Ontario Health

Information Security Policy

Version: 2.8

Document ID: 3541

Document Control

Next Review Date: Every two years or otherwise established by the Connecting Security Committee.

Approval History

APPROVER(S)	APPROVED DATE
Connecting Security Committee	2017-02-21
Connecting Security Committee	2018-03-26
Connecting Security Committee	2019-07-04
Connecting Security Committee	2021-03-18

Revision History

VERSION NO.	DATE	SUMMARY OF CHANGE	CHANGED BY
2.0	2013-12-23	Nov 2013 version adopted from the cGTA PSWG and revision.	Mark Carter
2.1	2014-08-20	Updated based on feedback of CSC Members. Added a reference to the Privacy and Assurance Policy including bullet points to support content.	Mark Carter
2.2	2014-09-09	Policy approved at the CSC meeting September 9th.	Mark Carter
2.3	2015-01-21	Aligned name of access control policy based on final wave 3 CSC decision.	Mark Carter
2.4	2015-10-19	Updated policies to note the change in governance. The Steering Committee was replaced by the Applicable Oversight Body. The regional privacy and security committee has been removed from the exemption decision process. Governance responsibilities of the Connecting Security Committee have been added to the roles and responsibilities section.	Mark Carter
2.5	2017-02-21	Updated policies to incorporate 2017 refresh changes. Definition of EHR Solution was adjusted. A number of controls were rephrased to note “participating” in the EHR Solution.	Ravi Addepalli
2.6	March 16, 2018	Updated standard to include Patient access to the EHR.	Geovanny Diaz
2.7	July 4th, 2019	Updated Policy to include references to the Threat Risk Management Standard and to require EHR Security Assessments.	Ravi Addepalli

VERSION NO.	DATE	SUMMARY OF CHANGE	CHANGED BY
2.8	2021-01-21	Review of the document with minor changes, updated references and the review cycle to biennially.	Ana Fukushima

Information Security Policy

Purpose

To protect the confidentiality, integrity, and availability of [the EHR Solution] and personal health information (PHI) stored in or processed by [the EHR Solution]. In doing so, this policy will outline the framework for [the EHR Solution] information security governance by:

- Defining the information security principles to manage:
    - Personal Health Information (PHI);
    - [The EHR Solution] and information systems or information technologies that connect to [the EHR Solution]; and
- Establishing the roles and responsibilities for ensuring the principles in this policy are implemented and maintained.

Scope

This policy applies to [the EHR Solution] Program, their agents and their Electronic Service Providers and to [the EHR Solution], including all Patient Portals/Applications.

For health information custodians (HICs) that use [the EHR Solution] to view, handle or otherwise deal with PHI by provisioning access through:

- Local identity provider technology (local IdP), this policy applies to:
    - The HIC's local access control and identity management infrastructure ("identity provider services") that manages the authentication and authorization used to provide access to [the EHR Solution] (e.g., [the EHR Solution] Security Token Service Solution, Microsoft Active Directory Federation Services 2.0, etc.)
    - Direct network connectivity to [the EHR Solution] Provider Portal and administrative functionality, including components in the connection path (firewalls, proxies, etc.)
    - The integration of [the EHR Solution] Provider Portal with the HIC's local health information system (HIS) or electronic medical record (EMR) application(s)
- Ontario Health's ONE® ID service, this policy applies to:
    - Direct network connectivity to [the EHR Solution] administrative functionality, including components in the connection path (firewalls, proxies, etc.)

In addition to the scope set out for viewing sites, for HICs that create or contribute PHI to [the EHR Solution] Clinical Data Repository ("contributing sites"), this policy also applies to:

- The data contribution endpoints that provide PHI to [the EHR Solution]'s Clinical Data Repository

- The information technology and processes that ensure the quality of the data submitted (e.g., terminology mapping)

This policy does not apply to any HIC, their agents or their Electronic Service Providers who do not view, create or contribute to [the EHR Solution].

Definitions

[The EHR Solution]: [The EHR Solution] and supporting systems designed to store and make available specified electronic PHI from the electronic health information systems of HICs.
[The EHR Solution] includes Patient Portals/Applications (HIC or non-HIC affiliated) that facilitate Patient access to the EHR. These applications may be:

- Provider-Gated (Provider facilitates communication with Patient)
- Direct-to-Patients (Patient has direct access to EHR)
- Patient-Gated (Patient delegates access to a Substitute Decision Maker/additional delegates (i.e., family member, physician)

[The EHR Solution] Program: Also known as the Program Office; consists of Agents and Electronic Service Providers who support [the EHR Solution] including privacy and security-related activities, initiatives and processes.

Applicable Oversight Body: The Applicable Oversight Body is comprised of senior-level executives who oversee all aspects of [the EHR Solution]. See the Policy Governance Structure section within the Information Security Policy.

Connecting Security Committee (CSC): The provincial security forum consisting of senior security representatives from across the regions and Ontario Health. This is a decision making body responsible for establishing a functional and usable information security governance framework for participating organizations in the EHR.

Data Contribution End Point(s): Technology and related processes that provide data to the Clinical Data Repository or are queried to provide data to a Clinical Viewer. Typically, these systems are the Information System (e.g., Hospital Information System, Laboratory Information System, Clinical Information System, HL7 Interface Engine, etc.) that directly connects to [the EHR Solution] to provide clinical data.

EHR Security Assessment: A self-security assessment based on EHR security standards.

Electronic Service Provider: A person or entity that provides goods or services for the purpose of enabling a HIC to use electronic means to collect, use, modify, disclose, retain or dispose of PHI, and includes a health information network provider.

Identity Provider Services: Technology and related supporting services, policies, processes, and procedures that are used to create, maintain, secure, validate, assert, and manage electronic identities to [the EHR Solution].
Information system: A discrete set of information technology organized for the collection, processing, maintenance, use, disclosure, destruction, or disposal of information.

Information security: Refers to the protection of all types of information, information systems and information technologies from unauthorized access, collection, use, disclosure, transfer, disruption, modification, destruction or disposal.

Information system: A discrete set of information technology organized for the collection, processing, maintenance, use, disclosure, destruction, or disposal of information.

Information technology: Any asset (physical or logical) that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. It includes, but is not limited to, hardware, software, firmware, ancillary equipment, and related resources.

Threat Risk Assessment: An independent assessment that analyses software systems for vulnerabilities, potential threats, and evaluates the resulting risks.

Vulnerability Scan: An automated process of proactively identifying security vulnerabilities of Information Systems in order to determine if and where a system can be exploited. Vulnerability scanners use software to look for security flaws based on a database of known flaws, and may be credentialed or non-credentialed.

Shall/Must: Used for absolute requirements, i.e., they are not optional.

Should: Used when valid reasons exist in certain circumstances not to implement the requirement; however, the implementer must understand the implications before choosing a different course and must consider implementing compensating controls.

May: The requirement is only a recommendation, or provided as an implementation example and is not intended on being exhaustive.

Policy Requirements

1. Principles

Acceptable Use of Information and Information Technology

1.1. [The EHR Solution] Program and HICs must define behavioural requirements governing the acceptable use of information and information technology to which [the EHR Solution]'s agents and Electronic Service Providers, and HICs, their agents and Electronic Services Providers with access to [the EHR Solution] must adhere.

Refer to the Acceptable Use of Information and Information Technology Standard.

Information Security Training

1.2. [The EHR Solution] Program and HICs must foster an information security-positive culture. This may be achieved by implementing an information security awareness and education program to help all persons with access to [the EHR Solution] to understand their information security-related obligations.

Refer to the Privacy and Security Training Policy.

Threat Risk Management

1.3. [The EHR Solution] Program must perform information security threat risk assessments (TRAs) and EHR Security Assessments on [the EHR Solution] and must track, and mitigate or formally accept all of their risks that are identified through a TRA and EHR security assessment.

1.4. HICs should perform information security TRAs on their identity provider services and data contribution endpoints.

Refer to the Threat Risk Management Standard.

Cryptography

1.5. [The EHR Solution] Program must implement cryptographic solutions in [the EHR Solution] to protect the confidentiality and integrity of PHI where appropriate, as well as to confirm the identity of the originator of a communication.

1.6. HICs must implement cryptographic solutions on their relevant information systems to protect the confidentiality and integrity of PHI that is accessed through [the EHR Solution].

Refer to the Cryptography Standard.

Information and Asset Management

1.7. [The EHR Solution] Program must classify and define protection requirements for PHI in [the EHR Solution] in a manner that protects its confidentiality, integrity, and availability in any form (e.g., paper or electronic) throughout its information lifecycle.

Refer to the Information and Asset Management Standard.

Access Control and Identity Management

1.8. [The EHR Solution] Program and HICs must establish appropriate access and identity management controls to manage all persons and information system access to [the EHR Solution]. These controls must:

1.8.1. Define the information security responsibilities of all persons who have access to [the EHR Solution].

1.8.2. Ensure that only authorized persons are granted access to [the EHR Solution] and that personal accountability is assured.

1.8.3. Ensure that only authorized information systems are granted access to [the EHR Solution].

1.8.4. Provide authorized persons or information systems with only the least amount of privileges that are sufficient to enable them to perform their duties but do not permit them to exceed their authority.

Refer to the Access Control and Identity Management Standard for System Level Access and the Identity Federation Standard.

Logging and Monitoring

1.9. [The EHR Solution] Program must log and monitor all access to [the EHR Solution], and must log and monitor information system events on [the EHR Solution].

1.10. HICs must log and monitor all access by the HIC, their agents or Electronic Service Providers to [the EHR Solution]'s Provider Portal, and must log and monitor information system events on their identity provider services and data contribution endpoints.

Refer to the Security Logging and Monitoring Standard.

Network and Operations

1.11. [The EHR Solution] Program must implement controls to secure their network infrastructure, and establish procedures to secure the ongoing management and operation of [the EHR Solution].

1.12. HICs must implement controls to secure their network infrastructure, and establish procedures to secure the ongoing management and operation of their identity provider services and data contribution endpoints.

Refer to the Network and Operations Standard.

System Development Lifecycle

1.13. [The EHR Solution] Program must define information system development and change control requirements, and ensure that all system development activities performed on [the EHR Solution] are carried out in accordance with these requirements.

1.14. HICs should define information system development and change control requirements and ensure that identity provider services and data contribution endpoint development activities are carried out in accordance with these requirements.

Refer to the System Development Lifecycle Standard.

Electronic Service Providers

1.15. [The EHR Solution] Program must ensure that their Electronic Service Providers who will have access to [the EHR Solution], or who manage or provide support to [the EHR Solution] have adequate information security controls in place to protect and maintain the level of confidentiality, integrity and availability.

1.16. HICs must ensure that their Electronic Service Providers who will have access to their identity provider services or data contribution endpoints, or who manage or provide support to these systems have adequate information security controls in place to protect and maintain the level of confidentiality, integrity and availability.

Refer to the Electronic Service Provider Standard.

Physical Security

1.17. [The EHR Solution] Program must implement controls to protect against the risks of unauthorized physical access and environmental damage to [the EHR Solution].

1.18. HICs must implement controls to protect against the risks of unauthorized physical access and environmental damage to their identity provider services and data contribution endpoints.

Refer to the Physical Security Standard.

Business Continuity

1.19. [The EHR Solution] Program must implement procedures necessary to ensure that [the EHR Solution]:

1.19.1. Remains available, especially in the event of a disaster; or

1.19.2. Can be recovered in the event that operations are disrupted.

1.20. HICs should develop business continuity plans to ensure that their identity provider services and data contribution endpoints:

1.20.1. Remain available, especially in the event of a disaster; or

1.20.2. Can be recovered in the event that operations are disrupted.

Refer to the Business Continuity Standard.

Information Security Incident Management

1.21. [The EHR Solution] Program and HICs must implement an information security incident management process to identify and resolve information security incidents related to [the EHR Solution] quickly and effectively while minimizing their impact and reducing the risk of similar information security incidents from occurring.

Refer to the Information Security Incident Management Standard.

Privacy and Security Assurance

1.22. HICs must identify and mitigate privacy and security risks and areas of non-compliance in respect of [the EHR Solution], including through privacy and security readiness self-assessments, privacy and security operational self-attestations, auditing and monitoring activities and assurance of agents and Electronic Service Providers.

1.23. [The EHR Solution] Program Office must identify and mitigate privacy and security risks and areas of non-compliance in respect of [the EHR Solution], including through privacy impact assessments, threat risk assessments, privacy and security readiness self-assessments, privacy and security operational self-attestations, auditing and monitoring activities and assurance of agents, Electronic Service Providers and third parties.

Refer to the Privacy and Security Harmonized Assurance Standard.

2. Information Security Exemption Requirements

2.1. All shall/must requirements are mandatory. Any deviation from a mandatory requirement in a [the EHR Solution] information security policy, standard, or supporting document must be approved by the Applicable Oversight Body.

2.2. All information security exemption requests must be assessed by the Ontario Health Privacy and Security Operations Team and then reviewed by the Applicable Oversight Body for approval.

2.3. [The EHR Solution] Program must log all information security exemption requests.

2.4. Information security exemptions may be requested and granted for any length of time. However, all approved exemptions must be reviewed by the Ontario Health Privacy and Security Operations Team at a minimum, every two years, to ensure that the level of risk has not increased or that new risks have not appeared. If the Ontario Health Privacy and Security Operations Team reassesses the risk at a higher level or identifies additional risks, then the exemption must be presented to the Applicable Oversight Body for re-approval.

2.5. The Applicable Oversight Body has the right to revoke any approved information security exemptions. However, participants must be provided with at least six months to comply with the policy if their information security exemption is revoked.

Refer to Appendix A: Information Security Exemption Requests.

3. Roles and Responsibilities

Privacy and Security Committee

3.1. The Privacy and Security Committee must:

3.1.1. Review, provide feedback and ratify all [the EHR Solution] information security policies and standards.

Applicable Oversight Body

3.2. The Applicable Oversight Body must:

3.2.1. Approve all information security policies and standards.

3.2.2. Approve or deny all information security exemption requests.

3.2.3. Where applicable, hold all [the EHR Solution] agents and Electronic Service Providers, and HICs accountable for unauthorized or inappropriate access, collection, use, disclosure, disposal, modification, or interference with [the EHR Solution], PHI or [the EHR Solution] information.

Ontario Health Privacy and Security Operations Team

3.3. Ontario Health Privacy and Security Operations Team must:

3.3.1. Provide information security leadership and guidance to HICs.

3.3.2. Develop, implement and maintain an information security program that will establish an information security governance, strategy and policy framework for the HICs, Innovators and external service providers.

3.3.3. Develop, implement and maintain supporting policies, standards and supporting documents that uphold and expand upon the principles of this policy.

3.3.4. Provide guidance to the participants on information security training and awareness activities.

3.3.5. Monitor, report, and make recommendations for action or improvement to the PSC or CSC on information security posture, information security incidents, and the status and effectiveness of the information security program.

3.3.6. Review, and provide recommendations on all information security policy exemptions to the Applicable Oversight Body.

Health Information Custodians (HICs) and [The EHR Solution] Program Office

3.4. All HICs must:

3.4.1. Develop, implement and maintain an information security policy for their organization that upholds the principles of this policy and any other applicable information security policies, standards and supporting documents.

3.4.2. Designate an information security lead to ensure compliance with the principles outlined in this policy. The information security lead may be the same person as the appointed contact person required by Personal Health Information and Protection Act, 2004 (PHIPA) section15 or the site contact identified in the participation agreement.

3.4.3. Ensure that all agents and Electronic Service Providers who have access to [the EHR Solution] Services are appropriately informed of their information security responsibilities.

3.4.4. Require all agents and Electronic Service Providers who have access to [the EHR Solution] to agree to an end-user agreement that includes confidentiality provisions before being provided with access to [the EHR Solution].

3.4.5. Hold individual agents and Electronic Service Providers accountable for unauthorized or inappropriate access, collection, use, disclosure, disposal, destruction, modification, or interference with [the EHR Solution], or their information systems.

3.5. Connecting Security Committee:

3.5.1. Approve all information security policies.

3.5.2. Review trend reporting of security exemptions.

3.5.3. Review security incident reports.

Exemptions Any exemptions to this Policy must be approved by the Applicable Oversight Body, who will authorize exemptions only where there is clear justification to do so and only to the minimum extent necessary to meet the justified need.

See Appendix A: Information Security Exemption Requests in the Information Security Policy.

Enforcement All instances of non-compliance will be reviewed by the Applicable Oversight Body.

The Applicable Oversight Body has the authority to impose appropriate penalties, up to and including termination of Agreements with the HIC, Electronic Service Provider or termination of the access privileges of agents, and to require the implementation of remedial actions.

Policy Governance Structure

EHR Solution	Applicable Oversight Body
Connecting Ontario CDR	Ontario Health Strategy Committee
Digital Health Drug Repository	Ontario Health Strategy Committee
Diagnostic Imaging Common Services	Ontario Health Strategy Committee
Primary Care CDR	Ontario Health Strategy Committee

References

Legislative

- PHIPA, ss. 12, 13 and Part V.1
- O. Reg. 329/04, s. 6

International Standards

- ISO/IEC 27001:2013, Information Technology – Security Techniques – Information Security Management Systems – Requirements
- ISO/IEC 27002:2013, Information Technology – Security Techniques – Code of Practice for Information Security Management
- ISO/IEC 27005: 2018 Information Technology – Security Techniques – Information Security Risk Management
- ISO 27799:2016 Health Informatics – Information security management in health using ISO/IEC 27002

Ontario Health EHR Policy Documents

- Information Security Policy
- Acceptable Use of Information and Information Technology Standard
- Access Control and Identity Management Standard for System Level Access
- Local Registration Authority Procedures Standard
- Identity Federation Standard
- Business Continuity Standard
- Cryptography Standard
- Electronic Service Providers Standard
- Information Security Incident Management Standard
- Information and Asset Management Standard
- Network and Operations Standard
- Security Logging and Monitoring Standard
- Systems Development Lifecycle Standard
- Physical Security Standard
- Threat Risk Management Standard

Appendix A: Information Security Exemption Requests

Stage	Responsibility	Description
1	[The EHR Solution]'s agent or Electronic Service Provider - OR – A HIC, their agent or Electronic Service Provider ("Requestor")	Completes section 1 of the Information Security Exemption Request Form and sends the form to the Ontario Health Privacy and Security Operations Team.
2	The Ontario Health Privacy and Security Operations Team	Reviews the Information Security Exemption Request Form and completes section two.
3	Applicable Oversight Body	Reviews the request and either: • Approves the request • Approves the request with conditions; OR • Denys the request
4	The Ontario Health Privacy and Security Operations Team	Logs the Applicable Oversight Body's decision. Informs the requestor of the Applicable Oversight Body's decision and sends the HIC a copy of the Information Security Exemption Request Form. Stores the Information Security Exemption Request Form.

The following is the process for reviewing, and if necessary, reapproving information security exemptions that were originally approved for a period of greater than two years.

Stage	Responsibility	Description
1	The Ontario Health Privacy and Security Operations Team	Reviews the approved Information Security Exemption Request Form to assess if there is any change to the levels of risk originally identified. If there are no new risks and the original levels of risk have not increased: • The information security exemption request log is updated to indicate that the review was performed but there were no additional risks or increase to the level of original risks • Advises the requestor that the exemption request has been renewed • Logs renewal [process ends here] If new risks have been identified or the original level of risks have increased:

Stage	Responsibility	Description
		• The Ontario Health Privacy and Security Operations Team updates the information security exemption request form and notifies the requestor of the change in assessed risk.
2	Requestor	Reviews the updated information security exemption form and updates the form with any additional compensating controls that have been put in place or that they will be put in place to address the additional or increased level of risk.
3	The Ontario Health Privacy and Security Operations Team	Reviews the updated information security exemption form and revises the residual risk rating if necessary. Sends the information security exemption request form to the Applicable Oversight Body.
4	Applicable Oversight Body	Reviews the request and either: • Renews the exemption • Renews the exemption with conditions; OR • Revokes the exemption.
5	The Ontario Health Privacy and Security Operations Team	Logs the Applicable Oversight Body's decision. Informs the requestor of the Applicable Oversight Committee's decision and sends the HIC a copy of the Information Security Exemption Request Form. Stores the Information Security Exemption Request Form.

Information Security Exemption Request Form

Use this form to request an information security exemption. Please contact the Ontario Health Privacy and Security Operations Team before completing this form.

Form Completion Instructions		
1. Complete all fields as specified. Mandatory fields for the requestor are marked with an asterisk (*). If the form is incomplete, it will be returned to you. Indicate "Not Applicable" or "N/A" if the field is not applicable. 2. Once completed, please email the completed form to the Ontario Health Privacy and Security Operations Team. 3. If you have any questions regarding the completion of this form, please contact your [EHR Solution] Site Coordinator or the Ontario Health Privacy and Security Operations Team. **FORM TIPS: ● The form will open with the pointer in the start position. Begin typing your information ● Use the TAB key on your keyboard to move to the next box. You can use SHIFT + TAB to move back ● Click your left mouse button to fill in checkboxes**		
SECTION 1: Request (To be completed by the requestor)		
Requestor information		
First Name *		Last Name *
Title * *(e.g., CEO, CIO)*	Business Telephone * *(include ext.)* ( )	Business Email *
Organization/Site/Hospital Name *(e.g., ABC Hospital)*		
Name of policy/standard/supporting document for which an exemption is being requested: *		
Requirement(s) *		
Reason(s) for non-compliance: *		
Lists the information systems or specific information technologies for which this exemption will be applied: *		
Type and sensitivity of affected data: *		
Proposed plan for managing/mitigating the risks associated with non-compliance or list of compensating controls that have been implemented: *		
Anticipated duration (length of time) for exemption: *		

Additional Information:		
Internal Endorsement (e.g., endorsement by HIC's CIO):		
Please list the endorser's full name and job title (e.g., John Smith, Chief Information Officer). Attach an email from the endorser when you email your exemption request to the [the EHR Solution] Program.		
SECTION 2: Assessment (to be completed by the Ontario Health Privacy and Security Operations Team)		
[The EHR Solution] Reviewer's Information		
First Name *	Last Name *	
Title * *(e.g., Security Analyst)*	Business Telephone * *(include ext.)* ( )	Business Email *
Description of Risk(s) to [the EHR Solution] Program or the Connecting Solution*		**Level of Residual Risk** * *(e.g., high, medium, or low)*
Recommendation by the Ontario Health Privacy and Security Operations Team*		
[NOTE: Recommendation options are either: 1) approve request as is, 2) approve request with conditions (must list conditions), OR 3) deny request.]		
SECTION 3: Decision (to be completed by the Ontario Health Privacy and Security Operations Team)		
Applicable Oversight Body's Decision*		**Date of Endorsement***
[NOTE: Endorsement options are either: 1) recommend approving request as is, 2) recommend approving request with conditions (must list conditions); OR 3) recommend denying request.]		
Evidence of decision*		
(An email from an Applicable Oversight Body chair or copy of the meeting minutes is acceptable. Please include this evidence in the space below by inserting the file (.msg or PDF) as an object into this document. Note: You must unlock the form to embed the file.		