Ontario Health

Local Registration Authority Practices Standard

Version: 1.8

Document ID: 3543

Document Control

Next Review Date: Every two years or otherwise established by the Connecting Security Committee.

Approval History

APPROVER(S)	APPROVED DATE
Connecting Security Committee	2015-01-22
Connecting Security Committee	2021-03-18

Revision History

VERSION NO.	DATE	SUMMARY OF CHANGE	CHANGED BY
1.1	2013-12-23	Nov 2013 version adopted from the cGTA PSWG	Mark Carter
1.2	2014-12-05	Updates based on feedback from Membership and ONE ID group. Added definition of Agent, LRA, Sponsor. Updated Appendix D and E to include options to enroll new, revoke, reinstate or suspend Agent and ESP access. Noted options for the RA to be a delegate rather than always [the EHR Solution]; Entitlement section was modified to put responsibilities on the Sponsor vs. LRA; Noted alternate processes for registration in Appendix D; a role field was added to Appendix E; Added Appendix F – Enrollment form for user already registered	Mark Carter
1.3	2014-12-18	Updated document based on the Dec 17th meeting of the CSC. Updated the entitlement section to allow access to permitted administration functionality of [the EHR Solution]	Mark Carter
1.4	2015-01-22	Added statement 2.5 which requires the Legally Responsible Person to identity individuals who have the authority to act as a sponsor. Reorganized statement 2.7.1 to provide more clarity. Policy approved by the CSC.	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 to a Standard to align with the IT Rules Management Plan. EHR Solution definition was updated. Revised controls based on feedback. Assigning Credentials moved into Federation Standard.	Raviteja Addepalli
1.7	2020-04-27	Added 1.7 as part of regular review set out by the Connecting Security Committee	Trina Dobson

VERSION NO.	DATE	SUMMARY OF CHANGE	CHANGED BY
1.8	2021-01-21	Review of the document with minor changes, updated references and the review cycle to biennially.	Ana Fukushima

Local Registration Authority Practices Standard

Purpose

To define the procedures for enrolling Local Registration Authorities (LRAs) and for enrolling Agents and Electronic Service Providers for access to [the EHR Solution].

Scope

These procedures apply to all health information custodians (HICs) that will provide their Agents and Electronic Service Providers with access to [the EHR Solution] through their local identity provider technology or another Federated Identity Provider.

This procedure does not apply to HICs that provide their agents and Electronic Service Providers with access to [the EHR Solution] through Ontario Health's ONE ID identity management 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.

Agent: In relation to a health information custodian, means a person that, with the authorization of the custodian, acts for or on behalf of the custodian in respect of personal health information for the purposes of the custodian, and not the agent's own purposes, whether or not the agent has the authority to bind the custodian, whether or not the agent is employed by the custodian and whether or not the organization is being remunerated. For example, an agent may be an organization, employee or contractor that validates identities of the EHR users on behalf of a HIC; an Agent may perform data correction services for a HIC on their data contribution endpoint.

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.

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.

Electronic Service Provider: A person or entity that provides goods or services for the purpose of enabling a HIC to use electronic means to collect, use, modify, disclose, retain or dispose of PHI, and includes a health information network provider.

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].

Legally Responsible Person (LRP): Often a senior executive within the organization, such as the Chief Information Officer. This person is legally responsible for the enrollment process at their HIC. The LRP is responsible for authorizing Sponsors and LRAs to act on behalf of the HIC in the enrollment and enrollment processes.

Local Registration Authority (LRA): A person who has been authorized by a HIC's Legally Responsible Person to manage the registration and/or enrollment process for the HIC's agents and Electronic Service Providers to obtain access to [the EHR Solution] through the HIC's access control processes, procedures, policies and identity management system. LRAs are registered with [the EHR Solution] Program or its delegate and enroll and register agents and Electronic Service Providers on behalf of [the EHR Solution]. To note, the definition of LRA applies in the context of this policy and [the EHR Solution].

May: The requirement is only a recommendation, or provided as an implementation example and is not intended on being exhaustive.

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.

Sponsor: Any person who has the authority to authorize the access of agents and Electronic Service Providers to [the EHR Solution]. Typically, LRPs authorize persons such as managers to act as Sponsors, this may also be delegated to an LRA. To note, the definition of Sponsor applies in the context of this policy and [the EHR Solution].

Standard Requirements

1. Requirements for Health Information Custodians

1.1. The Legally Responsible Person (LRP) must identify a named person(s), group(s), or role(s) that has the authority to act as a Sponsor.

1.2. The Sponsor must only provide access to [the EHR Solution] clinical components to Agents whose purpose of access is to collect PHI for providing or assisting in the provision of healthcare.

Examples of end-users who may meet the criteria of providing healthcare or assisting in the provision of healthcare, may include, but are not limited to:

1.2.1. Regulated health professionals who see patients

1.2.2. Residents providing care to patients

1.2.3. Administrative staff who pull charts for physicians

1.2.4. Ward clerks who review results to flag abnormal for physicians

1.3. The Sponsor must only provide access to [the EHR Solution] administration components to Agents and Electronic Service Providers whose purpose of access is to:

1.3.1. Provide support for defined and permitted functionality within the administration roles of [the EHR Solution] (e.g. Privacy Officers, System Administrators Agents and Electronic Service. Providers must not be granted access to functionality intended for those providing health care or assisting in the provision of health care (e.g. Clinicians).

For example, system administrators may require access to error queue management functionality to correct and process messages; privacy officers may require access to privacy reports to generate audit reports; data mapping specialists may require access to the terminology mapping functions to map codes and terminologies. These individuals must not be granted access to functionality intended for those providing healthcare or assisting in the provision of health care (e.g. clinicians).

1.4. The Sponsor must not provide access to [the EHR Solution] if access is requested for purposes other than providing or assisting in the provision of healthcare, e.g., providing access for the purposes of:

1.4.1. Program planning, evaluation, or monitoring

1.4.2. Risk or error management

1.4.3. Improving the quality of care, programs, and services

1.4.4. Education and training (unless the individual is a student or resident who requires access to provide care)

1.4.5. For processing payments.

1.5. The Sponsor must not provide access to [the EHR Solution] if access is requested for the purpose of research.

1.6. If an agent or Electronic Service Provider has multiple roles, e.g., is both a clinician and a risk manager, the Sponsor may assign that person with access to [the EHR Solution] for the purposes of collecting PHI for providing or assisting in the provision of health care and must ensure that the end-user understands their permissions and obligations.

1.7. The Sponsor must remove entitlements that are no longer needed by the agent, e.g. the agent no longer works for the HIC.

Exemptions Any exemptions to this Policy 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 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 27001:2013, Information Technology – Security Techniques – Information Security Management Systems – Requirements
- ISO/IEC 27002:2013, Information Technology – Security Techniques – Code of Practice for Information Security Management
- ISO/IEC 27005: 2018 Information Technology – Security Techniques – Information Security Risk Management
- ISO 27799:2016 Health Informatics – Information security management in health using ISO/IEC 27002

Ontario Health 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 Standard
- 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