eHealth Ontario
It's working for you

System Development Lifecycle Standard

Version: 1.7

Document ID: 3546

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	2017-03-30
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 based on the cGTA edits presented May 13th. Updates include configuration and penetration testing topics.	Mark Carter
1.2	2014-10-09	Revised based on feedback from cGTA, cSWO and eHealth Privacy. Revised scope, exemption and enforcement sections to align with CPC policy. Included a definition of data contribution end point and IDP services. Enhanced scope to clearly cover ESPs and organizations that leverage the EHR Solution to integrate it with their own systems. Revised separation of prod and non-prod environments to consider sensitivity of data. Revised requirement for a VA and configuration scan on major releases.	Mark Carter
1.3	2014-11-05	Policy approved at the Nov 5 CSC meeting.	Mark Carter
1.4	2015-01-21	Aligned name of access control policy based on final wave 3 CSC decision.	Mark Carter
1.5	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
1.6	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
1.7	March 16, 2018	Updated standard to include Patient access to the EHR.	Geovanny Diaz

System Development Lifecycle Standard

Purpose

To define the information security controls that are required to securely develop and implement information systems.

Scope

This standard applies to [the EHR Solution] Program and [the EHR Solution] including all Patient Portals/Applications and development by Electronic Service Providers supporting [the EHR Solution].

This standard applies to organizations leveraging [the EHR Solution] to integrate data into their own solutions.

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
- 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 view, create, contribute 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 retention, collection, processing, maintenance, use, disclosure, or disposition of information.

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.

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 perform development and testing activities on their identity provider services and data contribution endpoints in non-production environments.

1.2. HICs should implement controls to segregate their production environments from their non-production environments. These controls may include:

1.2.1. Using separate access controls

1.2.2. Using separate hardware for production and non-production activities

1.2.3. Segmenting the production network from non-production networks (e.g., through the use of network gateways)

Requirements Analysis and Specification

1.3. HICs should perform an initial information security review on new or proposed upgrades or modifications to their identity provider services and data contribution endpoints.

1.4. HICs should document information security requirements of their identity provider services and data contribution endpoints so that they can be used as a basis for requirements of future releases of these systems.

Design

1.5. HICs should review design specifications and processes for new or proposed modifications to their identity provider services and data contribution endpoints to ensure that sufficient controls are place to address information security requirements.

Development

1.6. HICs should protect any source code related to their identity provider services and data contribution endpoints against unauthorized access and modification (e.g., through the use of access controls).

1.7. HICs should store all source code related to their identity provider services and data contribution endpoints in a source code repository and implement version control to manage code development.

1.8. HICs should require custom code related to their identity provider services and data contribution endpoints to be reviewed prior to release into production. Reviews of custom code ("code reviews") may be performed manually or with the assistance of automated review tools.

1.9. HICs should ensure that security deficiencies or vulnerabilities identified during the code review are corrected or the risk is accepted prior to production implementation.

Testing

1.10. HICs should ensure that procedures for testing identity provider services and data contribution endpoint developments cover the:

1.10.1. Types of hardware, software and services to be tested.

1.10.2. Use of structured test plans, including user involvement.

1.10.3. Types of testing (e.g., end-to-end and performance testing).

1.10.4. Data use for performing tests.

1.10.5. Document, review and sign-off of the testing results.

1.11. HICs should conduct tests on new identity provider services and data contribution endpoints with the system running in expected, unexpected (e.g. excessive load, or unavailable services), and infrequent (e.g. limited connectivity or delayed service responses) conditions.

Security Testing

1.12. HICs should perform vulnerability assessments on their identity provider services and data contribution endpoints to identify weaknesses in the information security controls and perform penetration tests to demonstrate how vulnerabilities can be exploited.

1.13. HICs should implement a process to ensure that flaws or security weaknesses identified during the testing process for their identity provider services and data contribution endpoints are resolved in a consistent manner.

Promotion and Installation

1.14. Before new identity provider services or data contribution endpoints are promoted into the production environment, HICs should ensure that:

1.14.1. Information security assessments have been performed.

1.14.2. Limitations of information security controls have been documented.

1.14.3. Service level agreements have been established to support systems in the production environment, if required.

1.15. HICs should define and implement an installation process or deployment plan.

1.16. HICs should create a rollback strategy prior to implementing changes.

1.17. HICs should only permit specific agents and Electronic Service Providers to update production operational software, applications, and program libraries.

Change Control

1.18. HICs should document and implement a change control process to govern all changes to production identity provider services and data contribution endpoints.

1.19. HICs should ensure that their change control process:

1.19.1. Maintains a record of agreed authorization levels.

1.19.2. Ensures changes are submitted by authorized users.

1.19.3. Reviews information security controls to ensure that they will not be compromised by the changes.

1.19.4. Identifies all software, information, database entries, and hardware that require amendment.

1.19.5. Obtains formal approval from information system owner for detailed proposals before work commences.

1.19.6. Ensures authorized users accept changes prior to implementation.

1.19.7. Ensures the information system documentation set (i.e., the document(s) relevant to the information system being changed) is updated on the completion of each change, and the old documentation is archived or disposed.

1.19.8. Maintains a version control for all software updates.

1.19.9. Maintains an audit trail of all change requests.

1.19.10. Ensures that all information included in the change control process (database names, accounts, network addresses, etc.) are disclosed only to the relevant parties in the appropriate steps of the change control procedure.

Post Implementation Review

1.20. HICs should develop a process to test the information security controls of their information systems after implementation. The process should ensure that:

1.20.1. A review of the application control and integrity procedures is completed to ensure that they have not been compromised by the operating system changes.

1.20.2. Appropriate changes are made to the business continuity plans.

2. Requirements for [the EHR Solution]

2.1. [The EHR Solution] Program must perform development and testing activities in non-production environments.

2.2. [The EHR Solution] Program should implement controls to segregate their production environments from their non-production environments keeping in mind the sensitivity of the data in non-production environments and practices. These controls may include:

2.2.1. Using separate access controls.

2.2.2. Using separate hardware for production and non-production activities.

2.2.3. Segmenting the production network from non-production networks (e.g., through the use of network gateways).

2.2.4. Creating separate warning banners and display features that clearly indicate the environment.

Requirements Analysis and Specification

2.3. [The EHR Solution] Program should perform an initial information security review on all their proposed information systems based on the known information system requirements and the business objectives to provide information security requirements for the developers.

2.4. Where the information security functionality in a proposed product does not satisfy the specified information security requirements, then [the EHR Solution] Program should consider the risks that would be introduced by the information system prior to purchasing the product.

2.5. [The EHR Solution] Program should document information security requirements so that they can be used as a basis for requirements of future releases of the information system.

Design

2.6. [The EHR Solution] Program should review their information system development design specifications and processes to ensure that sufficient controls are place to address information security requirements.

2.7. [The EHR Solution] Program should use the information requirements for the application to document the information system architecture design.

2.8. [The EHR Solution] Program should develop and document a detailed design for each information system module, component, or service. The detailed design should be refined into lower levels containing application units that can be coded, compiled, and tested.

2.9. [The EHR Solution] Program should develop and document a detailed design for the interfaces external to the information system module/component/service, between the information system components, and between the application units.

Development

2.10. [The EHR Solution] Program must protect source code against unauthorized access and modification (e.g., through the use of access controls).

2.11. [The EHR Solution] Program should store all source code in a source code repository and implement version control to manage code development.

2.12. [The EHR Solution] Program should develop all applications in accordance with secure coding guidelines. Guidance on secure coding is available from:

2.12.1. CERT®.

2.12.2. National Institute of Standards and Technology (NIST).

2.12.3. Open Web Application Security Project (OWASP).

2.12.4. SANS Institute.

2.13. [The EHR Solution] Program must ensure that accounts, user IDs, private encryption keys, and passwords are not imbedded in the source code or published solution.

2.14. [The EHR Solution] Program should review all custom code prior to release into production. Reviews of custom code ("code reviews") may be performed manually or with the assistance of automated review tools.

2.15. All manual code reviews should be performed by agents or Electronic Service Providers other than the original custom code developer (or outsourced code developer), and who are knowledgeable in code review techniques and secure coding practices.

2.16. All code reviews should identify and remediate, at a minimum, all of the following coding vulnerabilities:

2.16.1. Injection flaws: The code reviewer must validate input to verify that data inputted by an end user cannot modify the meaning of commands and queries, utilize parameterized queries, etc. (e.g., to prevent SQL injection, OS Command Injection, LDAP and XPath injection flaws).

2.16.2. Buffer overflows: The code reviewer must validate buffer boundaries and truncate input strings.

2.16.3. Insecure cryptographic storage: The code reviewer must validate that cryptographic functions are used properly when used to protect stored data.

2.16.4. Insecure communication: The code reviewer must validate that all authenticated and sensitive communications are properly encrypted.

2.16.5. Improper error handling: The code reviewer must validate that sensitive information is not leaked via error messages.

2.17. In addition to the above, all custom code used for web applications and application interfaces must be tested and remediated for all of the following coding vulnerabilities:

2.17.1. Cross-site scripting (XSS): The code reviewer must validate all parameters before inclusion, utilize context sensitive escaping, etc.

2.17.2. Improper Access Control: The code reviewer must validate that end users are properly authenticated, input is sanitized, and internal object references are not exposed to end users and the access control is not bypassed via any backdoors.

2.17.3. Cross-site request forgery (CSRF): The code reviewer must validate that applications do not reply on authorization credentials and tokens automatically submitted by browsers.

2.17.4. Invalidated Redirects and Forwards: The code reviewer must validate that all the supplied URL values are valid and authorized for the user.

2.18. [The EHR Solution] Program must ensure that all security deficiencies or vulnerabilities identified during the code review are corrected or the risk is accepted prior to production implementation.

2.19. [The EHR Solution] Program should ensure that code review results are reviewed, approved, and signed-off by their respective management prior to release.

Outsourced Code Development

2.20. Where access to external party source code (or equivalent) is restricted, [the EHR Solution] Program should ensure that a copy of the code is:

2.20.1. Maintained in escrow by a trusted external party.

2.20.2. Checked regularly to ensure it is up-to-date and works correctly.

2.21. Vendor-supplied software packages should be used without modification (i.e. without modification to the base vendor application features).

2.22. When a vendor-supplied package needs to be modified, [the EHR Solution] Program should consider the following:

2.22.1. The risk of built-in controls and integrity processes being compromised.

2.22.2. Obtaining the required changes from the vendor as a standard program update.

2.22.3. The impact of becoming responsible for future maintenance of the software as a result of the change.

Testing

2.23. [The EHR Solution] Program should ensure that procedures for testing information systems under development cover the:

2.23.1. Types of hardware, software and services to be tested.

2.23.2. Use of structured test plans, including user involvement.

2.23.3. Types of testing (e.g., end-to-end and performance testing).

2.23.4. Data use for performing tests.

2.23.5. Document, review and sign-off of the testing results.

2.24. New information systems should be tested in accordance with predefined, documented test plans, which shall be cross-referenced to the information system design/specification to ensure complete coverage. Key user representatives should be involved in planning tests, providing test data and reviewing test results.

2.25. [The EHR Solution] Program should ensure that the information system testing environment mimics the production environment to the greatest degree possible.

2.26. The complete information system environment should be tested to identify any conflicts or dependencies with other information systems, which includes:

2.26.1. Using the underlying technical security infrastructure.

2.26.2. Interfacing with other applications.

2.26.3. Running different operating systems, runtime libraries and browser software.

2.26.4. Interfacing with databases and directory services.

2.26.5. Processing on particular hardware, including service/mobile device/hand-held configurations.

2.27. [The EHR Solution] Program should conduct information system tests with the information system running in expected, unexpected (e.g. excessive load, or unavailable services), and infrequent (e.g. limited connectivity or delayed service responses) conditions.

2.28. [The EHR Solution] Program should not use production data, with the exemption of data classified as Public, in non-production environments, unless the information security controls in the non-production environment mirrors the information security controls implemented (or to be implemented) in the production environment. Otherwise, [the EHR Solution] Program should sanitize all production data (e.g., masked, scrambled, scrubbed), prior to loading and using it in non-production environments, in a way that:

2.28.1. A record or transaction cannot be traced to an individual.

2.28.2. The information, if disclosed to unauthorized individuals, will not have an adverse effect on [the EHR Solution], its agents or Electronic Service Providers, or HICs, their agents or Electronic Service Providers, or any patient.

Security Testing

2.29. Security testing activities should be incorporated where possible as part of the overall testing activities of [the EHR Solution] to provide frequent feedback on potential information security enhancements or improvements.

2.30. [The EHR Solution] Program must perform vulnerability and configuration scans on any new infrastructure deployment or service prior to its production release, with all [EHR Solution] major releases being supported by a comprehensive vulnerability assessment.

2.31. [The EHR Solution] program must perform penetration tests on all major releases of internet-facing applications that are part of [the EHR Solution] and that provide or support access to PHI prior to its availability in the production environment.

2.32. 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 (e.g., SQL/LDAP injection, cross-site scripting, session token attacks and URL forgery) and must be subject to rigorous external content review.

2.33. [The EHR Solution] Program should use prepared test data (e.g., high volume of concurrent users, URLs, command-line inputs and random data) designed to identify system faults or system weaknesses (e.g., buffer overflow and faulty memory) to perform information security tests on their information systems.

2.34. [The EHR Solution] Program should implement a process to ensure that flaws or security weaknesses identified during the testing process are resolved in a consistent manner, which includes:

2.34.1. Recording details of security weaknesses identified (e.g., in a test log).

2.34.2. Assessing the associated risks.

2.34.3. Implementing actions to address these risks.

2.34.4. Repeating tests of the application following corrective actions.

2.34.5. Security testing results that identify weaknesses should be handled as confidential until the specific flaw has been addressed.

2.35. Where information security testing reveals one or more weaknesses in a third-party product, [the EHR Solution] Program should communicate their findings directly to the third-party.

Promotion and Installation

2.36. Before new information systems are promoted into the production environment, [the EHR Solution] Program should ensure that:

2.36.1. Information security assessments have been performed.

2.36.2. Limitations of information security controls have been documented.

2.36.3. Approval has been obtained from an appropriate representative.

2.36.4. Service level agreements have been established to support systems in the production environment, if required.

2.37. [The EHR Solution] Program should not permit code to be promoted directly from a development environment to a production environment, or vice versa, but should require all code to follow a code promotion process.

2.38. [The EHR Solution] Program must only permit executable code to be promoted to the production environment. Development code or compliers must be prohibited in the production environment.

2.39. [The EHR Solution] Program should define and implement an installation process or deployment plan.

2.40. [The EHR Solution] Program should create a rollback strategy prior to implementing changes.

2.41. [The EHR Solution] Program should use a configuration control system to keep control of all implemented software, as well as the system documentation.

2.42. [The EHR Solution] Program should only permit designated agents and Electronic Service Providers to update production operational software, applications, and program libraries.

Change Control

2.43. [The EHR Solution] Program must implement a change control process to govern all changes to production information systems.

2.44. [The EHR Solution] Program should ensure that their change control process:

2.44.1. Maintains a record of agreed authorization levels.

2.44.2. Ensures changes are submitted by authorized users.

2.44.3. Reviews information security controls to ensure that they will not be compromised by the changes.

2.44.4. Identifies all software, information, database entries, and hardware that require amendment.

2.44.5. Obtains formal approval from information system owner for detailed proposals before work commences.

2.44.6. Ensures authorized users accept changes prior to implementation.

2.44.7. Ensures the information system documentation set (i.e., the document(s) relevant to the information system being changed) is updated on the completion of each change, and the old documentation is archived or disposed.

2.44.8. Maintains a version control for all software updates.

2.44.9. Maintains an audit trail of all change requests.

2.44.10. Ensures that all information included in the change control process (database names, accounts, network addresses, etc.) are disclosed only to the relevant parties in the appropriate steps of the change control procedure.

Post Implementation Review

2.45. [The EHR Solution] Program must develop a process to test the information security controls of their information systems after implementation. The process should ensure that:

2.45.1. A review of the application control and integrity procedures is completed to ensure that they have not been compromised by the operating system changes.

2.45.2. Appropriate changes are made to the business continuity plans.

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 which will recommend appropriate action to [the EHR Solution] Steering Committee.

The Applicable Oversight Body has the authority to impose appropriate penalties, up to and including termination of the Agreements with the HIC 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)

Other

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