the corresponding retention period:

Information Type	Retention Period
Audit logs and audit reports that contain PHI created and maintained for compliance purposes	The longer of 30 years or when PHI is removed from the EHR.
Information collected to respond to patients related to their: o Request for Access or Request for Correction under PHIPA; o Request to make, modify, or withdraw a Consent Directive under PHIPA; or o Inquiries or Complaints under PHIPA.	Two years after the request was made. For complaints, retain for two years after the complaint has been closed by the HIC, eHealth Ontario, or the IPC, whichever is longer.
Information created about a patient as part of an investigation of Privacy Breaches and/or Security Incidents.	Two 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 PI	Seven years after last use
End User Credential Information where HIC is an Identity Provider	Permanent
System-level logs, tracking logs, reports and related	For a minimum of two years

documents for privacy and security tasks that do not contain PHI	
Authentication Events where HIC is an Identity Provider	60 days online, 24 months total in archive
Templates or resources developed by eHealth Ontario in respect of the EHR;	For a minimum of two years
Assurance-related documents	10 years

The specific types of PHI that are included in each of the information types can be found in the *EHR Retention Policy*.

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 ConnectingOntario. 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 ConnectingOntario. Training should be completed prior to being provisioned an account for accessing the ConnectingOntario ClinicalViewer. eHealth Ontario has developed role-based training materials to facilitate this training requirement. For more information on what to include in privacy and security training, please see the *EHR Privacy and Security Training Policy and the Privacy Toolkit*. All end users must have received the applicable privacy training before accessing the system.

HICs are required to track which of their agents, electronic service providers, and any end users have received privacy and security training. After initial training has taken place, training should 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 patient 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.

Quick Tip

A HIC shall report an actual or suspected privacy breach to eHealth Ontario by calling the 24/7 service desk at 1-866-250-1554 as soon as possible.

Privacy Breach Management

The *EHR Privacy Breach Management Policy* describes detailed steps to be taken in the event of a privacy breach/incident.

A HIC shall report an actual or suspected privacy breach to eHealth Ontario by calling the 24/7 service desk at 1-866-250-1554 as soon as possible, but in any event no later than the end of the next business day. Reporting a breach / incident to eHealth Ontario is required when a HIC becomes aware of an actual or suspected privacy 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.

In instances where a breach is caused by a HIC who solely created and contributed the data to ConnectingOntario, the HIC shall follow its internal policies, procedures, and practices to notify the patient(s) to whom the PHI relates at the first reasonable opportunity in accordance with PHIPA and to contain, investigate and remediate the privacy breach.

In instances where a breach was solely caused by a HIC that did not solely create and contribute the PHI to ConnectingOntario, the HIC, in consultation with 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*.

Security Incident and Breach Management

This section includes instructions for HICs to report to eHealth Ontario any security incidents or breaches (defined below) related to the ConnectingOntario ClinicalViewer.

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 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 PHI to ConnectingOntario.

Instructions for Health Care Providers

If you become aware of, or suspect, a security incident or breach of ConnectingOntario or data by you or any of your employees, agents, or service providers, you must immediately report the incident or breach to your 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 advise the service desk that you would like to open a security incident ticket. You are expected to cooperate in any incident or breach containment activities or with any investigation undertaken by ConnectingOntario. During the 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.

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.

Instructions for Privacy Officers

If you become aware of, or suspect, an incident or breach related to ConnectingOntario or 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 service desk 1-866-250-1554 and advise the service desk that you would like to open a security 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 will 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 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 or team will be engaged to deal with the situation. A remediation plan will be developed in consult with the requestor.

Summary of Security Safeguards in Place at eHealth Ontario

Administrative Safeguards

- eHealth Ontario has a Chief Privacy Officer and a Chief Security Officer; these patients are accountable for health information privacy and security
- The privacy and security committee (made up of the health care organizations participating in ConnectingOntario) oversees the privacy and security programs
- Health care organizations must ensure that their health care providers are informed of their duties
- Agreements, policies and procedures define each organization's role in protecting PI/PHI. They also define the roles of any people working for the organization or service providers who provide the health care organizations with services. Staff members and contractors are required to read the relevant policies and sign an attestation that they have read, understood and are committed to complying with them

- Privacy and security assessments are conducted to identify new risks to privacy and security when the privacy and security committee feels that there is a significant enough change to ConnectingOntario or information system
- eHealth Ontario notifies health care organizations of any unauthorized access to PI/PHI that the healthcare organization added to ConnectingOntario
- ConnectingOntario staff, consultants, suppliers and users must promptly report any privacy and security breaches for investigation. A 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

Technical Safeguards

- Only approved health care providers and staff that support them can view the information in the ConnectingOntario ClinicalViewer
- Users are authenticated each time they access the system
- The actions of everyone who views the personal information and personal health information are recorded electronically
- The PI/PHI is always encrypted when it is transmitted to and from participating sites
- Networks are protected by devices (firewalls and routers) that limit access to and from systems
- All actions in the information system are logged so that the privacy officers of the health care organizations are able to monitor and audit their health care providers and staff who view PI/PHI in the information system
- Security agents are installed on each system to protect ConnectingOntario from malware and detect intrusions
- Vulnerability assessments of technical configurations and operational security practices are conducted periodically

Physical Safeguards

- The PI/PHI is stored in a data centre with cameras, restricted access, alarms, and 24/7 security
- When servers are no longer needed, the hard disks storing the PI/PHI are physically destroyed or permanently erased
- Information is not physically removed from the data centre

Glossary

Acronym	Term
CCAC	Community Care Access Centre

CDR	Clinical Data Repository
DI	Diagnostic Imaging
EHR	Electronic Health Record
ESP	Electronic Service Provider
HIAL	Health Integration Access Layer
HIC	Health Information Custodian
IPC	Information and Privacy Commissioner
IT	Information Technology
OLIS	Ontario Laboratory Information System
PHI	Personal Health Information
PHIPA	*Personal Health Information Protection Act, 2004*
PI	Personal Information
SDM	Substitute Decision Maker