Health Care Provider Guide

Diagnostic Imaging Common Service

Version: 2.0
**General Information**

Purpose and Scope ........................................................................................................... 3
Audience ............................................................................................................................... 3
Related Documents .............................................................................................................. 3
Glossary ................................................................................................................................. 4

**Service Description**

Overview ............................................................................................................................... 5
Benefits .................................................................................................................................. 6
To You
To Your Patients .................................................................................................................. 6

**Privacy and Security**

Patient Consent .................................................................................................................... 7
Consent Management ........................................................................................................... 7
Applying Consent Directives .............................................................................................. 8
Overriding a Consent Directive ............................................................................................ 8
Access Requests ................................................................................................................... 10
Access Requests Made by Patients for DI Common Service data ........................................ 10
Requests for Audit Logs ....................................................................................................... 10
Correction Requests ............................................................................................................ 10
Privacy Complaints and Inquiries ....................................................................................... 11
Privacy Breach Management ................................................................................................. 11
Retention ............................................................................................................................... 12
Privacy and Security Training ............................................................................................... 14
Privacy-Related Questions from Health Care Provider Sites .................................................. 14
Security Incident and Breach Management ........................................................................... 14
Instructions for Health Care Providers .................................................................................. 15
Instructions for Privacy Officers ........................................................................................... 15

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

Administrative Safeguards ................................................................................................... 16
Technical Safeguards .......................................................................................................... 17
Physical Safeguards ............................................................................................................. 18
General Information

Purpose and Scope

This guide describes the functions and associated benefits provided by eHealth Ontario’s Diagnostic Imaging (DI) Common Service application as well as the privacy and security procedures and obligations 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 our DI Common Service application to access patients’ DI Results.

Related Documents

The DI service 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
## Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPS</td>
<td>Certification Practices Statement</td>
</tr>
<tr>
<td>DI</td>
<td>Diagnostic Imaging</td>
</tr>
<tr>
<td>DI-r</td>
<td>Regional Diagnostic Imaging repository</td>
</tr>
<tr>
<td>EHR</td>
<td>Electronic Health Record</td>
</tr>
<tr>
<td>ENITS</td>
<td>Emergency Neuro Image Transfer System</td>
</tr>
<tr>
<td>HIC</td>
<td>Health Information Custodian</td>
</tr>
<tr>
<td>HN</td>
<td>Health (Card) Number</td>
</tr>
<tr>
<td>IHF</td>
<td>Independent Health Facility</td>
</tr>
<tr>
<td>ONE® ID</td>
<td>Set of systems and processes for assigning and managing electronic identities to allow secure access to eHealth Ontario services</td>
</tr>
<tr>
<td>PHI</td>
<td>Personal Health Information</td>
</tr>
<tr>
<td>PHIPA</td>
<td>Personal Health Information Protection Act, 2004</td>
</tr>
<tr>
<td>PI</td>
<td>Personal Information</td>
</tr>
<tr>
<td>RA</td>
<td>Registration Authority</td>
</tr>
</tbody>
</table>
Service Description

Overview

Diagnostic Imaging (DI) Common Service is an initiative that enables all hospital and community-based health care providers across Ontario to share and view DI results.

DI Common Service gives authorized providers important information to make better decisions about a patient’s treatment. Prior to DI Common Service, authorized providers could share images and reports securely with other providers only within their respective regional DI repositories. Now, with the first phase of DI Common Service, diagnostic reports can be shared across the entire province; future releases will enable sharing of other types of diagnostic imaging information, such as images. The diagnostic images and corresponding reports are stored in repositories from which they can be retrieved in digital format. This capability is providing clinicians with quicker access to information resulting in faster diagnoses.

The DI Program gives Ontario’s health care providers important information to make better decisions about a patient’s treatment anywhere at any time. Authorized health care providers can share images and reports securely with other providers. The diagnostic images and corresponding reports are stored in a regional repository from which they can be retrieved in digital format. This capability is reducing the need for patients to travel to see a specialist. The program contains a number of initiatives in addition to the DI Common Service, which include hospital Diagnostic Imaging Repositories, integration of Independent Health Facilities (IHF) and the Emergency Neuro Image Transfer System (ENITS).

The DI program 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 activity information when they need it.
Benefits

To You

- Access to diagnostic reports across Ontario
- Faster and easier access to images and reports 24/7
- Remote access to diagnostic imaging reports for off-hours coverage
- Real-time clinical collaboration, increasing access to a broader range of specialists

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
- Eliminates the need to physically transfer images or compact discs to specialists

1 The initial release of DI Common Service enables provincial sharing of diagnostic reports, while future releases will enable provincial sharing of diagnostic images and other types of DI information.
Privacy and Security

Patient Consent

Quick Tip

The EHR system gives patients, or their substitute decision maker, the option to allow or restrict access to patient data. Should a patient choose to place a consent directive in the DI Common Service, he/she must fill out the EHR Consent form at http://www.ehealthontario.on.ca/en/initiatives/resources 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.

Consent Management

The electronic health record (EHR) system gives patients or their substitute decision maker the option to allow or restrict access to patient data within DI Common Service. If a patient restricts access to his/her data by applying a consent directive, providers querying DI Common Service will be unable to access information relating to that patient information to which a consent directive has been applied.

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

- All of a patient’s records (Global/Domain Consent Directive)\(^2\)
- A particular report (Record-level Consent Directive)
- All users from a particular organization (HIC-Agent Consent Directive).

---

\(^2\) 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; therefore 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) and wishes to either place a restriction on access to his / her information, or reinstate access (remove the restriction), the HIC should:

- Capture the consent directive information on the EHR Consent Form at [http://www.ehealthontario.on.ca/en/initiatives/resources](http://www.ehealthontario.on.ca/en/initiatives/resources), 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 at [http://www.ehealthontario.on.ca/en/initiatives/resources](http://www.ehealthontario.on.ca/en/initiatives/resources), or contact us directly at 416-946-4767.

In all instances, eHealth Ontario will apply consent directives within seven 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 at your direction.

**Overriding a Consent Directive**

**Quick Tip**

DI Common Service permits a health care provider to temporarily override a patient’s consent directive. If you perform a consent override, you will be asked by eHealth Ontario 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, 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 four hours.

DI Common Service 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:

---

3 Providers accessing DI Common Service 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.
• With the express consent from the patient or the patient’s substitute decision maker;
• 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 individual 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 individual to whom the PHI relates to or to a group of persons.

A temporary override will be logged in DI Common Service, along with the identity of the overriding health care provider. The override will be in effect for no more than four hours.

eHealth Ontario will notify the HIC if one of his /her agents overrides the consent directive. Once contacted by eHealth Ontario, it is the responsibility of the HIC 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.\(^4\)

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 individual 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 at http://www.ehealthontario.on.ca/en/initiatives/resources.

\(^4\) For more information on what to include in this notice to the patient, please see the EHR Consent Management Policy at http://www.ehealthontario.on.ca/en/initiatives/resources. If you cannot notify the patient, contact eHealth Ontario and notify the patient on your behalf.
**Access Requests**

**Quick Tip**
When a patient requests to view or correct data your practice has contributed, 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 data that other HICs have 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 Common Service data**

Under PHIPA, patients or their substitute decision makers have a right to access data held by a HIC. When a provider receives a request for records he / she has collected, created and / or contributed to, he / she 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 involves information contributed by another HIC or by multiple HICs, providers are required to:

- Notify the individual that the request for access involves PHI not within his / her custody or control, and
- Direct the individual to contact eHealth Ontario at 1-866-250-1554 or online at [http://www.ehealthontario.on.ca/en/contact](http://www.ehealthontario.on.ca/en/contact).

As per the EHR Access and Correction Policy at [http://www.ehealthontario.on.ca/en/initiatives/resources](http://www.ehealthontario.on.ca/en/initiatives/resources), 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 an individual related to audit logs for records stored in DI Common Service, 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 online at [http://www.ehealthontario.on.ca/en/contact](http://www.ehealthontario.on.ca/en/contact).

**Correction Requests**

When a HIC receives a request for correction directly from an individual related to health records that were created and contributed to DI Common Service 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 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 his /her 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 an
individual related to records that were 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 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.

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

**Privacy Complaints and Inquiries**

**Quick Tip**

When an individual submits an inquiry or complaint related to DI Common Service, 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 DI Common Service, or his/her agents and/or service providers, the HIC is required to follow his/her own internal policies, procedures, and practices.

When a HIC directly receives an inquiry/complaint related solely to DI Common Service or to eHealth Ontario’s agents or electronic service providers that he/she is unable to address, he/she must immediately:

- Notify the individual that you are unable to respond to the inquiry/complaint, and
- Direct the individual to contact eHealth Ontario at 1-866-250-1554 or online through http://www.ehealthontario.on.ca/en/contact.

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

**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* at http://www.ehealthontario.on.ca/en/initiatives/resources 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 no later than the end of the following 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 to 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 DI Common Service, 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 in accordance with PHIPA 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 DI Common Service, 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.

**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 2 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 at http://www.ehealthontario.on.ca/en/initiatives/resources.
HICs will retain records containing the following information for the corresponding retention period:

<table>
<thead>
<tr>
<th>Information Type</th>
<th>Retention Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>PHI in the EHR system</td>
<td>The longer of the following time periods:</td>
</tr>
<tr>
<td></td>
<td>- As long as the HIC that created and contributed the PHI to the EHR retains the PHI in its local systems;</td>
</tr>
<tr>
<td></td>
<td>- In accordance with the retention schedule of the HIC that created and contributed the PHI to the EHR;</td>
</tr>
<tr>
<td></td>
<td>- 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.</td>
</tr>
<tr>
<td>Audit logs and audit reports that contain PHI:</td>
<td>30 years or when PHI is removed from EHRs — whichever is longer.</td>
</tr>
<tr>
<td>Backups of PHI in the EHR system and audit logs and audit reports containing PHI</td>
<td>Retained no longer than 2 years.</td>
</tr>
<tr>
<td>Information collected to respond to individuals related to their:</td>
<td>2 years after the request was made.</td>
</tr>
<tr>
<td>o Request for Access or Request for Correction under PHIPA;</td>
<td>For complaints, retain for 2 years after the complaint has been closed by the HIC, eHealth Ontario, or the IPC, whichever is longer.</td>
</tr>
<tr>
<td>o Request to make, modify, or withdraw a Consent Directive under PHIPA or</td>
<td></td>
</tr>
<tr>
<td>o Inquiries or Complaints under PHIPA.</td>
<td></td>
</tr>
<tr>
<td>Information created about an individual as part of an investigation of privacy breaches and/or security incidents.</td>
<td>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.</td>
</tr>
<tr>
<td>Information used for identity provider registration that contains PI</td>
<td>7 years after last use.</td>
</tr>
<tr>
<td>System-level logs, tracking logs, reports and related documents for privacy and security tasks that do not contain PHI</td>
<td>For a minimum of 2 years.</td>
</tr>
<tr>
<td>Templates or resources developed by eHealth Ontario in respect of the EHR</td>
<td>For a minimum of 2 years.</td>
</tr>
<tr>
<td>Assurance-related documents</td>
<td>10 years.</td>
</tr>
<tr>
<td>eHealth Ontario business documentation</td>
<td>For a minimum of 7 years.</td>
</tr>
</tbody>
</table>
Specific types of PHI included in each of the information types can be found in the EHR Retention Policy at http://www.ehealthontario.on.ca/en/initiatives/resources.

**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 accessing DI Common Service. 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 (PI) or personal health information (PHI) in any emails to eHealth Ontario.

**Security Incident and Breach Management**

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

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 DI Common Service.

**Instructions for Health Care Providers**

If you become aware of, or suspect, a security incident or breach of DI Common Service 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 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 Common Service 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 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 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 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 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’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 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.

- 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 PHI 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 managers 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 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 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 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 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.
Copyright Notice
Copyright © 2016, eHealth Ontario

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

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