Ontario Health

Acceptable Use of Information and Information Technology Standard

Version: 2.0

Document ID: 3534

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	2017-02-21
Connecting Security Committee	2018-03-26
Connecting Security Committee	2019-07-04
Connecting Security Committee	2021-03-18

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	2014-08-18	Updates based on feedback from CSC Members. Inserted footnote 1 and 2. Realigned point 1.8 under Emailing PHI, adjusted language in 1.24 and 2.32, added point 1.25, 1.26, removed 2.1, and added language to 2.11, aligned references.	Mark Carter
1.2	2014-10-09	Revised based on Sept 9th 2014 feedback from the CSC. Updated 1.1 and 1.2 to use credentials vs. user id and password, expanded 1.4 to note willfully bypass, 1.8 – added requirement for all users to lock computing devices while unattended, 1.9, 2.5 – revised device to tools and processes, 1.13, 2.19 included caveats to note "where possible", 1.21 – included a note to report the incident, 1.22 added option for approve SSO managers, 1.23 added reference to the IDP standard, 1.30 – requested full disk encryption where data is downloaded and devices are used remotely.	Mark Carter
1.3	2014-10-16	Revised based on Oct 15th CSC Meeting. Updated 1.30to broaden acceptable implementations of encryption on the device.	Mark Carter
1.4	2014-11-05	Revised based on Nov 5th CSC Meeting. Updated 1.8 to should, 1.10 was reworded and 1.30 indicated a preference for full disk encryption. Policy was approved by the CSC.	Mark Carter
1.5	2015-01-21	Aligned name of access control policy based on final wave 3 CSC decision.	Mark Carter

VERSION NO.	DATE	SUMMARY OF CHANGE	CHANGED BY
1.6	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
1.7	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
1.8	March 16, 2018	Updated standard to include Patient access to the EHR and NIST password recommendations (NIST 800-63B).	Geovanny Diaz / Ola Edidi
1.9	July 4, 2019	Updated standard to require locking of devices and using passphrases	Ravi Addepalli
2.0	2021-01-21	Review of the document with minor changes, updated references and the review cycle to biennially.	Ana Fukushima

Acceptable Use of Information and Information Technology

Purpose

To define the behavioural requirements for all agents and Electronic Service Providers of [the EHR Solution], as well as all health information custodians (HICs), their agents and Electronic Service Providers who have access to [the EHR Solution]. These requirements are intended to help protect the confidentiality, integrity, and availability of personal health information (PHI) stored in or processed by [the EHR Solution].

Scope

This standard applies to:

- Agents and Electronic Service Providers of [the EHR Solution], including all Patient Portals/Applications.
- All HICs, their agents and Electronic Service Providers who create, contribute, view or have access to [the EHR Solution]. This standard does not apply to:
- Any HIC, their agents or 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 the 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 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.

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, their Agents and Electronic Service Providers

HICs, their agents and Electronic Service Providers ("all persons") must:

1.1. Always use their assigned credential to participate in [the EHR Solution].

1.2. Never allow another person to use their credentials to participate in [the EHR Solution]. All persons are accountable for any actions performed on [the EHR Solution] with their ID.

1.3. Never participate in [the EHR Solution] unless their role requires them to do so, they are expressly authorized to do so, it is necessary to do so (e.g., to provide or assist in the provision of healthcare), and in accordance with their respective HIC's or [the EHR Solution]'s privacy policies.

1.4. Never disable, override or willfully bypass any information security control when participating in [the EHR Solution].

1.5. Never attempt to exploit any suspected security weakness on [the EHR Solution], even to explore that such a weakness may exist, unless it is part of their assigned job duties or responsibilities and they are explicitly authorized to do so.

1.6. Never knowingly perform an act that will interfere with the normal operations of [the EHR Solution], or try to disrupt [the EHR Solution] by either intentionally making the solution unavailable or by affecting the integrity of the data being stored in or processed for the participation in [the EHR Solution].

1.7. Abide by the terms and conditions of [the EHR Solution].

1.8. All users must lock their computing devices when leaving their device unattended while logged on to [the EHR Solution] within the HIC's premises.

1.9. Use a [the EHR Solution] or HIC-approved tools and processes to participate in [the EHR Solution].

1.10. Never take a picture of data displayed on [the EHR Solution].

Emailing PHI

All persons must:

1.11. Only email PHI to [the EHR Solution] Program Office when it is necessary for the purposes of providing or assisting in the provision of health care or [the EHR Solution] business, and is acceptable under their respective HIC's and [the EHR Solution]'s policies or procedures.

1.12. Either encrypt emails that contain PHI, use a secure file transfer solution or use a secure email system approved by their respective HIC or [the EHR Solution].

1.13. Never use external email accounts (e.g., Hotmail, or Gmail) to send PHI to or receive PHI from [the EHR Solution].

Creating and Protecting Passwords

All persons must:

1.14. Use phrases (e.g., IL0v3EatingP!zza) when creating passwords used to participate in [the EHR Solution].

All persons must:

1.15. Always create passwords used to participate in [the EHR Solution] that are at least eight characters, with a maximum not less than 64 characters long, and include at least three of the following conditions of complexity:

1.15.1. One number

1.15.2. One uppercase letter

1.15.3. One lowercase letter, or

1.15.4. One special 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.

1.16. Never create passwords used to participate in [the EHR Solution] that include:

1.16.1. All or part of their ID.

1.16.2. Easily obtained personal information about themselves (e.g., names of family members, pets, birthdays, anniversaries, or hobbies).

1.16.3. Three consecutive characters (e.g., AAA).

1.17. Choose passwords used to participate in [the EHR Solution] that are easy to remember but hard to guess by someone else.

1.18. Never change passwords used to participate in [the EHR Solution] in an easily recognized pattern (e.g., changing “IL0v3EatingP!zza1” to “IL0v3EatingP!zza2”).

1.19. Ensure their passwords used to participate in [the EHR Solution] are different from their password(s) used to access other accounts (e.g., corporate email account, personal banking, etc.).

1.20. Commit passwords used to participate in [the EHR Solution] to memory. All persons must avoid keeping a record of their passwords (e.g., on paper, or stored on in a file), unless it:

1.20.1.1. Can be stored securely, and

1.20.1.2. Does not indicate the associated ID or that it is for [the EHR Solution].

1.21. Keep their passwords used to participate in [the EHR Solution] a secret, never telling anyone their password, including a system administrator, help desk personnel or a manager.

1.22. Immediately change their password used to participate in [the EHR Solution] if they suspect or confirm that their password has been disclosed or compromised and notify their information security incident initial point of contact (e.g., a helpdesk or Privacy Officer) of the security incident, see "Reporting Information Security Incidents Related to [the EHR Solution] below.

1.23. Not include their ID or password used to participate in [the EHR Solution] in any automated single sign-on process (SSO) (e.g., stored in a macro or function key) except [EHR Solution] approved SSO management systems.

1.24. Always change any password used to participate in [the EHR Solution] that is provided to them at initial login and as directed by their Identity Provider.

Working Remotely

All persons must:

1.25. Use a [the EHR Solution] or HIC-approved remote access solution (e.g., through a virtual private network or terminal services) to remotely participate in [the EHR Solution].

1.26. Follow the proper procedures to disconnect from a remote access connection used to participate in [the EHR Solution] (e.g., if the remote access solution has a disconnect option, use this option to disconnect rather than simply closing the application).

1.27. Never participate in [the EHR Solution] in an area where unauthorized individuals can view the information (e.g., Internet cafés, public transit, and other non-private settings).

1.28. Never leave their mobile computing device that has the ability to participate in [the EHR Solution] unattended in a public place.

1.29. When required to leave their mobile computing device in a vehicle, all persons must place it out of view and lock the vehicle.

1.30. Ensure that if personal health or personal information is downloaded onto a mobile device from [the EHR Solution], the location where the data is stored is encrypted or the end-user tool utilizes full disk encryption. Full disk encryption is the preferred option on mobile devices; however, containerized implementations of encryption on shared personal and corporate devices are also acceptable.

Reporting Information Security Incidents Related to [the EHR Solution]

All persons must:

1.31. Immediately report suspected or confirmed information security incidents related to [the EHR Solution] to their information security incident initial point of contact (e.g., a help desk or Privacy Officer). Alternatively, HICs may instruct agents to report the incident to their manager or supervisor, who in turn must report it to the information security incident initial point of contact.

Examples of information security incidents include, but are not limited to:

- Unauthorized disclosure of PHI.
- Theft or loss of information technology that contains PHI or has access to [the EHR Solution] even if it is encrypted.
- Virus or malware infection on a device that has access to [the EHR Solution].
- Attempts (either failed or successful) to gain unauthorized access to [the EHR Solution].
- Compromised password, i.e., another individual knows your password that is used to access [the EHR Solution].

1.32. Provide their full cooperation to [the EHR Solution] Program Office, their agents or Electronic Service Providers with any information security incident investigation.

2. Agents and Electronic Service Providers of [the EHR Solution]

Agents and Electronic Service Providers of [the EHR Solution] ("all persons") must:

2.1 Always use their assigned ID and password to participate in [the EHR Solution].

2.2 Never allow another person to use their ID to participate in [the EHR Solution]. All persons are accountable for any actions performed with their ID on [the EHR Solution].

2.3 Never participate in [the EHR Solution] unless their role requires them to do so, they are expressly authorized to do so, it is necessary to do so (e.g., providing or assisting in the provision of healthcare), and in accordance with [the EHR Solution]'s privacy policies.

2.4 Never disable or override any information security controls (e.g., disabling anti-virus protection on their workstation).

2.5 Only use tools and processes [the EHR Solution] approves and endorses to participate in [the EHR Solution].

2.6 Never attempt to exploit any suspected security weakness, even to explore that such a weakness may exist, unless it is part of their assigned job duties or responsibilities and they are explicitly authorized by [the EHR Solution] Program Office to do so.

2.7 Never knowingly perform an act that will interfere with the normal operations of [the EHR Solution], or try to disrupt [the EHR Solution] by either intentionally making such services unavailable or by affecting the integrity of the data being stored in or processed by [the EHR Solution].

2.8 Abide by the terms and conditions of [the EHR Solution] provided.

Protecting PHI

All persons must:

2.9 Never discuss PHI with any person that does not have a need-to-know or is not authorized to know the information.

2.10 Never discuss PHI in public areas, including elevators, as it may be easily overheard by those who do not have a need-to-know.

2.11 Lock up PHI in any form (e.g., locking paper, printed copies originating from the [EHR Solution] or portable storage media in a cabinet) when left unattended in an unsecured area, especially when the office or area is vacated.

2.12 Always log-off or lock unattended computers or workstations to prevent unauthorized individuals from accessing PHI.

2.13 Only store PHI on [the EHR Solution]-approved devices or storage networks, and only store the minimal amount of PHI necessary on any encrypted portable storage media.

2.14 Always ensure that paper documents containing PHI are shredded or placed in a secure shredding receptacle when they are no longer needed.

2.15 Follow internal procedures for the proper secure disposal of any information technology that may have PHI stored on it.

Emailing PHI

All persons must:

2.16 Only email PHI when it is necessary for the purposes of providing or assisting in the provision of health care or [the EHR Solution] business, and is acceptable under [the EHR Solution]'s policies or procedures.

2.17 Encrypt all emails that contain PHI, use a secure file transfer solution or use a secure email system approved by [the EHR Solution].

2.18 Never use external email accounts (e.g., Hotmail, or Gmail) to send or receive PHI.

Creating and Protecting Passwords

All persons should:

2.19 Where possible, use phrases (e.g., IL0v3EatingP!zza) when creating passwords.

All persons must:

2.20 Always create passwords used to participate in [the EHR Solution] that are at least eight characters, with a maximum not less than 64 characters long, and include at least three of the following conditions of complexity:

2.20.1 One number

2.20.2 One uppercase letter

2.20.3 One lowercase letter, or

2.20.4 One special 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.

2.21 Never create passwords that include:

2.21.1 All or part of their ID.

2.21.2 Easily obtained personal information about themselves (e.g., names of family members, pets, birthdays, anniversaries, hobbies).

2.21.3 Three consecutive characters (e.g., AAA).

2.22 Choose passwords that are easy to remember but hard to guess by someone else.

2.23 Never change passwords in an easily recognized pattern (e.g., changing "IL0v3EatingP!zza1" to "IL0v3EatingP!zza2").

2.24 Ensure that their passwords used to participate in [the EHR Solution] are different from their password(s) used to access other accounts (e.g., corporate e-mail account, personal banking, etc.).

2.25 Commit their passwords to memory. All persons must avoid keeping a record of their passwords (e.g., on paper, or stored on in a file), unless it:

2.25.1 Can be stored securely, and

2.25.2 Does not indicate the ID, information system or information technology for which the ID is associated.

2.26 Keep their passwords a secret, never telling anyone their password, including a system administrator, help desk personnel, or a manager.

2.27 Change their password immediately if they suspect or confirm that their password has been disclosed or compromised.

2.28 Not include their ID or password in any automated sign-on process (e.g., stored in a macro or function key).

2.29 Always change passwords that are provided to them at initial login.

Working Remotely

All persons must:

2.30 Use a [the EHR Solution] approved remote access solution (e.g., through a virtual private network or terminal services) to remotely participate in [the EHR Solution].

2.31 Follow the proper procedures to disconnect from remote access (e.g., if the remote access solution has a disconnect option, use this option to disconnect rather than simply closing the application).

2.32 Never access [the EHR Solution] in an area where unauthorized individuals can view the information (e.g., Internet cafés, public transit, and other non-private settings).

2.33 Never leave their mobile computing device that has the ability to access [the EHR Solution] unattended in a public place.

When required to leave their mobile computing device in a vehicle, all persons must place it out of view and lock the vehicle.

Reporting Information Security Incidents

All persons must:

2.34 Immediately report suspected or confirmed information security incidents to [the EHR Solution] information security incident initial point of contact (e.g., a help desk). Alternatively, agents may report the incident to their manager or supervisor, who in turn must report it to the information security incident's initial point of contact.

Examples of information security incidents include, but are not limited to:

- Unauthorized disclosure of PHI
- Theft or loss of information technology that contains PHI even if it is encrypted
- Virus or malware infection on a device that has access to [the EHR Solution]
- Attempts (either failed or successful) to gain unauthorized access to [the EHR Solution]
- Compromised password, i.e., another individual knows your password

2.35 Provide their full cooperation to [the EHR Solution] Program Office, their agents or Electronic Service Providers with any information security incident investigation.

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 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