eHealth Ontario
It's working for you

Electronic Service Provider Standard

Version: 1.6

Document ID: 3538

Ontario
eHealth Ontario

Copyright Notice

All rights reserved

Trademarks

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	2013-12-20	Nov 2013 version adopted from the cGTA PSWG	Mark Carter
1.1	2014-10-09	Updated based on feedback from cGTA, cSWO and eHealth Privacy. Minor edits to the scope, exemption and enforcement sections to align with the CPC policies, provided a formal definition of the data contribution endpoint and identity provider services, expanded 1.4.10, 1.5, 2.3, 2.4.10, 2.5 to include privacy controls, added a footnote to 2.6, clarified the example in 2.7 to note it as an optional control.	Mark Carter
1.2	2014-11-05	Policy approved at the Nov5th 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 was replaced by the Applicable Oversight Body. The regional privacy and security committee has been removed from the exemption decision process.	Mark Carter
1.5	2017-03-20	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	Update standard to include Patient access to the EHR.	Geovanny Diaz

Electronic Service Provider Standard

Purpose

To define the requirements for managing Electronic Service Providers.

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 Electronic Service Providers who will support or have access 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 Electronic Service Providers who will support or have access to:
  - Direct network connections 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, this standard also applies to Electronic Service Provider who will support or have access 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 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, 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 should identify Electronic Service Providers and categorize them according to supplier type (e.g., application service provider, network service provider, storage service provider, etc.) and criticality of the services they provide.

1.2. HICs must assess the potential information security and privacy risks posed by all new Electronic Service Providers to [the EHR Solution] prior to engaging in a contractual relationship with that Electronic Service Provider.

1.3. HICs must define and document all information systems and services to be provided by new Electronic Service Providers or on renewal of service agreements. Service agreements should specify:

1.3.1. Roles and responsibilities under PHIPA and under the privacy and information security policies and procedures implemented in respect to [the EHR Solution].

1.3.2. Roles and responsibilities for implementing, maintaining and supporting the information systems or services to be provided.

1.3.3. The level of criticality of the service.

1.3.4. The dates and times when the service is required.

1.3.5. The capacity requirements of systems and networks.

1.3.6. Maximum permissible down-time and service level objectives.

1.3.7. Service level reports and frequency.

1.3.8. Critical timescales, i.e., the timescale beyond which a loss of service would be unacceptable to the HIC.

1.3.9. The penalties to be imposed in the event the Electronic Service Provider fails to deliver the pre-agreed level of service or fails to fulfill its roles and responsibilities.

1.3.10. Minimum information security and privacy controls.

1.3.11. Expected deliverables.

1.3.12. Representatives of Electronic Service Providers.

1.4. HICs must require new Electronic Service Providers to implement applicable information security and privacy controls as outlined in the EHR policy and standard prior to the Electronic Service Provider being granted access or providing support to [the EHR Solution].

1.5. HICs should establish a consistent method for handling the termination of relationships with Electronic Service Providers, which may include:

1.5.1. Designating agents responsible for managing the termination.

1.5.2. Revocation of physical and logical access rights to the organization's information.

1.5.3. Secure return, transfer or destruction of all assets (e.g., back-up media storage, documentation, hardware, and authentication devices)

2. Requirements for [the EHR Solution]

2.1. [The EHR Solution] Program should identify Electronic Service Providers and categorize them according to supplier type (e.g., application service provider, network service provider, storage service provider, etc.) and criticality of the services they provide.

2.2. [The EHR Solution] Program must assess the potential information security and privacy risks posed by Electronic Service Providers to [the EHR Solution] prior to engaging in a contractual relationship with that Electronic Service Provider.

2.3. [The EHR Solution] Program must define and document all information systems and services to be provided by any new Electronic Service Provider or on renewal of any service agreements. At a minimum, service agreements must specify:

2.3.1. Roles and responsibilities under PHIPA and under the privacy and information security policies and procedures implemented in respect of [the EHR Solution].

2.3.2. Roles and responsibilities for implementing, maintaining and supporting the information systems or services to be provided.

2.3.3. The level of criticality of the service.

2.3.4. The dates and times when the service is required.

2.3.5. The capacity requirements of systems and networks.

2.3.6. Maximum permissible down-time and service level objectives.

2.3.7. Service level reports and frequency.

2.3.8. Critical timescales, i.e., the timescale beyond which a loss of service would be unacceptable to [the EHR Solution].

2.3.9. The penalties to be imposed in the event the Electronic Service Provider fails to deliver the pre-agreed level of service or fails to fulfill its roles and responsibilities.

2.3.10. Minimum information security and privacy controls.

2.3.11. Expected deliverables.

2.3.12. Representatives of Electronic Service Providers.

2.4. [The EHR Solution] Program must require Electronic Service Providers to implement all applicable information security and privacy controls prior to the Electronic Service Provider being granted access to [the EHR Solution].

2.5. [The EHR Solution] Program must ensure that threat risk assessments are performed on their Electronic Service Providers[1].

2.6. [The EHR Solution] Program must give consideration to restricting the location of information, information processing, and information system services controlled or provided by Electronic Service Providers (e.g., an organization may choose to prohibit an Electronic Service Provider from storing their information on servers located outside of Canada).

2.7. [The EHR Solution] Program should establish a consistent method for handling the termination of Electronic Service Provider relationships, which should include:

2.7.1. Designating agents responsible for managing the termination.

2.7.2. Revocation of physical and logical access rights to the organization's information.

2.7.3. Secure return, transfer or destruction of all assets (e.g., back-up media storage, documentation, hardware, and authentication devices).

2.8. [The EHR Solution] Program must establish contingency arrangements to ensure that their respective business processes can continue in the event that the Electronic Service Provider is not available (e.g., due to contract termination, a disaster, or labour disputes). These arrangements should be based on the results of a threat risk assessment, and may include:

2.8.1. The provision of alternative, secure facilities for business processes to continue.

2.8.2. Escrow of information and close/propriety technologies (e.g., application source code and cryptographic keys using a trusted external party, such as a lawyer.

2.8.3. Recovery arrangements to ensure continued availability of information stored at an outsource provider or in the cloud.

2.8.4. Alignment with [the EHR Solution] business continuity program.

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

[1] See the *Threat Risk Management Policy* for more information on threat risk assessments (TRAs), including frequency.

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

References

Legislative

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

International Standards

- ISO/IEC 27001:2005, Information Technology – Security Techniques – Information Security Management Systems – Requirements.
- ISO/IEC 27002:2005, Information Technology – Security Techniques – Code of Practice for Information Security Management
- ISO/IEC 27005: 2008 Information Technology – Security Techniques – Information Security Risk Management
- ISO 27799:2008(E), Health Informatics – Information security management in health using ISO/IEC 27002

eHealth Ontario EHR Policy Documents

- Information Security Policy
- Acceptable Use of Information and Information Technology Standard
- 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)