eHealth Ontario

Information and Asset Management Standard

Version: 1.6

Document ID: 3540

Ontario
eHealth Ontario

Document Control

Next Review Date : Annually or otherwise established by the Connecting Security Committee.

Approval History

APPROVER(S)	APPROVED DATE
Connecting Security Committee	2014-09-09
Connecting Security Committee	2018-03-26

Revision History

VERSION NO.	DATE	SUMMARY OF CHANGE	CHANGED BY
1.0	2013-12-23	Nov 2013 version adopted from the cGTA PSWG	Mark Carter
1.1	2014-08-21	Update based on feedback from CSC Members. Simplified scope section; revised section 2.7 to provide more clarity on information removal; aligned enforcement conditions with CPC policy, adjusted language in appendix B to align definitions of restricted and confidential.	Mark Carter
1.2	2014-09-09	Revised 2.7 to remove term “for repair” as it was not applicable. Policy approved at the CSC meeting September 9th 2014	Mark Carter
1.3	2015-01-21	Aligned name of access control policy based on final wave 3 CSC decision.	Mark Carter
1.4	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.	Mark Carter
1.5	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
1.6	March 16, 2018	Update standard to include Patient access to the EHR.	Geovanny Diaz

Information and Asset Management

Purpose

To define the information security controls that are required to protect information and physical information technology ("assets").

Scope

This standard applies to:

- [the EHR Solution] Program and [the EHR Solution], including all Patient Portals/Applications.
- All HICs, their Agents and Electronic Service Providers who create, contribute, view or have access to [the EHR Solution].

This standard does not apply to:

- Any HIC, their Agents or their Electronic Service Providers who do not create, contribute, view or have access 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 Policy Governance Structure section within the Information Security Policy.

Double-wrapped: When an envelope or container is placed inside of another envelope or container, usually used for physical transport of paper materials and assets.

Electronic Service Provider: A person 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.

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.

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, etc.) that directly connects to [the EHR Solution] to provide clinical data.

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].

Dual control: A control procedure whereby the active involvement of two people is required to complete a specified process.

Split Knowledge: A procedure whereby information is handled as multiple components from the time of generation until they are combined for use. Each component provides no knowledge of the ultimate message.

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.

Standard Requirements

1. Requirements for Health Information Custodians

1.1. HICs must ensure that all PHI that is transmitted to [the EHR Solution] Program Office or [the EHR Solution] is done in a secure manner, e.g., through the use of secure email, encryption, or virtual private network tunnel.

2. Requirements for [the EHR Solution]

2.1. [The EHR Solution] Program must implement and maintain an information and asset classification scheme for the confidentiality, availability and integrity of all information and assets it owns or manages. See *Appendix A: [the EHR Solution] Information and Asset Handling Classification Scheme*.

Labeling

2.2. [The EHR Solution] Program must label information and assets in accordance with the labeling requirements listed below:

Media Type	Public	Internal	Confidential	PHI	Restricted
Paper material	Optional		Must be labeled on the first page, and each subsequent page.		
Electronic Information	Optional		Must be labeled on the first page, and each subsequent page of any electronic information capable of being printed (e.g., screen capture, PDF, word processing document, spreadsheet, slide show presentation).		
Email	Optional		Must be labeled in the body or subject.		
Portable removable media	Optional				
Integrated Storage Device	Optional				

2.3. Although not required, [the EHR Solution] Program may label information and assets according to their integrity and availability classification.

General Protection requirements

2.4. [The EHR Solution] Program must ensure that all PHI and all assets that process or store PHI are protected, at a minimum, in accordance with Appendix B: Information and Asset Handling Protection Requirements. [The EHR Solution] Program may choose to implement additional controls than those required in *Appendix B*.

2.5. When information is combined or aggregated with information of a lower classification, [the EHR Solution] Program must ensure that the highest classification level contained therein shall determine, at a minimum, the overall classification of all the information.

2.6. [The EHR Solution] Program must ensure that all copies of paper material classified as Restricted must be individually numbered at time of creation and a master list associating each numbered copy with the individual that it was distributed to is maintained.

2.7. [The EHR Solution] Program must remove all information (PHI and [the EHR Solution] information) classified as Internal or higher from integrated storage devices and removable media prior to being sent externally. The removal of information classified as Confidential or higher must be done in a manner such that the information cannot be recovered and viewed.

2.8. [The EHR Solution] Program must log the destruction of the PHI in [the EHR Solution] CDR, as soon as possible but no longer than 5 days after the destruction. At a minimum the log must include:

2.8.1. Date that the PHI was destroyed.

2.8.2. Description of the scope of PHI that was destroyed.

2.8.3. Description of how the PHI was destroyed.

2.8.4. Identity of the person who destroyed the PHI.

2.8.5. Identity of the person who authorized destruction of the PHI.

Exemptions Any exemptions to this Standard 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 the Agreements with the HIC, Electronic Service Provider or termination of the access privileges of agents, and to require the implementation of remedial actions.

References

Legislative

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

International Standards

- ISO/IEC 27001:2005, Information Technology – Security Techniques – Information Security Management Systems – Requirements.

- ISO/IEC 27002:2005, Information Technology – Security Techniques – Code of Practice for Information Security Management
- ISO/IEC 27005: 2008 Information Technology – Security Techniques – Information Security Risk Management
- ISO 27799:2008(E), Health Informatics – Information security management in health using ISO/IEC 27002

eHealth Ontario EHR Policy and Standard Documents

- Information Security Policy
- Acceptable Use of Information and Information Technology
- Access Control and Identity Management Standard for System Level Access
- Local Registration Authority Procedures
- 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
- Harmonized Privacy Protection Policies

Canada Health Infoway Reference

- Canada Health Infoway Electronic Health Record Privacy and Security Requirements (Version 1.1 Revised February 7, 2005)

Other

- Information and Privacy Commissioner of Ontario's Guidelines on Facsimile Transmission Security (January 2003)

Appendix A: [The EHR Solution] Information and Asset Classification Scheme

Classes		Description	Examples of Information or Assets	Examples of Risk Impacts
Confidentiality	**Integrity and Availability**			
Public	**LOW**	Information or assets that are used in the normal course of business and that are unlikely to cause harm. **Available to the public.**	• Information found on the external [the EHR Solution] website • External job postings	• No impact if made publically available • If lost would not result in injury to patients, [the EHR Solution] or its agents or Electronic Service Providers, or HICs, their agents or Electronics Service Providers • Loss of integrity or availability does not have adverse impact on patients, [the EHR Solution], its agents or Electronic Service Providers, or HICs, their agents or Electronic Service Providers
Internal		Information or assets that have a low sensitivity outside of [the EHR Solution] and could have low levels of impact on service levels or performance, or result in low levels of financial loss. **Available to all agents of [the EHR Solution], and Electronic Service Providers of [the EHR Solution] and HICs with a need to know.**	• User manuals for [the EHR Solution] applications • High-level [the EHR Solution] planning documents • High-level financial information concerning the effective operation of [the EHR Solution]	• Low degree of risk if made publically available. • Loss of integrity or availability may have minimal adverse impact on patients, [the EHR Solution], its agents or Electronic Service Providers, or HICs, their agents or Electronic Service Providers

Confidential	**MEDIUM**	Information or assets that have a moderate to high sensitivity within [the EHR Solution] and outside of [the EHR Solution], and could have a moderate impact to service levels or performance, or result in moderate levels of financial loss. **Available only to a specific function, group or role in [the EHR Solution], its agents or Electronic Service Providers or HICs, their agents or Electronic Service Providers.**	• Personal information (not including PHI), e.g., an identifiable agent's rate of pay • Information covered by non-disclosure agreements • Financial transactions that do not include PHI or Restricted information • Detailed network architecture documents	• Loss of reputation • Loss of confidence in [the EHR Solution] • Loss of personal privacy • Loss of trade secrets or intellectual property • Loss of integrity or availability may have moderate adverse impact on patients, [the EHR Solution], its agents or Electronic Service Providers, or HICs, their agents or Electronic Service Providers
PHI	**HIGH**	All PHI. **Available only to a specific function, group or role in [the EHR Solution], its agents or Electronic Service Providers or HICs, their agents or Electronic Service Providers.**	• PHI	• Loss of reputation • Loss of personal health information privacy • Loss of confidence in [the EHR Solution] • Loss of integrity or availability may have moderate to serious adverse impact on a patient, [the EHR Solution], its agents or Electronic Service Providers, or HICs, their agents or Electronic Service Providers
Restricted	**CRITICAL**	Information or assets that are extremely sensitive both inside and outside of [the EHR Solution], and could have high impact to service levels or performance, or result in high levels of financial loss. **Available only to named individuals or specified positions. (e.g., John Doe or Vice President of Operations), in [the EHR Solution], its agents or Electronic Service Providers or HICs, their agents or Electronic Service Providers.**	• Cryptographic Keys • Passwords • Hardware Security Modules	• Loss of reputation • Significant financial impact • Loss of significant amounts of personal health information privacy • Loss of confidence in [the EHR Solution] • Destruction of partnerships and relationships • Loss of integrity or availability may have a serious to extreme adverse impact on patients, [the EHR Solution], its agents or Electronic Service Providers, or HICs, their agents or Electronic Service Providers

Appendix B: Information and Asset Handling Protection Requirements

Storage Requirements

Information/ Asset Type	Public	Internal	Confidential	PHI	Restricted
Paper material	No special confidentiality, integrity, or availability requirements.	Locked in storage container left unsupervised in areas with access to the public. - OR - Stored in an area that can only be accessed by [the EHR Solution], its agents or Electronic Service Providers.	Locked in storage container if left unsupervised in areas with access to the public or unauthorized persons. - OR – Stored in an access controlled area in which all with access are authorized to view the information.	Locked in storage container if left unsupervised in areas with access to the public or unauthorized persons. - OR- Stored in an access controlled area in which all with access are authorize to view the information.	Must be held under dual control and split knowledge. Audit trail kept for all physical access (e.g., log of signatures maintained each time a person accesses the information). Must be stored in an access controlled area AND locked in storage container.
Electronic Information	No special confidentiality, integrity, or availability requirements.	Must be stored on an internal network or storage device.	Must be stored on an encrypted device - OR – Stored on internal network storage that has logical controls to prevent unauthorized access.	Must be stored on an encrypted device and only the minimum amount of PHI required must be stored. - OR - Stored on an encrypted internal network storage that has logical controls, and where applicable physical controls, to prevent unauthorized access.	Must be stored on an encrypted device and only the minimum amount of Restricted information must be stored. - OR - Stored on an encrypted internal network storage that has logical controls, and where applicable physical controls, to prevent unauthorized access.
Portable removable media	No special confidentiality, integrity, or availability requirements.	Must be stored in an access controlled area.	Must be encrypted. Must be locked in storage container or access controlled area when not in use or unsupervised.	Must be encrypted. Must be locked in storage container or access controlled area when not in use or unsupervised.	Must be encrypted. Must be stored in an access controlled area AND locked in storage container, when not in use or unsupervised. • Should be held under dual control Audit trail should be maintained for all physical access to device.

Information/ Asset Type	Public	Internal	Confidential	PHI	Restricted
Integrated Storage Device	Should be stored in an access controlled area. Regular back-ups should be performed to ensure availability and integrity	Must be stored in an access controlled area. Regular back-ups should be performed to ensure availability and integrity.	Should be encrypted. Must be stored in an access controlled area. Regular back-ups must be performed to ensure availability and integrity.	Must be encrypted. Must be stored in an access controlled area. Regular back-ups must be performed to ensure availability and integrity.	Must be encrypted. Must be stored in a highly-secured access controlled area. Must maintain audit trail for physical access to device. Regular back-ups must be performed to ensure availability and integrity.

Transmission/Transport Requirements

Information/ Asset Type	Public	Internal	Confidential	PHI	Restricted
Paper material *(Refers to physical transport of paper material)*	No special requirements.		Internally (same physical location) • Must be placed in a sealed opaque envelope or container that is labeled with its classification Internally (different physical location) • Must be placed in a sealed opaque envelope or container that is labeled with its classification • Must be double-wrapped in a sealed opaque envelope or container. The outer envelope must NOT be labeled with its classification • Must require the recipient's signature		Internally (same physical location) • Must be placed in a sealed opaque tamper evident envelope or container that is labeled with its classification Internally (different physical location) and Externally • Must be placed in a sealed opaque tamper evident envelope or container that is labeled with its classification • Must be double-wrapped in a sealed opaque tamper-evident envelop. The outer envelope must NOT be labeled with its classification. • Must require the recipient's signature • If mailed, must be sent by a secure courier • If transported by agents or Electronic Service Providers of [the EHR Solution] or HICs, their agents or External Service Providers, it must remain under dual custody
Electronic Information *(Refers to electronic transmission of information)*			Must be sent through a secure channel.		
Portable removable media *(Refers to physical transport of the device)*			Internally (same physical location) • Must be placed in a sealed opaque envelope or container that is labeled with its classification Internally (different physical location) and Externally • Must be placed in a sealed opaque envelope or container that is labeled with its classification • Must be double-wrapped in a sealed opaque envelope or container. The outer envelope or container must NOT be labeled with its classification • Must require the recipient's signature		Internally (same physical location) • Must be placed in a sealed opaque tamper evident envelope or container that is labeled with its classification Internally (different physical location) and Externally • Must be placed in a sealed opaque tamper evident envelope or container that is labeled with its classification • Must be double-wrapped in a sealed tamper evident envelope or container. The outer envelope or container must NOT be labeled with its classification • Must require the recipient's signature • If mailed, must be sent by a secure courier • If transported by agents or External Service Providers of [the EHR Solution], or HICs, their agents or Electronic Service Providers, it must remain under dual custody
Integrated Storage Device *(Refers to physical transport of the device)*					

Decommissioning/Disposal/Destruction Requirements

Information/ Asset Type	Public	Internal	Confidential	PHI	Restricted
Paper material	No special requirements.	Shredded using a cross cut shredder or placed in a secure disposal bin to be shredded using a cross-cut shredder or incinerated by a designated agent or an Electronic Service Provider.	Shredded using a cross cut shredder or placed in a secure disposal bin to be shredded using a cross-cut shredder or incinerated by a designated agent or an Electronic Service Provider.	Shredded using a cross cut shredder or placed in a secure disposal bin to be shredded using a cross-cut shredder or incinerated by a designated agent or an Electronic Service Provider.	Must be incinerated on site under dual control - OR – Must be shredded using cross-cut shredder AND then placed in a designated secure disposal bin to be shredded using a cross-cut shredder or incinerated by a designated agent (or group of agents) or an external service provider.
Electronic Information	No special requirements.	Erase/delete information.	Erase/delete information stored on the encrypted device or the internal storage network. For CDs and DVDs, these may be shredded using a cross cut shredder or placed in a secure disposal bin to be shredded using a cross-cut shredder or incinerated by a designated agent or an Electronic Service Provider.	Erase/delete the information stored on the encrypted device or the encrypted internal network storage. For CDs and DVDs, these may be shredded using a cross cut shredder or placed in a secure disposal bin to be shredded using a cross-cut shredder or incinerated by a designated agent or an Electronic Service Provider.	Must be securely wiped or overwritten in a way that renders the information unrecoverable.
Portable removable media **Integrated Storage Device**	No special requirements.	Erase/delete all files.	Must be securely wiped or overwritten in a way that renders the information unrecoverable, or Must be physically destroyed in a way that renders the information unrecoverable	Must be securely wiped or overwritten in a way that renders the information unrecoverable, or Must be physically destroyed in a way that renders the information unrecoverable Destruction of PHI in the CDR must be logged (see 2.8).	<u>For devices containing cryptographic keys:</u> • Must be physically destroyed in a way that renders the information unrecoverable <u>For all other devices:</u> • Must either be securely wiped or overwritten in a way that renders the information unrecoverable, or physically destroyed in a way that renders the information unrecoverable