eHealth Ontario
It's working for you

Physical Security Standard

Version: 1.6

Document ID: 3545

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	2014-11-05
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	2014-10-09	Revised based on feedback from the cGTA, cSWO and eHealth Privacy group. Aligned scope, exemption and enforcement section with CPC policies. Provided a definition for data contribution end points and identity provider services. Modified HIC power failure and facility requirements in 1.5 to should from must. Clarified requirements by adding identity provider services and data contribution end points throughout many clauses throughout the HIC requirements section.	Mark Carter
1.2	2014-11-05	Policy approved at the November 5th CSC meeting.	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 exception decision process.	Mark Carter
1.5	2017-03-20	Updated Standard to align with ITSM. The document title was changed from Policy to Standard. EHR Solution definition was updated. Revised controls based on feedback.	Raviteja Addepalli
1.6	March 16, 2018	Updated standard to include Patient access to the EHR.	Geovanny Diaz

Physical Security Standard

Purpose

To define the requirements for the physical security of [the EHR Solution], and HIC's identity provider services and data contribution endpoints.

Scope

This standard applies to [the EHR Solution] and the [the EHR Solution] Program, including all Patient Portals/Applications.

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

- **Local identity provider technology** (local IdP), this standard applies to:
    - The HIC's local access control and identity management infrastructure ("identity provider services") that manages the authentication and authorization used to provision 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)
- **eHealth Ontario's ONE ID service** , this standard 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 standard also applies to:

- The data contribution endpoints that provide PHI to [the EHR Solution]'s Clinical Data Repository; and
- The information technology and processes that ensure the quality of the data submitted (e.g. terminology mapping).

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.

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.

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

Information technology: Any equipment or 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].

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 implement physical security perimeters to protect identity provider services and data contribution endpoints from unauthorized physical access and environmental damage.

1.2. HICs should ensure that highly sensitive facilities (i.e., buildings or storage areas that house identity provider services and data contribution endpoints) are protected against unauthorized physical access. Methods for preventing physical access may include:

1.2.1. Fitting vulnerable doors and windows with locks or bolts.

1.2.2. Installing and monitoring closed-circuit television (CCTV).

1.2.3. Employing security guards.

1.2.4. Installing intruder detection systems on external doors and testing accessible windows regularly.

1.3. HICs must ensure that highly sensitive facilities that house identity provider services and data contribution endpoints are not accessible to the public. Details about highly sensitive facilities should be kept confidential (e.g., by using discrete signs or excluding details from directories or telephone books).

1.4. HICs should ensure that visitors to highly sensitive facilitates are:

1.4.1. Permitted physical access only for specific, authorized purposes.

1.4.2. Monitored by recording arrival and departure times.

1.4.3. Obliged to wear visitor badges at all times.

1.4.4. Supervised at all times.

1.4.5. Made aware of behaviour or actions that are prohibited (e.g., filming or photography).

Utilities and Environmental

1.5. HICs should ensure that data contribution endpoints and identity provider services are protected from power failures and other disruptions caused by failures in supporting utilities (e.g., electricity, water supply, heating/ventilation, and air-condition).

1.6. HICs should ensure that power cables to highly sensitive facilities hosting the data contribution endpoints and identity provider services are protected. Methods of protection may include:

1.6.1. Segregating them from communications cables to prevent interference.

1.6.2. Concealed installation.

1.6.3. Locked inspection/termination points.

1.6.4. Alternative feeds or routing.

1.6.5. Avoidance of routes through public areas.

1.7. HICs must ensure that the power supply for data contribution endpoints and identity provider services are protected and meet vendor requirements. Methods of protection may include:

1.7.1. Using uninterruptible power supply (UPS) devices that have enough battery capacity to support an orderly shutdown.

1.7.2. Installing surge protection equipment.

1.7.3. Providing back-up electricity generators in the event of an extended power supply.

1.7.4. Installing emergency lighting in case of main power failure.

1.7.5. Locating emergency power-off switches near emergency exits to facilitate rapid power-down in case of an emergency.

1.7.6. Meeting the vendor-specified requirements for cooling, heating, humidity and air quality.

Telecommunications Cabling

1.8. Telecommunications cabling used to transmit information that supports data contribution endpoints and identity provider services must be protected from interception or damage. Methods of protection may include:

1.8.1. Installation of armoured conduit, and locked rooms or boxes at inspection and termination points.

1.8.2. Use of alternative routings and/or transmission media.

1.8.3. Use of fibre optic cabling.

1.8.4. Use of electromagnetic shielding to protect the cables.

1.8.5. Placement of redundant links.

1.8.6. Initiation of technical sweeps and physical inspections for unauthorized devices being attached to the cables.

1.8.7. Controlled access to patch panels and cable rooms.

Hazard Protection

1.9. HICs should ensure that highly sensitive facilities hosting data contribution endpoints and identity provider services are protected from natural and man-made hazards (e.g. in an area with a low risk of flooding, fire, explosion, or damage from neighbouring activities).

1.10. HICs should minimize the impact of hazards in highly sensitive facilities hosting data contribution endpoints and identity provider services by:

1.10.1. Locating fire extinguishers so that minor incidents can be tackled without delay.

1.10.2. Training agents, and where appropriate Electronic Service Providers, in the use of fire extinguishers, other emergency/safety equipment, and in emergency evacuation procedures.

1.10.3. Monitoring and controlling the temperature and humidity.

1.11. HICs should ensure that fire alarms in highly sensitive facilities hosting data contribution endpoints and identity provider services are monitored continuously, tested regularly and serviced in accordance with manufacturer specifications.

Data Centres

1.12. HICs should ensure that existing data centre facilities and those being acquired by lease, purchase, or construction hosting data contribution endpoints and identity provider services are periodically assessed to ensure that physical security controls are in place to physically protect the information stored or processed in that data centre.

1.13. HICs should layer physical security zones in data centres hosting data contribution endpoints and identity provider services to provide for defence in depth protection.

1.14. HICs must ensure that physical access points in data centres hosting data contribution endpoints and identity provider services, such as delivery and loading areas and other points where unauthorized persons may enter the premises are controlled and, if possible, isolated from areas that house highly sensitive information systems to avoid unauthorized physical access.

1.15. HICs should require their agents and Electronic Service Providers to obtain approval before leaving the data centre premises with technology used to operate identity provider services and data contribution endpoints.

2. Requirements for [the EHR Solution]

2.1. [The EHR Solution] Program must implement physical security perimeters to protect physical components of [the EHR Solution] from unauthorized physical access and environmental damage.

2.2. [The EHR Solution] Program must ensure that the strength of each perimeter depends on the physical security requirements of the information and information technology within the perimeter and, if applicable, the results of a threat risk assessment.

2.3. [The EHR Solution] Program must ensure that highly sensitive facilities (i.e., buildings or storage areas that house information systems that store or process PHI or Restricted information) are protected against unauthorized physical access. Methods for preventing physical access may include:

2.3.1. Fitting vulnerable doors and windows with locks or bolts.

2.3.2. Installing and monitoring closed-circuit television (CCTV).

2.3.3. Employing security guards.

2.3.4. Installing intruder detection systems on external doors and testing accessible windows regularly.

2.4. [The EHR Solution] Program must ensure that highly sensitive facilities are located away from areas that are easily accessible to the public. Details about highly sensitive facilities should be kept confidential (e.g., by using discrete signs or excluding details from directories or telephone books).

2.5. [The EHR Solution] Program should ensure that visitors to highly sensitive facilitates are:

2.5.1. Permitted physical access only for specific, authorized purposes.

2.5.2. Monitored by recording arrival and departure times.

2.5.3. Obliged to wear visitor badges at all times.

2.5.4. Supervised at all times.

2.5.5. Made aware of behaviour or actions that are prohibited (e.g., filming or photography).

Utilities and Environmental

2.6. [The EHR Solution] Program must ensure that highly sensitive information systems (e.g., information systems that store or process PHI or Restricted information) are protected from power failures and other disruptions caused by failures in supporting utilities (e.g., electricity, water supply, heating/ventilation, and air-condition).

2.7. [The EHR Solution] Program must ensure that power cables to highly sensitive facilities are protected. Methods of protection may include:

2.7.1. Segregating them from communications cables to prevent interference.

2.7.2. Concealed installation.

2.7.3. Locked inspection/termination points.

2.7.4. Alternative feeds or routing.

2.7.5. Avoidance of routes through public areas.

2.8. [The EHR Solution] Program must ensure that the power supply to highly sensitive facilities is protected. Methods of protection may include:

2.8.1. Using uninterruptible power supply (UPS) devices that have enough battery capacity to support the orderly shutdown of sensitive information systems.

2.8.2. Installing surge protection equipment.

2.8.3. Providing back-up electricity generators in the event of an extended power supply.

2.8.4. Installing emergency lighting in case of main power failure.

2.8.5. Locating emergency power-off switches near emergency exits to facilitate rapid power-down in case of an emergency.

2.8.6. Meeting the vendor-specified requirements for cooling, heating, humidity and air quality.

Telecommunications Cabling

2.9. [The EHR Solution] Program must ensure that telecommunications cabling that transmits information that supports [the EHR Solution] are protected from interception or damage. Methods of protection may include:

2.9.1. Installation of armoured conduit and locked rooms or boxes at inspection and termination points.

2.9.2. Use of alternative routings and/or transmission media.

2.9.3. Use of fibre optic cabling.

2.9.4. Use of electromagnetic shielding to protect the cables.

2.9.5. Placement of redundant links.

2.9.6. Initiation of technical sweeps and physical inspections for unauthorized devices being attached to the cables.

2.9.7. Controlled access to patch panels and cable rooms.

2.10. [The EHR Solution] Program should ensure that telecommunications equipment is connected to the utility provider by at least two diverse routes to prevent connection failures.

Hazard Protection

2.11. [The EHR Solution] Program must ensure that highly sensitive facilities are protected from natural and man-made hazards (e.g. in an area with a low risk of flooding, fire, explosion, or damage from neighbouring activities).

2.12. [The EHR Solution] Program must minimize the impact of hazards in highly sensitive facilities by:

2.12.1. Locating fire extinguishers so that minor incidents can be tackled without delay.

2.12.2. Training agents, and where appropriate Electronic Service Providers, in the use of fire extinguishers, other emergency/safety equipment, and in emergency evacuation procedures.

2.12.3. Monitoring and controlling the temperature and humidity.

2.13. [The EHR Solution] Program must ensure that fire alarms in highly sensitive facilities are monitored continuously, tested regularly and serviced in accordance with manufacturer specifications.

Data Centres

2.14. [The EHR Solution] Program must ensure that existing data centre facilities, and those being acquired by lease, purchase, or construction, are periodically assessed to ensure that physical security controls are in place to physically protect the information stored or processed in that data centre.

2.15. [The EHR Solution] Program data centres facilities must be separated into distinct areas depending on operational requirements (e.g., server rooms, wiring closets, call centres, system support areas, service delivery, receiving, etc.).

Each area must be assigned a physical security zone to determine the physical security controls. Physical security zones with the corresponding minimum physical security controls for [the EHR Solution] are found in *Appendix A: [the EHR Solution] Physical Security Zones*.

2.16. [The EHR Solution] Program must layer physical security zones in data centres to provide for defence in depth protection.

If such an approach is not feasible (e.g., due to the physical layout of a particular environment or specific operational requirements), then the maximum number of zones that may be skipped in the design of a data centre environment must be limited to one. In such cases, the relevant threat risk assessment must reflect the skipped zone, and compensating controls must be investigated and implemented.

2.17. [The EHR Solution] Program must ensure that physical access points in data centres, such as delivery and loading areas and other points where unauthorized persons may enter the premises must be controlled and, if possible, isolated from areas that house highly sensitive information systems to avoid unauthorized physical access.

2.18. [The EHR Solution] Program must require all agents and Electronic Service Providers to obtain approval from a senior-level executive in [the EHR Solution] Program before leaving the data centre premises with information technology that is necessary for the operation of their information systems (e.g., servers and network devices). A record of all assets removed off-site should be maintained.

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 Providers 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 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)

Appendix A: [The EHR Solution] Physical Security Zones

Zones	Description	Requirements
Public Zone	Any public entrance to a physical facility and the immediate environment around it is considered a public zone. Public zone examples include: • Facility parking lots • Grounds surrounding a facility • Any area of unimpeded public access during posted business hours.	No special requirements for public zones, as it is not always possible to manage these environments directly.
Reception Zone	A reception zone is an area where public access intersects with facility staff or operations for administrative reasons or to obtain access. Reception zone examples include: • Main entrance of a facility or a floor in shared accommodation situations; • Visitor receiving and waiting areas; and • Public service desks and kiosks.	• Physical access control must be in place to restrict further public movement (e.g., through the use of a reception desk, guards, or physical access devices, such as card readers). • Where possible, public/visitor access to the reception zone should be limited to specific hours (e.g., it may be limited in a data centre, but not in a hospital). • Any required authentication and approval for facility access (e.g., presentation of credentials or validation of authorized access) should take place within the reception zone.
Operations Zone	An operations zone is a periodically or informally monitored area within the facility where access is limited to authorized personnel and approved/escorted visitors only. Operation zone examples include: • Storage closets • Employee offices and similar areas	• Must have a recognizable perimeter. • Must not permit public access, and employ physical barriers (e.g., walls, locked doors etc.) for this purpose. • Must only be accessible via a reception zone, and separated from the reception zone by a wall and locking door (unless subject to an exemption as per requirement 2.17 of this document).

Zones	Description	Requirements
Security Zone	A security zone is an area within the facility that is monitored continuously, and is accessible to authorized personnel and approved/escorted visitors only. The secure raised floor portion of a data centre is appropriate for inclusion within a security zone. Other areas of a facility (e.g., sensitive wiring closets) may also be defined as security zones.	• Must have a recognizable perimeter and employ robust, reliable high-effectiveness physical barriers to access; • Must be constructed such that all barriers and doors remain continuously closed and locked when not in use; • Must employ activity monitoring with immediate response; • Access must be controlled and recorded at all times, e.g., through the use of a guard to gain entry or through the use of a card-reader that records access; and • Must be located within an operations zone (unless subject to an exemption as per requirement 2.17 of this document).
High Security Zone	A high security zone is an area within the facility that is monitored continuously, and is accessible only to a specific list of screened and authorized personnel, or approved/escorted visitors accompanied by screened and authorized personnel. A dedicated, sensitive processing environment that must be physically separated from raised floor operations is appropriate for inclusion within a high security zone.	• Must have a recognizable perimeter and employ robust, reliable high-effectiveness physical barriers to access. • Must be constructed such that all barriers and doors remain continuously closed and locked when not in use. • Must employ continuous activity monitoring with immediate response. • All access must be controlled and recorded at all times, and must be audited, at a minimum, monthly. • Persons who require access must successfully undergo screening and be added to a list or roster of authorized persons prior to being granted access. • All approved visitors must be accompanied at all times by a screened and authorized individual. • Must be located within a security zone (unless subject to an exemption as per requirement 2.17 of this document).