eHealth Ontario
It's working for you

Threat Risk Management Standard

Version: 1.6

Document ID: 3547

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	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	2014-08-20	Updated based on feedback from the CSC Members. Included reference to the Harmonized Assurance Policy; clarified language around HIC TRA requirements in 1.1; Included condition to consider a TRA revision when Agreements or Legislative changes occur; Added language requiring final approval of the TRA document by the Steering Committee prior to sharing the TRA with HICs.	Mark Carter
1.2	2014-09-09	Updated 1.5 and 2.7 to note that delta TRAs are options. Policy was approved at the September 9th 2014 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 The Steering Committee has been replaced by the Applicable Oversight Body. TRAs activities previously supported by the regional PSC have now moved to the Connecting Security Committee.	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

Threat Risk Management Standard

Purpose

To define the strategy for assessing and managing information security-related risks that are related to [the EHR Solution] or a HIC's identity provider service or data contribution endpoints.

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 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 interface engines 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 Electronic Service Providers who do not view, create or contribute to [the EHR Solution].

This standard should be read in conjunction with the Harmonized Assurance Policy and their associated procedures, as amended from time to time.

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.

Privacy and Security Committee (PSC): The Privacy and Security Committee (PSC) is a committee comprised of agents from participating HICs to support the privacy and information security governance structure.

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 in the Information Security Policy.

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

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.

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 are responsible for performing Threat Risk Assessments (TRAs) on their own identity provider services and data contribution endpoints. HICs may have a TRA performed by an entity on their behalf and leverage that work to satisfy this requirement.

1.2. HICs should perform TRAs on their identity provider services and data contribution endpoints in accordance with a TRA methodology that is publicly documented and published by a regulatory or international standards-setting body. These may include threat risk assessment methodologies published or recommended by:

1.2.1. Communications Security Establishment Canada (CSEC).

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

1.2.3. International Organization for Standardization (ISO).

1.2.4. European Network for Information Security Agency (ENISA).

1.3. HICs should request executive summaries (results) of TRAs that are completed on [the EHR Solution].

1.4. Where a HIC receives a TRA from [the EHR Solution] Program, the HIC must restrict access to that TRA and any supporting documentation, and ensure that the TRA is handled in a secure manner.

1.5. HICs should perform a TRA or delta TRA under the following conditions:

1.5.1. Prior to significant modification to existing back-end architecture or functionality;

1.5.2. Prior to significant changes to existing front-end technical design or functionality;

1.5.3. Prior to significant changes to operational support models, tools, process, or parties;

1.5.4. Prior to significant changes to existing policies or procedures;

1.5.5. Prior to providing new Electronic Service Providers with access to [the EHR Solution];

1.5.6. Prior to changes to applicable agreements that could be expected to impact the privacy of individuals or the security of their PHI;

1.5.7. Prior to Legislative changes to PHIPA that could be expected to impact the privacy of individuals or the security of their PHI;

1.5.8. On discovery of a vulnerability that resulted in, or could have resulted in, an information security incident that affects or would have affected [the EHR Solution], or

1.5.9. Every five years if none of the above has initiated a comprehensive TRA.

1.6. HICs should document a risk treatment option for all risks identified in their TRA. Risk treatment options may include one or more of the following:

1.6.1. Applying additional information security controls to further reduce the risk.

1.6.2. Accepting the risk.

1.6.3. Avoiding the risk by not allowing the actions that would cause the risk to occur.

1.7. Where a HIC chooses as the risk treatment option to apply additional information security controls, these controls should be implemented to meet the requirements identified in the TRA.

1.8. HICs should document and monitor all their risks in a risk register with identified owners, action plans (risk treatment option details), and status. Risks should be reviewed quarterly and risk treatment options updated if required.

2. Requirements for [the EHR Solution]

2.1. [The EHR Solution] Program shall be responsible for performing TRAs on [the EHR Solution].

2.2. [The EHR Solution] Program must perform all threat risk assessments (TRAs) in accordance with the Harmonized Threat and Risk Assessment Methodology published by the Communications Security Establishment Canada (CSEC).

2.3. [The EHR Solution] Program shall make executive summaries (results) of TRAs and relevant risk treatment plans available on request to HICs who have access to [the EHR Solution] within three business days upon approval of the TRA and remediation plan by the Applicable Oversight Body.

2.4. [The EHR Solution] Program shall maintain:

2.4.1. An asset listing that contains valuation and classification ratings for [the EHR Solution].

2.4.2. A risk listing that contains threat and vulnerability ratings for [the EHR Solution].

2.5. All revisions to asset and risk listings must be approved by the Applicable Oversight Body.

2.6. [The EHR Solution] Program must treat all completed or partially completed TRAs and supporting documentation in accordance with the protection requirements for information classified as Confidential.

2.7. [The EHR Solution] Program must perform a TRA or delta TRA on [the EHR Solution] under the following conditions:

2.7.1. Prior to significant modification to existing back-end architecture or functionality;

2.7.2. Prior to significant changes to existing front-end technical design or functionality;

2.7.3. Prior to significant changes to operational support models, tools, process, or parties;

2.7.4. Prior to significant changes to existing policies or procedures;

2.7.5. Prior to a change of Electronic Service Provider;

2.7.6. Prior to changes to applicable agreements that could be expected to impact the privacy of individuals or the security of their PHI;

2.7.7. Prior to Legislative changes to PHIPA that could be expected to impact the privacy of individuals or the security of their PHI;

2.7.8. On discovery of a vulnerability that resulted in, or could have resulted in, an information security incident as deemed necessary by Connecting Security Committee, or

2.7.9. At a minimum, every two years if none of the above has initiated a comprehensive TRA.

2.8. [The EHR Solution] Program must document a risk treatment option for all risks identified through the TRA process. Risk treatment options may include one or more of the following:

2.8.1. Applying additional information security controls to further reduce the risk;

2.8.2. Accepting the risk, or

2.8.3. Avoiding the risk by not allowing actions that would cause the risk to occur.

2.9. Where [the EHR Solution] Program chooses as the risk treatment option to apply additional information security controls, these controls must be implemented to meet the requirements identified in the TRA.

2.10. [The EHR Solution] Program must document and monitor all their accepted risks in a risk register with identified owners, action plans (risk treatment option details), and status. Risks should be reviewed quarterly and risk treatment options updated if required.

2.11. [The EHR Solution] Program must present all their TRAs to eHealth Ontario who will facilitate reporting to the Connecting Security Committee and to the Applicable Oversight Body for sign off.

Where medium or higher residual risks exist, the TRA must also be signed off by a senior level executive (e.g., CIO) in [the EHR Solution] Program prior to submission to eHealth Ontario.

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)

Other

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