eHealth Ontario
It's working for you

Access Control and Identity Management Standard for System Level Access

Version: 1.7

Document ID: 3535

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	2017-02-21
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	2014-12-05	Updates based on feedback from CSC Members and ONE ID. Scope of policy was narrowed to address system level access to the data contributor end point and identity provider services infrastructure. Guidance on end user registration has been referenced to the identity provider standard. Definition of End User was removed; LRA and Sponsor definitions were added. Ownership obligations added to service IDs – 1.19, 2.21; Appendix A was synchronized with the federation standard.	Mark Carter
1.2	2014-12-12	Updates based on the Dec 11th CSC meeting. 1.8, 2.10 was modified to provide flexibility of information captured if electronic or supporting workflow processes were used; 1.11, 2.13 was modified to ensure IDs and authorizations were reviewed; 1.20.1, 2.21.2 was modified to remove the requirement for service IDs to be changed annually; 1.25, 2.27 – passwords during entry must be concealed; 1,30,1.31, 2.33, 2.34 – clear text passwords must not be hard-coded; Appendix A modified to move password length of service IDs from 12 to 15 characters, move password change frequency to 120 days for personal and privilege user IDs, account lockout was moved to 10 attempts from 5	Mark Carter
1.3	2015-01-22	Updated 1.21 and 2.23 to require password changes on service IDs when technology changes and require new passwords to be selected. Appendix A was updated to highlight the requirement to communicate passwords securely. Policy approved by the CSC.	Mark Carter

VERSION NO.	DATE	SUMMARY OF CHANGE	CHANGED BY
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	2016-10-04	Appendix A was updated to communicate password change frequency approval of up to 1 year. Policy approved by the CSC.	Mark Carter
1.6	2017-02-21	Updated policies to incorporate 2017 refresh changes. Definition of EHR Solution was adjusted. A number of controls were rephrased to note "participating" in the EHR Solution.	Ravi Addepalli
1.7	March 16, 2018	Updated standard to include Patient access to the EHR and NIST password recommendations (NIST 800-63B)	Geovanny Diaz / Ola Edidi

Access Control and Identity Management Standard for System Level Access

Purpose

To define logical access control and identity management requirements for secure system level access to HIC Identity Provider Services and Data Contribution End Point infrastructure connected to [the EHR Solution] and system administrators accessing [the EHR Solution].

Scope

- The standard applies to health information custodians (HICs) system level 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.), including all Patient Portals/Applications.

- Direct network connectivity to [the EHR Solution] and administrative functionality, including components in the connection path (firewalls, proxies, etc.).

- The integration of [the EHR Solution] with the HIC's local health information system (HIS) or electronic medical record (EMR) application(s).

For HICs who create or contribute PHI to [the EHR Solution], this policy applies to HIC's systems administrators:

- Access to 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 policy applies to system level access from [the EHR Solution] and the Program Office.

Note: This standard does not address End Users accessing [the EHR Solution]. HICs acting as Identity Providers must follow the Federation Identity Provider Standard for direction and requirements when registering agents to access [the EHR Solution] and requirements for running IDP services.

This standard does not apply to any HIC, their agents or their Electronic Service Providers who do not 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.

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 agency 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.

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].

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.

Identifier (ID): A unique data string used as a key in an access control system to uniquely identify a person or information system that will have access to identity provider services and data contribution end point infrastructure connected to [the EHR Solution].

Local Registration Authority (LRA): A person who has been authorized by a HIC's Legally Responsible Person to manage the enrollment process for the HIC's agents and Electronic Service Providers to obtain access to [the EHR Solution] through the HIC's access control and identity management system. LRAs are registered with [the EHR Solution] Program and enroll 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].

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. To note, the definition of LRP applies in the context of this policy and [the EHR Solution].

Personal ID: An ID that is assigned to a person and is used for normal business operations to access identity provider services and data contribution end point infrastructure connected to [the EHR solution].

Privileged ID: An ID with privileges in excess of a normal Personal ID (e.g., administrator or root accounts).

Service ID: An ID used by an automated information system process to perform specific pre-determined activities (e.g., program start-up, file transfer, back-up).

Sponsor: Any person who has the authority to authorize the access of agents and Electronic Service Providers to the identity provider services and data contribution end point infrastructure connected to [the EHR Solution]. Typically, LRPs authorize persons such as managers to act as Sponsors. To note, the definition of Sponsor applies in the context of this policy and [the EHR Solution].

User: Any person (i.e., a HIC, agent or Electronic Service Provider of either a HIC or [the EHR Solution] Program) that is assigned an ID to manage the Identity Provider Services or Data Contribution End Point infrastructure connected to [the EHR Solution] or [EHR Solution] itself.

User ID: Any ID that is assigned to a user.

Remote Access: Any connection initiated via a virtual private network, terminal emulation, remote access software (e.g., RDP) from outside of the organization's network perimeter with the intent of accessing non-public or internal resources.

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

Human Resource Considerations

1.1. HICs must clearly define and document the information security responsibilities of all their agents and Electronic Service Providers with access to the identity provider services and data contribution end point infrastructure participating in [the EHR Solution]. These responsibilities may be combined with, or already covered by other information security responsibilities specified by the HIC.

1.2. HICs must implement a process to verify job application information for all new agents or Electronic Service Providers who will have access to the identity provider services and data contribution end point infrastructure participating in [the EHR Solution]. Verification methods may include:

1.2.1. Character or employment references.

1.2.2. Criminal record checks where possible taking into consideration employment arrangements of the organization and unions.

1.2.3. Verification of prior experience, academic record, and professional qualifications.

1.2.4. Verification of identity from government issued identification.

1.3. HICs must ensure that all their new agents and Electronic Service Providers who will have access to the identity provider services and data contribution end point infrastructure participating in [the EHR Solution] agree to maintain the security of personal health information (PHI). At a minimum, the terms and conditions of employment must:

1.3.1. Require adherence to their information security-related policies.

1.3.2. Explain the agent or Electronic Service Provider's legal responsibilities and rights (e.g., regarding protection of information or privacy legislation).

1.3.3. Include a non-disclosure/confidentiality clause that extends after employment.

1.3.4. State that information security responsibilities extend outside normal working hours, premises and networks, and continue after employment has ended.

General Access Controls

1.4. HICs must ensure that all access to the identity provider services and data contribution end point infrastructure participating in [the EHR Solution] is provisioned based on the requestor's established business needs, in accordance with their privacy policies, and in accordance with the principles of need-to-know and least-privilege (i.e., an agent or Electronic Service Provider is granted only the minimum access privileges required).

HICs are responsible for identifying all their agents and Electronic Service Providers who require access to the identity provider services and data contribution end point infrastructure participating in [the EHR Solution].

1.5. HICs must assign, and authentication services must ensure: that user ID's, Service IDs, and/or digital certificates/ Secure ID Tokens are unique and traceable to a single person when these are used to access the identity provider services and data contribution end point infrastructure connected to [the EHR Solution].

1.6. HICs must configure their access control and identity management systems to deny access by default to the identity provider services and data contribution end point infrastructure participating in [the EHR Solution] (i.e., access must be explicitly authorized).

Administering IDs

1.7. HICs must require the creation or amendment of a user ID that will have access to the identity provider services and data contribution end point infrastructure participating in [the EHR Solution] to be initiated by a written or electronic request (e.g., via an email or help desk ticket) that is approved by a Sponsor. The request for ID creation must contain access privileges requested and may contain the following information:

1.7.1. The Sponsor's details: full name, department, sponsor authority, location, and contact information (email and telephone number, where available).

1.7.2. Details of whom the ID is to be assigned to: full name, department and location, and contact information (email and telephone number, where available).

1.8. HICs should maintain a log of all requests for user IDs that they administer and will have access to the identity provider services and data contribution end point infrastructure participating in [the EHR Solution].

1.9. HICs must maintain a list of all individuals that have access to the identity provider services and data contribution end point infrastructure participating in [the EHR Solution]. The list must include the following:

1.9.1. The ID.

1.9.2. Person or information system's details: full name, department, and location, and contact information (email and telephone number, where available).

1.10. HICs must review a list of user IDs and authorizations that they administer and that have access to the identity provider services and data contribution end point infrastructure participating in [the EHR Solution] annually to ensure that authorized access remains appropriate, and must request modifications, suspensions, or revocations to privileges where inappropriate access is identified.

1.11. Upon termination of employment, contractual or other relationship, or a change in job duties or responsibilities, HICs must review and if necessary request a modification, suspension or revocation of access privileges on the identity provider services and data contribution end point infrastructure participating in [the EHR Solution] for their agents or Electronic Service Providers.

1.12. HICs must suspend IDs that have access to the identity provider services and data contribution end point infrastructure participating in [the EHR Solution] after 180 consecutive days (or 6 months) of inactivity either manually or automatically. HICs may send the user of the ID an email warning them of the imminent suspension.

Privileged IDs

1.13. HICs must not name Privileged IDs on their identity provider services and data contribution endpoints in a way that provides any indication of the ID's privilege level.

1.14. HICs must not assign privileged entitlements on their identity provider services and data contribution endpoints to a Personal ID. Persons requiring privileged access on a HIC's identity provider services and data contribution endpoints must be assigned a Privileged ID, and a Personal ID to be used for normal business activities.

1.15. HICs must ensure that the assignment and use of Privileged IDs on their identity provider services and data contribution endpoints is limited to the minimum number of persons who are directly responsible for operational support or administration.

Service ID

1.16. HICs should ensure that the names of Service IDs on their identity provider services and data contribution endpoints are different than the system names on which the Service IDs are created.

1.17. HICs should ensure that Service IDs on their identity provider services and data contribution endpoints are not capable of interactive sign-on.

1.18. HICs should ensure that an identified owner(s) is assigned to each service ID and maintained in an inventory.

1.19. HICs may use a non-expiring password for Service IDs on their identity provider services and data contribution endpoints with credentials that are incapable of being used by a person.

1.20. HICs must ensure that a Service ID on their identity provider services and data contribution endpoints with credentials that are capable of being used by a person and are embedded into an automated process have their passwords changed to a new password either:

1.20.1. Whenever the technology changes;

1.20.2. After an actual or suspected password compromise; or

1.20.3. After turnover of any person that knows the password.

Authentication

1.21. HICs must communicate initial passwords or passphrases ("passwords") used to access the identity provider services and data contribution end point infrastructure participating in [the EHR Solution] securely.

1.22. HICs must set initial passwords used to access the identity provider services and data contribution end point infrastructure participating in [the EHR Solution] to prompt the user to change their password at initial login or must ensure that the user is manually instructed to change their password at initial login.

1.23. HICs must ensure that passwords used to access the identity provider services and data contribution end point infrastructure participating in [the EHR Solution] are masked or concealed on entry (i.e., represented on the screen by a special character such as an asterisk). Temporary visibility of passwords is permitted depending on technology limitations.

1.24. HICs must ensure their information systems are technically capable of accepting User passwords used to access the identity provider services and data contribution end point infrastructure participating in [the EHR Solution] that meet the Personal ID password requirements and ensure compliance with the account lockout, lockout duration, history and minimum age requirements for passwords used to access the identity provider services and data contribution end point infrastructure participating in [the EHR Solution]. See *Appendix A*.

1.25. HICs must only reset a password used to access the identity provider services and data contribution end point infrastructure participating in [the EHR Solution] after the user's identity has been successfully verified.

1.26. HICs must encrypt passwords used to access the identity provider services and data contribution end point infrastructure participating in [the EHR Solution] in transmission.

1.27. HICs should encrypt passwords used to access the identity provider services and data contribution end point infrastructure participating in [the EHR Solution] in storage. Where passwords in storage cannot be encrypted, these passwords must not indicate the system or user ID for which they are associated.

1.28. HICs should not cache unencrypted passwords used to access the identity provider services and data contribution end point infrastructure participating in [the EHR Solution].

1.29. HICs should not hard-code clear text passwords used to access the identity provider services and data contribution end point infrastructure participating in [the EHR Solution] or store them in batch files.

1.30. HICs should ensure that clear text passwords used to access the identity provider services and data contribution end point infrastructure participating in [the EHR Solution] are not embedded in any automated login process, or stored in a macro or function key. Noted exemptions must be documented.

1.31. HICs should ensure that all paper-based passwords used for backup or contingency purposes for their identity provider services or data contribution endpoints are stored using the principle of dual control or split knowledge.

Sign-On Controls

1.32. In the event of an authentication failure (e.g., an invalid sign-on attempt) to the identity provider services and data contribution end point infrastructure participating in [the EHR Solution], HICs must ensure that their identity provider services do not indicate the reason for the failure (e.g., state that it was an incorrect password or that the ID does not exist on the system).

Default IDs and Passwords

1.33. HICs should rename all default IDs (commonly known as vendor IDs) on their identity provider services and data contribution endpoints.

1.34. HICs must change or set all default passwords on their identity provider services and data contribution endpoints, including null passwords, prior to deployment in a production environment and as soon as reasonably possible in a non-production environment.

Remote Access

1.35. HICs must ensure that additional authentication compensating factors (e.g., two-factor authentication or the use of challenge questions) are required when accessing the identity provider services and data contribution end point infrastructure participating in [the EHR Solution] remotely or from an untrusted source.

1.36. HICs must prohibit remote access to the identity provider services and data contribution end point infrastructure participating in [the EHR Solution] where no additional compensating factors are provided.

1.37. HICs must ensure that session management identifiers for remote access connections to the identity provider services and data contribution end point infrastructure participating in [the EHR Solution] are unique, maintain confidentiality and integrity for each individual session, and be valid only for the duration of the current session or for a predetermined finite time period.

Session Management

1.38. HICs must ensure that all users have the ability to end or terminate an active session when connected to the identity provider services and data contribution end point infrastructure participating in [the EHR Solution].

1.39. HICs must ensure that an interruption to a communication link to the identity provider services and data contribution end point infrastructure participating in [the EHR Solution] requires the person or information system to re-authenticate.

2. Requirements for [the EHR Solution]

Human Resource Considerations

2.1. [The EHR Solution] Program must clearly define and document the information security responsibilities of all their agents and Electronic Service Providers participating in [the EHR Solution].

2.2. [The EHR Solution] Program must implement a process to verify job application information for all their new agents or Electronic Service Providers who will participate in [the EHR Solution]. Verification methods may include:

2.2.1. Character or employment references.

2.2.2. Criminal record checks where possible taking into consideration employment arrangements of the organization and unions.

2.2.3. Verification of prior experience, academic record, and professional qualifications.

2.2.4. Verification of identity from government issued identification.

2.3. [The EHR Solution] Program must ensure that all their new agents and Electronic Service Providers who will participate in [the EHR Solution] agree to maintain the security of information, information systems and information technologies. At a minimum, the terms and conditions of employment must:

2.3.1. Require adherence to [the EHR Solution] information security-related policies.

2.3.2. Explain the agent or Electronic Service Provider's legal responsibilities and rights (e.g., regarding protection of information or privacy legislation).

2.3.3. Include a non-disclosure/confidentiality clause that extends after employment.

2.3.4. State that information security responsibilities extend outside normal working hours, premises and networks, and continue after employment has ended.

General Access Controls

2.4. [The EHR Solution] Program must verify the identities of all persons requesting participation in [the EHR Solution]. [The EHR Solution] Program may delegate this responsibility to HICs through the use of Local Registration Authorities.

2.5. [The EHR Solution] Program must ensure that all access is provisioned based on the requestor's established business needs, in accordance with their privacy policies, and in accordance with the principles of need-to-know and least-privilege (i.e., an agent or Electronic Service Provider is granted only the minimum access privileges required).

[The EHR Solution] Program is responsible for identifying all their agents and Electronic Service Providers who require access to participate in [the EHR Solution].

2.6. [The EHR Solution] Program must implement access control systems on [the EHR Solution]. The access control system must have authentication and authorization capabilities that:

2.6.1. Identify and authenticate individual persons or information systems, and

2.6.2. Limit or restrict access to an information system's resources, objects, data, and/or files.

2.7. [The EHR Solution] Program must assign all their agents, Electronic Service Providers, and information systems a unique ID before provisioning them with access to [the EHR Solution].

2.8. [The EHR Solution] Program must ensure that access to and use of [the EHR Solution] with a user ID is traceable to a single person and that access to and use of [the EHR Solution] with a Service ID is traceable to an information system.

2.9. [The EHR Solution] Program must configure its access control and identity management system to deny access by default to [the EHR Solution] (i.e., access must be explicitly authorized).

Administering IDs

2.10. [The EHR Solution] Program must require the creation or amendment of an ID managed by [the EHR Solution] Program to be initiated by a written or electronic request (e.g., via an email or help desk ticket) that is approved by a Sponsor unless the ID is created through an automated process (e.g., a Service ID during the installation of software). The request for ID creation must contain the access privileges requested and may contain the following information:

2.10.1. The Sponsor's details: full name, department, sponsor authority, location, and contact information (email and telephone number, where available).

2.10.2. Details of whom the ID is to be assigned to: full name, department, location, and contact information (email and telephone number, where available) or in the case of a Service ID, the details of the information system on which the ID is being created and owner.

2.10.3. Justification for request, if applicable (e.g., when requesting a Privileged ID).

2.11. [The EHR Solution] Program must maintain a log of all requests for IDs that they manage and that could be used to access [the EHR Solution].

2.12. [The EHR Solution] Program must maintain a list of all IDs that have access to [the EHR Solution]. The list should include the following:

2.12.1. The ID.

2.12.2. Person or information system's details: Full name, department, location, and contact information (email and telephone, where applicable).

2.12.3. Privileges associated with the ID.

2.12.4. Requirement/function (for Service IDs only).

2.12.5. Interactions (for Service IDs only).

2.13. [The EHR Solution] Program must review a list of IDs and authorizations they manage and that have access to [the EHR Solution] annually to ensure that authorized access remains appropriate and must request modifications, suspensions, or revocations to privileges where inappropriate access is identified.

2.14. Upon termination of employment, contractual or other relationship, or a change in job duties or responsibilities, [The EHR Solution] Program must review and if necessary request a modification, suspension or revocation of access privileges for their agents or Electronic Service Provider.

2.15. [The EHR Solution] Program must suspend user IDs that they manage and that have access to [the EHR Solution] after 180 consecutive days (or 6 months) of inactivity either manually or automatically. [The EHR Solution] Program may send the user of the ID an email warning them of the imminent suspension.

Privileged IDs

2.16. [The EHR Solution] Program must not name Privileged IDs on their information systems in a way that provides any indication of the IDs' privilege level.

2.17. [The EHR Solution] Program must not assign privileged entitlements on their information systems or information technologies to a Personal ID. All persons requiring privileged access must be assigned a Privileged ID, and a Personal ID to be used for normal business activities.

2.18. [The EHR Solution] Program must ensure that the assignment and use of Privileged IDs is limited to the minimum number of persons who are directly responsible for operational support or administration.

Service ID

2.19. [The EHR Solution] Program must ensure that the names of their Service IDs are different than the information system names on which the Service IDs are created.

2.20. [The EHR Solution] Program should ensure that Service IDs are not capable of interactive sign-on.

2.21. [The EHR Solution] Program should ensure that an identified owner is assigned to each service ID.

2.22. [The EHR Solution] Program may use a non-expiring password for Service IDs with credentials that are incapable of being used by a person.

2.23. [The EHR Solution] Program must ensure that a Service ID with credentials that are capable of being used by a person and are embedded into an automated process have their passwords changed to a new password either:

2.23.1. Whenever the technology changes;

2.23.2. After an actual or suspected password compromise; or

2.23.3. After turnover of any person that knows the password.

Authentication

2.24. [The EHR Solution] Program must communicate initial passwords or passphrases ("passwords") securely. Where an ID has been communicated through email, the associated password must be communicated through an alternative communication channel (e.g., via phone).

2.25. [The EHR Solution] Program must set initial passwords to prompt the user to change their password at initial login or must ensure that the user is manually instructed to change their password at initial login.

2.26. [The EHR Solution] Program must ensure that all passwords are masked or concealed on entry (i.e., represented on the screen by a special character such as an asterisk). Temporary visibility of passwords is permitted depending on technology limitations.

2.27. [The EHR Solution] Program must ensure that their information systems are technically capable of accepting all passwords that meet the requirements and ensure compliance with the account lockout, lockout duration, history and minimum age requirements for passwords used to access [the EHR Solution]. See *Appendix A*.

2.28. [The EHR Solution] Program must only reset a password after the user's identity has been successfully verified.

2.30. [The EHR Solution] Program must encrypt passwords in transmission.

2.31. [The EHR Solution] Program must protect passwords in storage. Where passwords stored in files cannot be encrypted, passwords must not indicate the information system or ID for which they are associated.

2.32. [The EHR Solution] Program must not cache unencrypted passwords.

2.33. [The EHR Solution] Program must not hard-code clear text passwords into information systems or stored in batch files.

2.34. [The EHR Solution] Program must ensure that clear text passwords are not embedded in any automated login process, or stored in a macro or function key.

2.35. [The EHR Solution] Program must ensure that all paper-based passwords used for backup or contingency purposes are stored using the principle of dual control or split knowledge.

Sign-On Controls

2.36. [The EHR Solution] Program must display a terms of use banner or message at, or prior to, initial user authentication. The terms of use must be accepted by the user in order to gain access to [the EHR Solution].

2.37. In the event of an authentication failure (e.g., an invalid sign-on attempt), [the EHR Solution] Program must ensure that [the EHR Solution] does not indicate the reason for the failure (e.g., state that it was an incorrect password or that the ID does not exist on the system)

Default IDs and Passwords

2.38. [The EHR Solution] Program must rename all default IDs (commonly known as vendor IDs).

2.39. [The EHR Solution] Program must change or set all default passwords, including null passwords, prior to deployment in a production environment and as soon as reasonably possible in a non-production environment.

Remote Access

2.40. [The EHR Solution] Program must ensure that additional authentication compensating factors (e.g., two-factor authentication or through the use of challenge questions) are required to access [the EHR Solution] remotely or from an untrusted source.

2.41. [The EHR Solution] Program must ensure that remote access for any of their users who have privileged access to [the EHR Solution], directly or indirectly (e.g., through the escalation of privileges), is permitted only through the use of [the EHR Solution]-approved virtual workspace computing solution.

2.42. [The EHR Solution] Program should maintain a record of all their agents and Electronic Service Providers that have authorized administrative remote access to [the EHR Solution]. At a minimum, the record should contain:

2.42.1. The agent or Electronic Service Provider's user ID.

2.42.2. The agent or Electronic Service Provider's full name.

2.42.3. The date of creation.

2.42.4. The level of entitlement granted.

2.42.5. The full name and position of the person who authorized the request.

2.43. [The EHR Solution] Program must employ cryptographic solutions to maintain session confidentiality and integrity of all remote access connections.

Session Management

2.44. [The EHR Solution] Program must ensure that Personal IDs are not capable of establishing multiple concurrent interactive sessions to [the EHR Solution]. [The EHR Solution] Program should ensure that Privileged IDs are not capable of establishing multiple concurrent interactive sessions to [the EHR Solution].

2.45. [The EHR Solution] Program must ensure that the state of a session is established and controlled by the information system providing the services.

2.46. [The EHR Solution] Program must implement session management mechanisms to protect session integrity and confidentiality (e.g., using Kerberos to maintain session integrity and using encryption to provide session confidentiality).

2.47. [The EHR Solution] Program must ensure that session management identifiers are unique for each individual session, and be valid only for the duration of the current session or for a predetermined finite time period.

2.48. [The EHR Solution] Program must ensure that all users have the ability to end or terminate an active session.

2.49. [The EHR Solution] Program must ensure that an interruption to a communication link to the source information system requires the person or information system to re-authenticate to the source information system.

2.50. [The EHR Solution] Program must ensure that their workstations and other User devices that have access to [the EHR Solution] either:

2.50.1. Have password-protected screen-locks, keyboard-locks or equivalent controls that are set to automatically lock after 15 minutes of inactivity; or

2.50.2. Set sessions to automatically terminate (e.g., sign-off active account) after a maximum period of 15 minutes of inactivity.

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.

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 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 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
- 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)

Appendix A: Minimum Password Requirements

The following is a list of minimum password requirements for IDs that have access to the identity provider services and data contribution end point infrastructure of HICs connected to [the EHR Solution] along with IDs of the Program Office connected to [the EHR Solution].

	Personal IDs & Privileged IDs	Service IDs
Length	At least 8 characters, with a maximum not less than 64 characters long.	At least 15 characters long.
Complexity	Contain at least **three** of the following conditions of complexity: • At least 1 uppercase character (A through Z) • At least 1 lowercase character (a through z) • At least 1 numerical digit (0 through 9) • At least 1 non-alphanumeric character (~!@#$%^&*_-+=' |\(){}[]:;"'<>,.?/): To permit no complexity, live screening of new passwords must be completed and displayed to users during password creation. Live screening must be done against a list of commonly used passwords: blacklist, dictionary, usernames, service names, sequential strings, and passwords from previous breaches.	Contain at least **all** of the following: • At least 1 uppercase character (A through Z) • At least 1 lowercase character (a through z) • At least 1 numerical digit (0 through 9) • At least 1 non-alphanumeric character (~!@#$%^&*_-+=' |\(){}[]:;"'<>,.?/);
Additional Password Attributes	• Where available, software that prohibits the use of recognizable patterns must be used • Passwords must not include all or part of the User's first / last names or any easily obtained personal (e.g., names of family members, pets, birthdays, anniversaries, all or part of a Login ID or a commonly known nickname); See the Acceptable Use of Information and Information Technology Policy • Initial or temporary passwords must be unique, not guessable, follow the password strength requirements and communicated securely following the requirements of this Policy • Passwords must not be blank and null passwords must not be used • Guest passwords must be disabled	
Expiration	Up to 1 year, provided suitable mitigating controls are in place, as outlined in the EHR Security Policies. Set password reset frequency to 90 days, if there are no suitable mitigating controls in place.	Service IDs are not required to be changed on a scheduled basis however equipment must use a new password when technologies change.
Account Lockout	After five unsuccessful consecutive attempts.	
Lockout duration	Until manually unlocked by: • An administrator, or • A self-service password reset facility. – OR – • Unlocked after a minimum 30 minutes.	
History	Last four passwords.	
Minimum Age	Two days.	