eHealth Ontario
It's working for you

Networking and Operations Standard

Version: 1.8

Document ID: 3544

Ontario
eHealth Ontario

Copyright Notice

Copyright © 2018, 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.

Document Control

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

Approval History

APPROVER(S)	APPROVED DATE
Connecting Security Committee	2017-03-20
Connecting Security Committee	2018-03-26

Revision History

VERSION NO.	DATE	SUMMARY OF CHANGE	CHANGED BY
1.0	2013-11-18	Nov 2013 version adopted from the cGTA PSWG	Mark Carter
1.1	2014-05-16	Updated content to align with cGTA May 13th PSWG meeting. Updates include patch management, configuration scanning and vulnerability management topics.	Mark Carter
1.2	2014-10-09	Updates based on feedback from cGTA, cSWO and eHealth Privacy. Revised language in the scope, enforcement and exemption sections to align with CPC polices. Provided a definition for data contribution and identity provider services. Updates to fail secure exemptions, references to CIS and vendor guidelines for system hardening, revised option to run multiple system functions on the same server if the security level is similar, provided alternates to AV and scanning frequency, provided options where patches could not be tested, revised gateway reviews to 12 months from 6, softened linkage of VA and Pen Test results into TRAs, clarified approval of VA scan tools, revised backup frequency based on RTO and RPO, revised full system restore testing requirements, created pointer to CPC retention policy.	Mark Carter
1.3	2014-10-16	Revision based on the Oct 15th CSC Meeting. 1.20 was created to address AV requirements on HIC approved tools. Revised 2.13 “external” to “data contribution endpoint and identity provider service and other assets” when discussing authentication of remote assets to the EHR. Broadened encryption implementations in 2.25.	Mark Carter
1.4	2014-11-26	Revised language in the hardening requirements 1.7 – 1.10 to allow flexibility based on Nov 5th discussion with CSC Members. Section 1.26 was modified to allow for vulnerability and configuration scans to occur every 6 months. Policy was approved at the CSC meeting.	Mark Carter

VERSION NO.	DATE	SUMMARY OF CHANGE	CHANGED BY
1.5	2015-01-21	Aligned name of access control policy based on final wave 3 CSC decision.	Mark Carter
1.6	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
1.7	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
1.8	March 16, 2018	Updated standard to include Patient access to the EHR.	Geovanny Diaz

Networking and Operations

Purpose

To define requirements for implementing and maintaining secure networks and information systems that comprise [the EHR Solution], as well as the networks and information systems of health information custodians (HIC) who view PHI via [the EHR Solution] or contribute PHI to [the EHR Solution].

Scope

This standard applies to [the EHR Solution] Program and [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 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 (e.g., firewalls, proxies, etc.); and
    - 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 (e.g., 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 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 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.

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.

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.

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.

Configuration Scan: An automated process of comparing the configuration of an information system against a configuration standard which includes specific security settings. Configuration scans, by their nature, must be credentialed.

Standard Requirements

1. Requirements for Health Information Custodians

1.1. HICs must maintain an inventory of assets related to their identity provider services and data contribution endpoints.

1.2. HICs should document and maintain network diagrams of all direct connections to their identity provider services and data contribution endpoints. Network diagrams may include:

1.2.1. Physical and logical topologies.

1.2.2. Network device configuration.

1.2.3. Gateways to external networks.

1.2.4. Connected network devices.

Network Zones

1.3. HICs should implement network zones and manage these network zones in a manner that observes the separation of different computing environments. The segregation of networks may be based on criteria, such as:

1.3.1. The classification of information transmitted on the network.

1.3.2. The level of assurance required.

1.4. HICs should control traffic between networks zones by using a security gateway at the zones' perimeter.

Security Gateways

1.5. HICs should configure their security gateways to filter traffic to or from network zones that contain their identity provider services and data contribution endpoints by denying all network traffic (inbound or outbound) by default and fail secure where availability requirements permit.

1.6. HICs should implement a process to review security gateway configurations at least annually. The process should ensure the:

1.6.1. Review of the rule sets on their security gateways.

1.6.2. Removal of expired or unnecessary rules.

1.6.3. Resolution of conflicting rules.

1.6.4. Removal of unused or duplicate objects, e.g., network or computer systems.

Network Connectivity

1.7. Where possible, HICs must disable unnecessary services, protocols, and ports on their identity provider services and data contribution endpoints. This must be in place when new systems and major upgrades to legacy systems are implemented. Alternate configurations are acceptable where perimeter systems implement access control lists or firewall rules to limit access to services on legacy systems that are sensitive to upgrades. HICs should document and maintain justification for the use of all services, protocols, and ports allowed, including security features implemented for services, protocols, and ports considered to be insecure (e.g., FTP, Telnet, POP3, IMAP, and SNMP). HICs should reference Vendor specifications and industry benchmarks such as the Center for Internet Security (CIS).

1.8. Where possible, HICs must implement network restrictions that secure participation in [the EHR Solution] data contribution endpoint services and identity provider services administrative functionality to explicitly authorized services or workstations. This must be in place when new systems and major upgrades to legacy systems are implemented.

System and Hardware Hardening

1.9. Where possible, HICs must harden all their identity provider services and data contribution endpoints prior to being implemented in the production environment. This must be in place when new systems and major upgrades to legacy systems are implemented. Alternate configurations are acceptable where perimeter systems implement access control lists or firewall rules to limit access to services on legacy systems that are sensitive to upgrades.

1.10. Where possible, HICs must remove unnecessary functionality (e.g., such as drivers, features, subsystems, file systems) on their identity provider services and data contribution endpoints. This must be in place when new systems and major upgrades to legacy systems are implemented. Alternate configurations are acceptable where perimeter systems implement access control lists or firewall rules to limit access to services on legacy systems that are sensitive to upgrades.

1.11. HICs should implement information security features for required services, protocols or daemons that are considered to be insecure (e.g., use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.) on their identity provider services and data contribution endpoints.

Servers

1.12. HICs should only implement one primary function per server to prevent functions that require different security levels from co-existing on the same server (e.g., web servers and database servers should be set-up on separate servers). Where functions share the same security level it may be acceptable to run more than one function per server. Where virtualization technologies are in use, only one primary function per virtual system component should be implemented.

Intrusion Detection and Prevention

1.13. HICs should implement intrusion detection and prevention mechanisms (e.g., host intrusion detection/prevention systems and network intrusion detection/prevention systems) on their identity provider services and data contribution endpoints.

1.14. HICs should protect their intrusion detection and prevention sensors (i.e., the hardware used to identify unauthorized activity in network traffic) against attack, for example, by using a network tap to hide the presence of the sensor.

1.15. HICs should update intrusion detection and prevention software within defined timescales and at the recommendation of the vendor (e.g., on discovery of a sever vulnerability).

1.16. HICs should configure their intrusion detection and prevention software to provide an alarm or alert when suspicious activity is detected or prevented.

1.17. HICs should configure thresholds for alarms and alerts to identify possible intrusion detection or prevention events or violations of their information security policies.

1.18. HICs should respond to information security incidents identified by intrusion detection and prevention mechanisms in accordance with their information security incident handling process.

Protection Against Malicious Code

1.19. HICs must implement malware detection and repair software or equivalent solution on their identity provider services and data contribution endpoints to protect from malicious code. Alternative solutions may include application whitelisting or utilization of thin client implementations which restrict writable capabilities. Questions regarding the appropriateness of alternative solution should be directed to the Security Lead for [the EHR Solution] which can be put forward to the Connecting Security Committee.

1.20. Malware detection and repair software or equivalent solution should be implemented on HIC approved tools, processes and workstations to protect from malicious code. Alternative solutions may include application whitelisting or utilization of thin client implementations which restrict writeable capabilities. Questions regarding the appropriateness of alternative solutions should be directed to the Security lead for [the EHR Solution] which can be put forward to the Connecting Security Committee.

1.21. HICs must keep their virus definition files for their identity provider services and data contribution endpoints up-to-date within one week.

1.22. HICs should keep their malware detection and repair software up-to-date.

1.23. HICs should automate virus definition updates and a verification capability should be in place to ensure that identity provider services and data contribution endpoints have been properly updated. Where updates to virus definition files are not automated, identity provider services and data contribution endpoints that have malware detection and repair software installed on them should be identified and updated manually.

1.24. HICs must program their malware detection and repair software on their identity provider services and data contribution endpoints to run at regular intervals.

Vulnerability Management

1.25. HICs should implement a vulnerability management process to address the following:

1.25.1. Scanning and monitoring.

1.25.2. Risk assessment.

1.25.3. Remediation.

1.26. HICs should perform vulnerability and configuration scans on their identity provider services and data contribution end points that interface with [the EHR Solution] every 6 months.

1.27. HICs should define timelines to react to the notification of potentially relevant vulnerabilities.

1.28. HICs must assess all risks posed by vulnerabilities they have identified on their identity provider services and data contribution endpoints.

Security Patch Management

1.29. If a patch is available, HICs must assess the risks associated with installing the patch (i.e. the risks posed by the vulnerability must be compared with the risk of installing the patch) on their identity provider services and data contribution endpoints.

1.30. Where possible, HICs must test and evaluate all patches prior to installation on their identity provider services and data contribution endpoints to ensure they are effective and do not result in side effects that the HIC cannot tolerate.

1.31. If a HIC decides not to apply a patch on their identity provider services and data contribution endpoints, the HIC must document the decision and should make the appropriate conforming changes to inventory records and disaster recovery plans.

1.32. If no patch is available or the decision is made not to patch their identity provider services and data contribution endpoints, HICs must consider implementing compensating controls to reduce the risks posed by the vulnerability. Controls may include:

1.32.1. Turning off services or capabilities related to the vulnerability.

1.32.2. Adapting or adding access controls (e.g., firewalls at the network border).

1.32.3. Increasing monitoring to detect or prevent actual attacks.

1.33. HICs should update their identity provider services and data contribution endpoints configurations or baseline security configuration standards as appropriate, to improve their effectiveness based on the results of vulnerability and configuration scans.

Change Control

1.34. HICs must ensure that all changes to their identity provider services and data contribution endpoints follow their defined change control procedures.

Backups

1.35. HICs should back up their relevant information systems.

1.36. HICs must secure all backups containing PHI. Encryption must be used when physically transferring data between sites.

1.37. HICs should ensure that backup media and relevant information systems are protected by physical and environmental controls equivalent with the physical and environmental controls applied at the main site.

1.38. HICs should regularly test backup media to ensure that they can be relied upon for emergency use when necessary. Whole system restores should be tested annually.

1.39. HICs should regularly test their restoration procedures to ensure that they are effective and that they can be completed within the time allotted in their operational procedures for recovery. Restoration procedures should be tested annually.

2. Requirements for [the EHR Solution]

2.1. [The EHR Solution] Program must maintain an inventory of all their physical information technologies that comprise [the EHR Solution]. The inventory of assets must include, but is not limited to:

2.1.1. Type of asset.

2.1.2. Information technology owner, where applicable.

2.1.3. Location of the information technology (and information technology owner, where applicable).

2.1.4. Backup information.

2.2. [The EHR Solution] Program must document and maintain network diagrams of all direct connections to [the EHR Solution]. Network diagrams should include, but are not limited to:

2.2.1. Physical and logical topologies.

2.2.2. Network device configuration.

2.2.3. Gateways to external networks.

2.2.4. Connected network devices.

2.3. [The EHR Solution] Program must document and maintain operating procedures for [the EHR Solution]. The operating procedures should specify the instructions for the detailed execution of jobs, such as performing backups, system restart and recovery procedures, and error handling.

2.4. [The EHR Solution] Program must restrict all access to system documentation and operating procedures based on the principles of least-privileged and need-to-know.

2.5. [The EHR Solution] Program should segregate duties and areas of responsibility for managing their network to reduce opportunities for unauthorized or unintentional access, collection, use, disclosure, transfer, modification or disposal.

Network Zones

2.6. [The EHR Solution] Program must implement network zones and manage these network zones in a manner that observes the separation of different computing environments. The segregation of networks should be based on criteria, such as:

2.6.1. The classification of information transmitted on the network.

2.6.2. The level of assurance required.

2.7. [The EHR Solution] Program must ensure that networks are segregated, logically or physically, between [the EHR Solution], HIC information systems, and public networks.

2.8. [The EHR Solution] Program must control traffic between networks zones by using a security gateway at its perimeter.

Security Gateways

2.9. [The EHR Solution] Program must configure their security gateways to filter traffic between network zones by denying all network traffic (inbound or outbound) by default and failing secure where availability requirements permit.

2.10. [The EHR Solution] Program should implement a process to review security gateway configurations at least annually. The process should ensure the:

2.10.1. Review of the rule sets on their security gateways.

2.10.2. Removal of expired or unnecessary rules.

2.10.3. Resolution of conflicting rules.

2.10.4. Removal of unused or duplicate objects, e.g., network or computer systems.

Network Connectivity

2.11. [The EHR Solution] Program must ensure that authentication and authorization processes are in place on [the EHR Solution] network before access to [the EHR Solution] is granted.

2.12. [The EHR Solution] Program must ensure that all connectivity to [the EHR Solution] is secured to ensure the confidentiality and integrity of PHI that is transmitted (e.g., through the use of Transport Layer Security (TLS), virtual private network (VPN) tunnels, terminal services, etc.).

2.13. [The EHR Solution] Program must require a [the EHR Solution]-approved identifier (e.g., digital certificate, MAC address, IP address) to be used to indicate whether an data contribution endpoint or identity provider service asset is permitted to connect to the network and which network zone the asset is permitted to connect. Considerations should be made for other assets connecting to [the EHR Solution].

2.14. [The EHR Solution] Program must disable all unnecessary services, protocols, and ports on their information systems. [The EHR Solution] Program should document and maintain justification for the use of all services, protocols, and ports allowed, including security features implemented for services, protocols, and ports considered to be insecure (e.g., FTP, Telnet, POP3, IMAP, and SNMP). [The EHR Solution] Program should reference Vendor specifications and industry benchmarks such as the Center for Internet Security (CIS).

2.15. [The EHR Solution] must terminate all direct inbound and outbound external connections in a semi-trusted network zone (e.g., a demilitarized zone (DMZ)).

2.16. [The EHR Solution] must ensure that all information system components that store information classified as Internal or higher are located in an internal network zone, segregated from the DMZ and other untrusted networks.

2.17. [The EHR Solution] must disable split tunnelling on any information system or information technology with access to [the EHR Solution], except for networking devices (e.g., routers, firewalls).

2.18. [The EHR Solution] should close a network connection once the established unsuccessful attempt threshold has been reached.

2.19. [The EHR Solution] should implement network routing controls based on positive source and destination address checking mechanisms.

System and Hardware Hardening

2.20. [The EHR Solution] must harden all their information systems prior to implementation into the production environment.

2.21. [The EHR Solution] must remove all unnecessary functionality (e.g., such as drivers, features, subsystems, file systems, and unnecessary web servers).

2.22. [The EHR Solution] must implement information security features for any required services, protocols or daemons that are considered to be insecure (e.g., use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.).

Servers

2.23. [The EHR Solution] should only implement one primary function per server to prevent functions that require different security levels from co-existing on the same server (e.g., web servers and database servers should be set-up on separate servers). Where functions share the same security level it may be acceptable to run more than one function per server. Where virtualization technologies are in use, only one primary function per virtual system component should be implemented.

Workstations

2.24. [The EHR Solution] Program must install personal firewall software on their agent's or Electronic Service Provider's workstation, laptop, and where technically feasible other mobile devices, with direct connectivity to the internet and [the EHR Solution].

2.25. [The EHR Solution] Program must ensure that mobile workstations (e.g., notebooks, laptops, etc.) that have a documented business requirement to work with data extracts containing PHI have full-disk or partial encryption securely installed. Full disk encryption is the preferred method; however, containerized implementations of encryption on directories or specific location are also acceptable. Implementations where PHI remains on managed servers in a protected data centre (i.e. Citrix) do not require encryption at rest.

Intrusion Detection and Prevention

2.26. [The EHR Solution] Program must implement intrusion detection and prevention mechanisms (e.g., host intrusion detection/prevention systems and network intrusion detection/prevention systems) on their information systems and networks.

2.27. [The EHR Solution] Program must protect their intrusion detection and prevention sensors (i.e., the hardware used to identity unauthorized activity in network traffic) against attack, for example, by using a network tap to hide the presence of the sensor.

2.28. [The EHR Solution] Program must update intrusion detection and prevention software within defined timescales and at the recommendation of the vendor (e.g., on discovery of a sever vulnerability).

2.29. [The EHR Solution] Program must configure their intrusion detection and prevention software to provide an alarm or alert when suspicious activity is detected or prevented.

2.30. [The EHR Solution] Program must configure thresholds for alarms and alerts to identify possible intrusion detection or prevention events, or violations of [the EHR Solution] information security policies and its associated procedures.

2.31. [The EHR Solution] Program must respond to information security incidents identified by intrusion detection and prevention mechanisms in accordance with their information security incident handling process.

Protection Against Malicious Code

2.32. [The EHR Solution] Program must implement malware detection and repair software or equivalent solution on all workstations (e.g., desktops, laptops, etc.) and servers. Alternative solutions may include application whitelisting or utilization of thin client implementations which restrict writable capabilities. Questions regarding the appropriateness of alternative solution should be directed to the Security Lead for [the EHR Solution] which can be put forward to the Connecting Security Committee.

2.33. [The EHR Solution] Program must ensure that virus definition files remain up-to-date within a week.

2.34. [The EHR Solution] Program must keep all their malware detection and repair software up-to-date.

2.35. [The EHR Solution] Program should automate virus definition file updates and a verification capability should be in place to ensure that workstations and servers have been properly updated. Where virus definition file updates are not automated, these workstations or servers must be identified and updated manually.

2.36. [The EHR Solution] Program must program their malware detection and repair software to run at regular intervals, at a minimum, weekly unless scanning is performed in real time. [The EHR Solution] Program must disconnect infected information systems and information technology from the network until it has been verified that they are malware-free.

2.37. [The EHR Solution] Program must implement malware detection and repair software to scan electronic or optical media, incoming files, electronic mail attachments, and downloads for malware before their use. These checks may be carried out at different places, such as electronic mail servers, and desktop computers.

Vulnerability Management

2.38. [The EHR Solution] Program must implement a vulnerability management process to address:

2.38.1. Scanning and monitoring.

2.38.2. Risk assessment.

2.38.3. Remediation.

2.39. [The EHR Solution] Program must monitor their information systems to identify new vulnerabilities.

2.40. [The EHR Solution] Program must perform vulnerability and configuration scans on [the EHR Solution] at a minimum, quarterly to determine the effectiveness of the implemented operational and technical security controls. [1]

2.41. [The EHR Solution] program must perform penetration tests, at a minimum, annually on all their internet-facing applications that provide access to PHI to ensure that these applications do not expose [the EHR Solution] to unknown threats.[2]

2.42. Penetration tests on internet-facing applications must include web-application testing techniques executed against a documented set of industry standards such as the OWASP Top 10, to identify weakness that are unique to web-based applications (such as SQL/LDAP injection, cross-site scripting, session token attacks and URL forgery), and must be subject to rigorous external content review.

2.43. Configuration scans should be executed to ensure compliance with the approved baseline security configuration standard.

2.44. Where possible, [the EHR Solution] program should incorporate findings from vulnerability and security configuration scans in threat risk assessments to provide an accurate risk overview of [the EHR Solution].

---

[1] See the Systems Development Lifecycle Policy for vulnerability scanning requirements for new deployment or releases of infrastructure or services.
[2] See the *Systems Development Lifecycle Policy* for penetration requirements for new deployments or releases of internet-facing applications.

2.45. [The EHR Solution] program must ensure that all risks posed by vulnerabilities are identified on their information systems and their remediation plans are assessed by a security analyst with independence to the operational teams.

2.46. [The EHR Solution] program must ensure that all vulnerabilities identified on their information systems are remediated within a defined timeline or must have the risk posed by the vulnerability formally accepted if the decision is made not to remediate.

2.47. [The EHR Solution] Program should maintain a list of vulnerability and configuration scanning tools which are approved by [the EHR Solution] Security Lead.

2.48. [The EHR Solution] Program must define timelines to react to the notification of potentially relevant vulnerabilities.

Security Patch Management

2.49. [The EHR Solution] Program must implement a security patch management process to ensure that available patches are identified, assessed and, where feasible, deployed. The security patch management process may be a part of a general patch management process.

2.50. If a patch is available, [the EHR Solution] Program must assess the risks associated with installing the patch (i.e. the risks posed by the vulnerability must be compared with the risk of installing the patch).

2.51. Where possible, [the EHR Solution] Program must test and evaluate all patches prior to installation to ensure they are effective and do not result in side effects that cannot be tolerated.

2.52. If the decision is made not to patch, then [the EHR Solution] Program must document the decision and make the appropriate conforming changes to inventory records and disaster recovery plans.

2.53. If no patch is available, or the decision is made not to patch, [the EHR Solution] Program must consider implementing compensating controls to reduce the risks posed by the vulnerability. Controls may include:

2.53.1. Turning off services or capabilities related to the vulnerability.

2.53.2. Adapting or adding access controls (e.g., firewalls at the network border).

2.53.3. Increasing monitoring to detect or prevent actual attacks.

2.54. [The EHR Solution] Program must review and update their information system configurations or baseline security configuration standards as appropriate, to improve their effectiveness based on the results of vulnerability scans and changing industry practices.

Change Control

2.55. [The EHR Solution] Program must ensure that all changes to networks and information systems follow their defined change control procedures.

Backups

2.56. [The EHR Solution] Program must back up [the EHR Solution] so that it may be recovered following a disaster or media failure.

2.57. At a minimum, [the EHR Solution] Program must ensure that [the EHR Solution] is backed up in accordance to established and approved recovery time objectives (RTO) and recovery point objectives (RPO).

2.58. [The EHR Solution] Program must ensure that backups are stored in a remote location, at a sufficient distance to escape any damage from a disaster at the main site.

2.59. [The EHR Solution] Program must secure all backups containing PHI. Encryption must be used when physically transferring data between sites.

2.60. [The EHR Solution] Program must ensure that backup media and information systems are protected by physical and environmental controls equivalent to the physical and environmental controls applied at the main site.

2.61. [The EHR Solution] Program must test backup media on a regular basis and backup failures need to be tracked, reported and remediated.

2.62. [The EHR Solution] Program must regularly test its restoration procedures to ensure that they are effective and that they can be completed within the time allotted in their operational procedures for recovery. At a minimum, restoration procedures must be tested, at a minimum, annually.

2.63. The retention period for data archives of [the EHR Solution] shall be determined by the record retention requirements of the information they contain, and in accordance to any legal or regulatory requirements and in accordance to the Connecting Privacy Committee Harmonized Retention and Destruction Policy.

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)