eHealth Ontario
It's working for you

Health Care Provider Guide

Diagnostic Imaging Common Service

Version 3

Ontario
eHealth Ontario

Contents

General Information

Purpose and Scope

This guide describes the functions and associated benefits provided by eHealth Ontario's Diagnostic Imaging Common Service (DI CS) application as well as the privacy and security procedures and obligations that health care providers and organizations must adhere to.

Audience

The primary audience for this document includes health care providers and organizations across Ontario's health care sector that use DI CS to access patients' DI Results.

Related Documents

The DI service guide should be read in conjunction with the following documents:

- 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 on the eHealth Ontario resources web site.

- 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

Diagnostic Imaging Common Service (DI CS) is an eHealth Ontario initiative that allows hospital- and community-based health care providers to view DI reports and images from across Ontario. DI CS gives authorized providers important information to make better decisions about treating patients.

Prior to DI CS, authorized providers could easily and securely view reports and images stored only within their local regional DI repository (DI-R). DI results in Ontario are divided geographically and stored in four DI-Rs.

Now, diagnostic reports and images are available across Ontario. The reports and images are still stored in the four DI-Rs, but DI CS creates links among them, so rather than being limited to their local DI-R, authorized users can use DI CS to retrieve DI reports and images from across the province (that is, from all four DI-Rs). This capability gives clinicians quicker access to information, leading to the possibility of faster diagnoses.

DI CS gives Ontario's health care providers important information to make better decisions about patients' treatments anywhere at any time. This capability reduces the need for patients to travel to see specialists.

DI CS is part of eHealth Ontario's overall approach to improve access to safe patient care. By putting in place a stable technical infrastructure, health care providers have access to vital clinical information when they need it.

Benefits

To You

- Access to diagnostic images and reports across Ontario
- Faster and easier access to images and reports 24/7
- Real-time clinical collaboration, increasing access to a broader range of specialists
- Eliminates the need to physically transfer images in hardcopy or on compact discs

To Your Patients

- Eliminates unnecessary travel
- Reduces wait times and lengths of stay thanks to faster exam reports and clinical decisions by physicians and specialists
- Reduces duplicate and unnecessary exams

Privacy and Security

Patient Consent

The eHealth Ontario electronic health record (EHR) system gives patients (or their substitute decision makers) the option to allow or restrict access to patient data through consent directives.

Consent Management

Should a patient choose to place a consent directive in DI CS, the patient must fill out the EHR consent form (available on the eHealth Ontario web site) and send it to eHealth Ontario. Providers may help patients fill out these forms and may forward them to eHealth Ontario on the patients' behalf.

If patients restrict access to their data by applying consent directives, providers querying DI CS will be unable to access the data to which the consent directive applies.

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

- Access to all of a patient's records (Global/Domain Consent Directive) [1]
- Access to a particular report (Record-level Consent Directive)
- Access for all users from a particular organization (HIC-Agent Consent Directive)

[1] The Domain Consent Directive allows a person to withhold or withdraw consent for one but not all of the EHR repositories. At this time, there is only one EHR repository, so the Domain and the Global Consent Directives are the same until other repositories are added.

Applying Consent Directives

If a patient contacts a Health Information Custodian (HIC) in order to either revoke or reinstate consent to access that patient's data, the HIC should do the following:

1. Capture the consent directive information on the EHR Consent Form available on the eHealth Ontario web site.
2. Submit the consent directive information to eHealth Ontario by faxing it to 416-586-4397 or 1-866-831-0107

After putting the consent directive in place on the EHR, 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 wishes to place or revoke a consent directive that applies to data contributed by more than one HIC, the patient should complete the EHR Consent Form (available on the eHealth Ontario web site) or phone eHealth Ontario at 416-946-4767.

In all instances, eHealth Ontario will apply consent directives within seven (7) days of verifying the identity of the patient making the request. After that, you, as the person who received the request for the change in consent status, notify the patient that the request has been fulfilled. If you cannot notify the patient, eHealth Ontario will do so on your behalf if you so desire.

Overriding a Consent Directive[2]

DI CS provides a way for health care providers to temporarily override a patient's consent directive. If you perform a consent override, the system will ask you to confirm the purpose of the override and to subsequently notify the patient of the override occurrence. An override can only be performed at the express consent of the patient. A consent directive override lasts for no more than four (4) hours and applies to all users at the site.

Providers can temporarily override a consent directive when the provider has express consent from the patient or the patient's substitute decision maker.

A temporary override will be logged in the DI CS audit trail along with the identity of the person who placed the override.

[2] Providers accessing DI CS via the ClinicalConnect Viewer will not have the functionality to perform a consent directive override until ClinicalConnect is fully integrated with the consent management solution.

If a HIC's agent overrides the consent directive, eHealth Ontario will notify that HIC. Once contacted by eHealth Ontario, it is the responsibility of the HIC to do the following:

1. Investigate the override to ensure it was for one of the reasons stated above
2. Notify the patient of the override at the first opportunity.[3]

Access Requests

Quick Tip

When a patient wishes to access or correct data that your practice has contributed, follow your internal procedures for allowing access to or correction of that data, and document the request.

When a patient wishes to access or correct data that another HIC has contributed, direct the patient to contact eHealth Ontario at 416-946-4767 as soon as possible to make the request.

Access Requests Made by Patients for DI CS Data

Under PHIPA, patients or their substitute decision makers have a right to access data held by a HIC. When providers receive requests for records that they have collected, created, or contributed, they must follow Part V of PHIPA as well as all its related internal policies, procedures, and practices before responding.

In instances where requests for access involve information contributed by another HIC or by multiple HICs, providers are required to do the following:

1. Notify the individual making the request that the request for access involves PHI that is beyond the control of that provider
2. Direct the individual making the request to contact eHealth Ontario at 1-866-250-1554 or http://www.ehealthontario.on.ca/en/contact.

As per the *EHR Access and Correction Policy* (available on the eHealth Ontario web site), eHealth Ontario may seek assistance from the HIC when responding to a request for access.

[3] For more information on what to include in this notice to the patient, see the *EHR Consent Management Policy* on the eHealth Ontario resources web site. If you cannot notify the patient, ask eHealth Ontario to notify the patient on your behalf.

Requests for Audit Logs

When an individual directly asks a provider for access related to DI CS audit logs, the HIC is required to do the following:

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

Correction Requests

When a person directly asks a HIC to correct health records that were created and contributed to DI CS solely by that HIC, that HIC is required to follow Part V of PHIPA and its internal policies, procedures, and practices. At the request of the patient, when a correction request is fulfilled, the HIC must notify eHealth Ontario of the correction and also request an audit report of who has accessed the patient's record. This audit report will indicate who has accessed the patient's DI CS records and what HIC(s) those people are connected to. The HIC must then contact relevant sites that have viewed the patient's record and notify them of the correction.

When a HIC receives a request for correction directly from an individual, and when the request relates to records that were created by another or more than one HIC, the HIC must respond no later than two (2) days after receiving the request by doing the following:

1. Notifying the individual that the request for correction involves PHI not within the HIC's custody or control
2. Directing the individual to contact eHealth Ontario at 1-866-250-1554 or http://www.ehealthontario.on.ca/en/contact.

Before eHealth Ontario responds to this type of request, it may seek assistance from the HIC(s).

Privacy Complaints and Inquiries

Quick Tip

When an individual submits an inquiry or complaint related to DI CS, tell the person to contact eHealth Ontario with the inquiry or complaint.

If a HIC directly receives an inquiry or complaint related solely to that HIC's agents, its service providers, or its DI CS records, the HIC is required to follow its own internal policies, procedures, and practices.

When a HIC directly receives an inquiry or complaint related solely to DI CS or to eHealth Ontario's agents or electronic service providers, and if that HIC is unable to address the situation, it must immediately do the following:

1. Notify the individual that the HIC is unable to respond to the inquiry/complaint
2. Direct the individual to contact eHealth Ontario at 1-866-250-1554 or http://www.ehealthontario.on.ca/en/contact.

If eHealth Ontario requires assistance when responding to inquiries or complaints, it may seek assistance from the HIC(s).

Privacy Breach Management

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.

The *EHR Privacy Breach Management Policy* (available on the eHealth Ontario web site) describes detailed steps to be taken in the event of a privacy breach or 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 no later than the end of the following business day. A HIC must report a breach or incident to eHealth Ontario when that HIC becomes aware of an actual or suspected privacy breach caused or contributed to by one or more of the following:

- 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
- Agents or electronic service providers working for eHealth Ontario
- 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 that solely created and contributed the data to DI CS, the HIC shall follow its internal policies, procedures, and practices to notify the individual(s) to whom the PHI relates at the first reasonable opportunity. These activities are intended to contain, investigate, and remediate the privacy breach in accordance with PHIPA.

In instances where a breach was caused by a HIC that did not solely create and contribute the PHI to DI CS, the HIC, in consultation with eHealth Ontario as well as the other HICs who contributed data, 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* (available on the eHealth Ontario web site).

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 (2) years after the request was made.

PHIPA requires HICs to ensure that their records are retained for a specified period and transferred and disposed of in a secure manner. HICs must ensure that records are protected and disposed of in accordance with the *Information Security Policy* (available on the eHealth Ontario web site).

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

Information Type	**Retention Period**
PHI in the EHR system	The longer of the following time periods: • As long as the HIC that created and contributed the PHI to the EHR retains the PHI in its local systems • In accordance with the retention schedule of the HIC that created and contributed the PHI to the EHR • 30 years after the most recent instance of PHI being used for the purpose of providing health care; or 10 years after the patient has expired and in accordance with any applicable court order or court action or other legal requirement
Audit logs and audit reports that contain PHI and are in either or both of the following categories: o Created and maintained for compliance purposes o Created and maintained for troubleshooting	The longer of 30 years or when PHI is removed from DI CS Retain audit logs and audit reports that contain PHI created and maintained for troubleshooting and other operational purposes only as long as needed but no longer than 60 days unless expressly authorized by appropriate by eHealth Ontario CPO or authorized delegate to retain longer.
Archival copies of the following: o The PHI in DI CS o Audit logs and audit reports containing PHI	Equals the retention period of the PHI in DI CS or the audit logs and audit reports respectively
Backups of PHI in the EHR system and audit logs and audit reports containing PHI	No longer than two (2) years

Information Type	Retention Period
Information collected to respond to individuals related to one or more of the following: ○ Request for Access or Request for Correction under PHIPA ○ Request to make, modify, or withdraw a Consent Directive under PHIPA ○ Inquiries or Complaints under PHIPA	Two (2) years after the request was made. For complaints, retain for two (2) years after the complaint has been closed by the HIC, eHealth Ontario, or the IPC, whichever is longer.
Information created about an individual as part of an investigation of privacy breaches and/or security incidents	Two (2) years after the privacy breach has been closed by the HIC, eHealth Ontario, or the Information and Privacy Commissioner of Ontario, whichever is longer
Information used for identity provider registration that contains PI	Seven (7) years after last use
End User Credential Information where the HIC is an Identity Provider	Permanent
System-level logs, tracking logs, reports, and related documents for privacy and security tasks that do not contain PHI	Minimum of two (2) years
Authentication Events where the 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	Minimum of two (2) years
Assurance-related documents	10 years
eHealth Ontario business documentation	Minimum of seven (7) years

Specific types of PHI included in each of the information types can be found in the *EHR Retention Policy* (available on the eHealth Ontario web site).

Privacy and Security Training

HICs are required to provide privacy and security training to their agents and electronic service providers prior to allowing them access to the 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 with respect to the EHR system. Training should be completed prior to being provisioned an account for accessing DI CS. Role-based training materials developed by eHealth Ontario can facilitate this training requirement. For information on what to include in privacy and security training, see the *EHR Privacy and Security Training Policy* (available on the eHealth Ontario web site). All end users must have taken 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 done 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 or breach management processes, contact eHealth Ontario at 1-866-250-1554.

Ensure that you do not include any personal information (PI) or personal health information (PHI) in any e-mail messages sent to eHealth Ontario.

Security Incident and Breach Management

This section instructs HICs on how to report security incidents and breaches to eHealth Ontario.

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

- 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, or 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 DI CS.

Instructions for Health Care Providers

If you become aware of or suspect a security incident or breach of DI CS 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, contact the eHealth Ontario service desk at 1-866-250-1554 and open a security incident ticket. 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 PHI or PI 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 DI CS 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 eHealth Ontario service desk at 1-866-250-1554 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 cooperate with any investigations conducted by eHealth Ontario with respect to 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 who reported the incident
3. Details about the reported incident (e.g., the type and how it was detected)
4. Any effects of the reported incident
5. Any actions aimed at containing the incident undertaken 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 consultation with the requestor.

Summary of Security Safeguards in Place at eHealth Ontario

Administrative Safeguards

- The Chief Privacy Officer and the Chief Security Officer at eHealth Ontario are accountable for privacy and security.
- A comprehensive set of information security policies that align with eHealth Ontario's 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 them, understood them, and are committed to complying with them.
- All staff and contractors must sign confidentiality agreements and undergo criminal background checks prior to joining or providing services to eHealth Ontario.
- A security screening policy requires eHealth Ontario staff to have an appropriate level of clearance for the sensitivity of the information they may access.
- Mandatory privacy and security awareness and training programs exist at eHealth Ontario.
- Staff and contractors at eHealth Ontario generally have no ability or permission to access PHI. If access to PHI is required in the course of providing eHealth Ontario services, individuals are prohibited from using or disclosing such information for any other purposes.
- Through formal contracts and service level agreements, eHealth Ontario ensures 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.
- Staff, consultants, suppliers, and clients of eHealth Ontario 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 as well as 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.
- Affected health information custodians may, at their request, receive written copies of the results of privacy impact assessments and security threat and risk assessments from eHealth Ontario.
- A formal risk management program at eHealth Ontario 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 that record user activities, system administrator's activities, exceptions, and information security events must be produced and kept for a minimum of six (6) months online and a minimum of 18 months in the archive. These logs exist to assist in incident and problem management, future investigations, and access control monitoring.
- An electronic record of all accesses to all or part of the PHI contained in the EHR is kept by eHealth Ontario. As well, eHealth Ontario 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 are 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 and is controlled via proper authorization and strong, two-factor authentication. All system and application access activities are logged.
- Network traffic is monitored by eHealth Ontario through security mechanisms such as routers, switches, and network firewalls, and eHealth Ontario 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 staff computers are lost or stolen, data confidentiality and integrity are not at risk.
- Data integrity controls are implemented as a quality assurance activity on the PHI 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 they can be easily restored in case of operational incidents.
- A comprehensive disaster recovery (DR) and business continuity plan (BCP) are in place and are tested and updated regularly.

Physical Safeguards

- The eHealth Ontario data centres are purpose-built facilities with appropriate environmental controls, and they are physically secured against unauthorized access. They are staffed and monitored continuously by trained security personnel.
- Specific physical security zones with increasing physical security controls are implemented to separate and control access to the public zone, the delivery and loading area, office space, and computer rooms.
- 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 PI or PHI is physically restricted to only the staff members whose role involves handling of PI or PHI. 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 PI or PHI 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.

Glossary

Term	Definition
CPS	Certification practices statement
DI	Diagnostic imaging
DI CS	Diagnostic Imaging Common Service (a.k.a. Provincial DI Viewer)
DI-R	Diagnostic imaging repository
EHR	Electronic health record
ENITS	Emergency Neuro Image Transfer System
HIC	Health information custodian
HN	Health (card) number
IHF	Independent health facility
ONE® ID	A set of systems and processes for assigning and managing electronic identities to allow secure access to eHealth Ontario services
PHI	Personal health information
PHIPA	Personal Health Information Protection Act, 2004
PI	Personal information
RA	Registration Authority

/end V3: April 2017/