Ontario Health

Security Logging and Monitoring Standard

Version: 2.0

Document ID: 3542

Copyright Notice

All rights reserved

Trademarks

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	2017-03-20
Connecting Security Committee	2018-03-26
Connecting Security Committee	2021-03-18

Revision History

VERSION NO.	DATE	SUMMARY OF CHANGE	CHANGED BY
1.1	2014-10-09	Revised based on feedback from cGTA, cSWO, and eHealth Privacy. Aligned scope, enforcement and exemption sections to CPC policy. Clarified distinction between security and privacy policies (system vs. application), deleted 1.24 related to retention as it was ambiguous and a duplicate of 1.23.	Mark Carter
1.2	2014-10-17	Revised based on Oct 15th CSC Meeting. 1.23, created a reference to the IDP and CPC Retention policies. Updated Appendix A to note content required in IDP Services and Data Contribution Endpoints.	Mark Carter
1.3	2014-10-28	Revised based on feedback from cNEO and discussions with membership.	Mark Carter
1.4	2014-11-26	Revised based on Nov 26th CSC meeting. Update to 1.20 to require review of logs on a quarterly basis. References to specific retention periods removed and pointed to the CPC Retention Policy. Policy approved at the meeting.	Mark Carter
1.5	2015-01-21	Aligned name of access control policy based on final wave 3 decision.	Mark Carter
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	2017-03-20	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

VERSION NO.	DATE	SUMMARY OF CHANGE	CHANGED BY
1.8	2018-03-16	Updated standard to include Patient access to the EHR.	Geovanny Diaz
1.9	2020-03-26	Updated standard to use new Ontario Health Template with minor control revisions.	Paul Cnudde
2.0	2021-01-21	Review of the document with minor changes, updated references and the review cycle to biennially.	Ana Fukushima

Security Logging and Monitoring Standard

Purpose

To define security logging and monitoring requirements for system level events and activities of [the EHR Solution] and HIC's identity provider technology, data contribution endpoints and supporting infrastructure.

Scope

This standard applies to [the EHR Solution] Program and [the EHR Solution], including all Patient Portals/Applications for system level logging as defined in Appendix A: Sources and Contents of Logs.

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:
  - The HIC's local access control and identity management infrastructure ("identity provider services") that manages the authentication and authorization used to provide 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)

- **Ontario Health'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 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)

Refer to the Connecting Privacy Committee (CPC) Logging and Auditing policy when applying in logging, auditing and monitoring of all instances where:

- All or part of the personal health information (PHI) in [the EHR Solution] is viewed, handled or otherwise dealt with;

- All or part of the PHI in [the EHR Solution]] is transferred to a health information custodian (HIC);
- All or part of the PHI in [the EHR Solution] is disclosed to and collected by a HIC as a result of an override of a Consent Directive; and
- A Consent Directive is made, modified or withdrawn in [the EHR Solution].

This standard does not apply to any HIC, their agents or their Electronic Service Providers who do not view, create, contribute or have access to [the EHR Solution].

Definitions

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.

Audit trail: A chronological set of logs of information system activities or the activities of a HIC, agent, or Electronic Service Provider. These logs can be used to reconstruct past events and track the activities that took place, and possibly detect and identify intruders.

Auditing: The practice of inspecting logs for the purpose of:

- Verifying activity performed on an information system or network by any agent or Electronic Service Provider of [the EHR Solution], or a HIC, their agents or Electronic Service Providers
- Verifying that an information system is in a desirable state
- Answering questions about how an information system arrived at a particular state

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 Engines, etc.) that directly connects to [the EHR Solution] to provide clinical data.

[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.

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.

Log: A record of the events occurring within [the EHR Solution] or a HIC's information systems and networks.

Logging: The process of recording a pre-defined set of HIC, agent or Electronic Service Provider or information system or network activities. The automated logging processes serve as the basis for establishing audit trails for activities and events on an information system.

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

Monitoring: The process of observing, supervising, or controlling information system or network activities on a continuous basis.

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.

Standard Requirements

1. Requirements for Health Information Custodians

1.1. HICs must log all HIC, agent, and Electronic Service Provider participation in the [the EHR Solution], and must log system events/activities on their local identity provider technology and data contribution endpoints. See Appendix A, Sources of Contents of Logs.

1.2. HICs should classify and protect logs in accordance with the highest level of information contained within the data contributor endpoint and identity provider service logs.

Log Generation

1.3. HICs must log all activities of administrators and operators on their identity provider services and their data contribution endpoints as part of the general audit trail process.

1.4. HICs must ensure that data contributor and identity provider services system logs, at a minimum and where relevant, contain the following information for each event/activity, consult the Identity Provider Standard for more specific logging requirements of the Identity Provider Service functions (e.g. registration, authentication):

1.4.1. Identifiers (as many as available) for the subject requesting the action (e.g., user ID, computer name, IP address, and MAC address).

1.4.2. Identifiers (as many as available) for the object the action was performed on (e.g., file names accessed, unique identifiers of records accessed in a database, IP address, and MAC address).

1.4.3. Date and time.

1.4.4. The event activity (e.g., sign-on and sign-off).

1.4.5. Status of the security event activity (e.g., success or failure, denied or allowed).

1.4.6. Type of access (e.g., read, write, execute).

1.4.7. Alarms raised by access control and network monitoring systems.

1.5. HICs must not filter their data contribution endpoint and identity provider service logs at the source.

1.6. HICs must synchronize their system clocks on their identity provider technology and data contribution endpoints to a centralized clock source. HICs must perform clock synchronization validation, at a minimum, daily to ensure on-going clock synchronization accuracy.

Protection of Logs

1.7. HICs must implement controls to protect the confidentiality and integrity of all local identity provider technology and data contribution endpoints logs both in storage and during transmission.

1.8. HICs must secure all access to local identity provider technology and data contribution endpoints logs.

1.9. HICs should maintain a list of all agents or Electronic Service Providers who have authorized access to identity provider technology and data contribution endpoints logs. The list should contain:

1.9.1. Full name of the agent or Electronic Service Provider.

1.9.2. ID that the agent or Electronic Service Provider uses to logically access the log.

1.9.3. Name/type of log to which the agent or Electronic Service Provider has access.

1.10. HICs should not configure local identity provider technology and data contribution endpoints logs to overwrite old data when the maximum log size limit has been reached.

1.11. HICs must prohibit their agents and Electronic Service Providers with authorized access to local identity provider technology and data contribution endpoints logs from erasing or deactivating logs of their own activities.

1.12. HICs must ensure that the management of their identity provider technology and data contribution endpoints log generation sources is logged and controlled via documented change control policies and procedures.

Monitoring and Log Analysis

1.13. HICs should implement automated mechanisms on their local identity provider technology and data contribution endpoints to consolidate logs to centralized log management servers.

1.14. HICs should implement automated tools on their respective information systems to convert local identity provider technology and data contribution endpoints logs with different content and formats to a single standard format with consistent data field representations.

1.15. HICs should monitor their local identity provider technology and data contribution endpoints logs to ensure that:

1.15.1. Log triggers are appropriately configured.

1.15.2. Log triggers are not compromised.

1.15.3. Faults are identified for further analysis and remediation steps

1.15.4. Identified faults are resolved or mitigated.

1.16. HICs must be able to correlate their logs from their local identity provider technology and data contribution endpoints to assist in the detection and prevention of information and information system misuse or intrusion.

1.17. HICs should implement automated correlation tools to look for patterns of events/activities across their local identity provider technology and data contribution endpoints logs.

1.18. HICs should review their identity provider technology and data contribution endpoints logs, at a minimum, monthly.

1.19. HICs should ensure that the logs of administrators and operators who support their local identity provider technology and data contribution endpoints are reviewed, at a minimum, quarterly.

1.20. Segregation of duties should exist for identity provider technology and data contribution endpoints log reviews, e.g., someone other than the administrator should review the logs for the systems he/she manages.

Log Retention and Storage

1.21. HICs should ensure that their logs relating to the data contribution endpoints and identity provider services are readily available online, at a minimum for the duration indicated in the Federation Identity Provider Standard and CPC Retention Policy. Logs must be available to facilitate investigations in a timely manner in accordance with the standard.

1.22. HICs must retain archived identity provider services and data contribution endpoints system logs for a minimum duration indicated in the Federation Identity Provider Standard and CPC Retention Policy whether the service is performed by the HIC, an agent or Electronic Service Provider.

1.23. HICs must archive their data contributor endpoint and identity provider service logs in a format that can be restored for as long as the data retention is required.

1.24. HICs should label and store their data contributor and identity provider services archive logs in an organized manner for easy retrieval.

2. Requirements for [the EHR Solution]

2.1. The EHR Solution] Program must log all information system events/activities on the [EHR Solution] found in Appendix A: Sources and Contents of Logs performed by Patients, HICs, Agent, and Electronic Service Provider with access to [the EHR Solution].

2.2. [The EHR Solution] Program must ensure that their logging capabilities are enabled and operational at all times. [The EHR Solution] Program must configure their information systems in a manner such that they are disabled if logging is not operational.

2.3. [The EHR Solution] Program must ensure that all logs are classified in accordance with the highest level of information contained within the logs.

Log Generation

2.4. [The EHR Solution] Program must log all activities of their information system administrators and information system operators as part of the general audit trail process.

2.5. [The EHR Solution] Program must ensure that all logs, at a minimum and where relevant, contain the following information for each event/activity:

2.5.1. Identifiers (as many as available) for the subject requesting the action (e.g., user ID, computer name, IP address, and MAC address).

2.5.2. Identifiers (as many as available) for the object the action was performed on (e.g., file names accessed, unique identifiers of records accessed in a database, IP address, and MAC address).

2.5.3. Date and time.

2.5.4. The event activity (e.g., sign-on and sign-off).

2.5.5. Status of the security event activity (e.g., success or failure, denied or allowed).

2.5.6. Type of access (e.g., read, write, execute).

2.5.7. Alarms raised by access control and network monitoring systems.

2.6. [The EHR Solution] Program must not filter logs at the source.

2.7. [The EHR Solution] Program must synchronize their information system clocks to a centralized clock source. [The EHR Solution] Program must perform clock synchronization validation, at a minimum, daily to ensure on-going clock synchronization accuracy.

Protection of Logs

2.8. [The EHR Solution] Program must implement controls to protect the confidentiality and integrity of logs both in storage and during transmission.

2.9. [The EHR Solution] Program must restrict all access to logs based on the principles of least privileged and need-to-know.

2.10. [The EHR Solution] Program must maintain a list of all agents or Electronic Service Providers who have authorized access to logs. At a minimum, the list must contain:

2.10.1. Full name of the agent or Electronic Service Provider.

2.10.2. Work phone number of the agent or Electronic Service Provider.

2.10.3. Work email address of the agent or Electronic Service Provider.

2.10.4. ID that the agent or Electronic Service Provider uses to logically access the log.

2.10.5. Name/type of log to which the agent or Electronic Service Provider has access.

2.11. [The EHR Solution] Program must not configure logs to overwrite old data when the maximum log size limit has been reached.

2.12. [The EHR Solution] Program must prohibit their agents and Electronic Service Providers with authorized access to logs from erasing or deactivating logs of their own activities.

2.13. [The EHR Solution] Program must ensure that the management of log generation sources is logged and controlled via documented change control procedures.

Monitoring and Log Analysis

2.14. [The EHR Solution] Program should implement automated mechanisms on their information systems to consolidate logs to centralized log management servers.

2.15. [The EHR Solution] Program should implement automated tools on their information systems to convert logs with different content and formats to a single standard format with consistent data field representations.

2.16. [The EHR Solution] Program must monitor their logs to ensure that:

2.16.1. Log triggers are appropriately configured.

2.16.2. Log triggers are not compromised.

2.16.3. Faults are identified for further analysis and remediation steps.

2.16.4. Identified faults are resolved or mitigated.

2.17. [The EHR Solution] Program should implement automated analysis tools on their information systems to assist in the detection and prevention of information and information system misuse or intrusion.

2.18. [The EHR Solution] Program should implement automated correlation tools on their information systems to look for patterns of events/activities across multiple information systems.

2.19. [The EHR Solution] Program must ensure that automated alerts are triggered for unsuccessful authentication attempts.

2.20. [The EHR Solution] Program must review their logs, at a minimum, monthly to detect anomalous events on the network or [The EHR Solution] agent or Electronic Service Provider behavior that is outside of standard or procedures, or to identify automated alerts generated that may indicate attacks or break-ins.

2.21. [The EHR Solution] Program must ensure that information system administrator and operator logs are reviewed, at a minimum, monthly.

2.22. [The EHR Solution] Program must ensure that segregation of duties must exist for all log reviews, e.g., someone other than the information system administrator must review the logs for the information system he/she manages.

Log Retention and Storage

2.23. [The EHR Solution] Program must ensure that their logs relating to production data are readily available online, at a minimum, for six months.

2.24. [The EHR Solution] Program must retain archived information system logs for a minimum duration as highlighted in the CPC Retention Policy.

2.25. [The EHR Solution] Program must retain archived logs of Patient, HIC, Agent, and Electronic Service Provider activities in accordance with [the EHR Solution] Retention Policy.

2.26. [The EHR Solution] Program must ensure that logs related to backups are readily available online for the same period as logs related to production data.

2.27. [The EHR Solution] Program must archive their logs in a format that can be restored for as long as the data retention is required.

2.28. [The EHR Solution] Program should label and store their archive logs in an organized manner for easy retrieval.

2.29. Upon retention expiry, [the EHR Solution] Program must ensure that their logs are disposed of in accordance with the requirements defined in Information and Asset Management Standard.

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 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

Appendix A: Sources and Contents of Logs

System/Software	Event/Activity to be Recorded
Anti-malware software (such as anti-virus, anti-spyware and root kit detectors)	• Instances of detected malware • File and information system disinfection attempts • File quarantines • Malware scans • Signature or software updates
Intrusion detection and intrusion prevention systems	• Suspicious behaviour • Detected attacks • Actions performed to stop malicious activity
Remote access and wireless access systems	• Login attempts • Amount of data sent and received during session
Web proxies and content filters	• URLs accessed • URLs blocked • Files Transferred
Vulnerability Management Software (includes patch management and vulnerability assessment software)	• Patch installation history • Vulnerability status • Known vulnerabilities • Missing software updates
Authentication Servers (includes directory servers and single sign-on servers)	• Authentication attempts
Routers and switches	• Blocked Activity
Firewalls	• Detailed logs of network activity
Network Access Control	• Status of host security checks • Quarantined hosts and reason
Identity Provider Services	• Reference the Log Generation section of this Security Logging and Monitoring standard and the Federation Identity Provider Standard.
Data Contribution End Points	• Reference the Log Generation section of this Security Logging and Monitoring standard.
Operating System (such as those for servers, workstations and networking devices (e.g., routers, switches))	• System Events ○ System shut down ○ Service starting • Security Events ○ File accesses ○ Policy changes ○ Account changes

System/Software	Event/Activity to be Recorded	
Applications (e.g., e-mail servers and clients, Web servers and browsers, file servers and file sharing clients, database servers etc.) * Note – Refer to the CPC Logging and Auditing Policy for requirements for Application (PHI) level logging and auditing requirements.	• Client requests and server response • Authentication attempts • Account changes • Use of privileges • Number and size of transactions • Operational events o Startup and shutdown	• Configuration changes • Application-specific events such as: o Email sends and receipts o File access o Service request o System level transactions o Function performed (such as read, write, modify, delete)
Mobile Application Logs	• Mobile application input/output validation failures • Authentication successes and failures • Authorization (access control) failures; session management failures • Use of higher-risk functionality (e.g. insecure network connections; application errors and system events; legal and other opt-ins)	