Ontario Health

Information Security Incident Management Standard

Version: 1.8

Document ID: 3539

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	2014-09-09
Connecting Security Committee	2018-03-26
Connecting Security Committee	2021-03-18

Revision History

VERSION NO.	DATE	SUMMARY OF CHANGE	CHANGED BY
1.0	2013-12-23	Nov 2013 version adopted from the cGTA PSWG	Mark Carter
1.1	2014-08-18	Updates based on CSC Member feedback. Revised scope to include view, handle or otherwise deal with PHI. Revised references to the Participation Agreement, aligned 1.6 and 2.6 to use terms from sections in the policy, update to 1.10 on communication options, added to 1.12 to broaden the responsibilities to report to the PSC, added in 1.17 the option to request periodic updates, added to 1.20 and 2.24 the requirement to have incidents reports presented to the PSC, aligned Exemption and Enforcement language.	Mark Carter
1.2	2014-09-09	Policy approved at the CSC meeting September 9th 2014	Mark Carter
1.3	2015-01-21	Aligned name of access control policy based on final wave 3 CSC decision.	Mark Carter
1.4	2015-10-19	Updated policies to note the change in governance. The Steering Committee was replaced by the Applicable Oversight Body. Responsibilities to review incident reports have been transferred to the Connecting Security Committee from the regional PSC.	Mark Carter
1.5	2017-03-20	Updated Standard to align with ITSM. The document title was changed from Policy to Standard. EHR Solution definition was updated. Revised controls based on feedback.	Raviteja Addepalli
1.6	2018-03-16	Updated standard to include Patient access to the EHR.	Geovanny Diaz
1.7	2020-03-30	Updated to use new template and minor revisions for clarity.	Paul Cnudde

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

Information Security Incident Management Standard

Purpose

To define the requirements for creating an information security incident ("incident") management process.

Scope

This standard only applies to incidents related to [the EHR Solution] Program or [the EHR Solution], including all Patient Portals/Applications. For health information custodians (HICs) that use [the EHR Solution] to view, handle or otherwise deal with Personal Health Information (PHI) by provisioning access through:

- **Local identity provider technology** (local IdP), this standard applies to incidents related to:
    - End-user devices that are used to access [the EHR Solution] including the applicable administrative functionality (consent management, reporting, etc.)
    - 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 incidents related to:
    - End-user devices used to access [the EHR Solution], including the administrative functionality (consent management, reporting, etc.)
    - 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 incidents related to:

- The data contribution endpoints that provide PHI to [the EHR Solution]'s Clinical Data Repository (CDR)
- The information technology and processes that ensure the quality of the data submitted (e.g., terminology mapping)

This standard does not apply to the handling of internal HIC incidents that do not impact [the EHR Solution] Program or [the EHR Solution], or to any HIC, their agents or their Electronic Service Providers who do not view, create, or contribute PHI 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.

[The EHR Solution] Information Security Lead: [The EHR Solution] Information Security Lead is an agent of [the EHR Solution] who acts as the single point of contact for information security decisions related to [the EHR Solution].

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 in the Information Security Policy.

Connecting Security Committee (CSC): The provincial security forum consisting of senior security representatives from across the regions and Ontario Health. This is a decision making body responsible for establishing a functional and usable information security governance framework for participating organizations in the EHR.

Data Contribution End Point(s): Technology and related processes that provide data to the Clinical Data Repository or are queried to provide data to a Clinical Viewer. Typically, these systems are the Information System (e.g. Hospital Information System, Laboratory Information System, Clinical Information System, etc.) that directly connects to [the EHR Solution] to provide clinical data.

Electronic Service Provider: A person who 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 security incident: Any violation or imminent threat of violation of information security policies, standards, procedures or practices or any information security event that may compromise operations or threaten the security of an information system or business process.

Information system: A discrete set of information technology organized for the retention, collection, processing, maintenance, use, disclosure, or disposition of information.

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

Privacy Breach: A privacy breach includes circumstances where:

- A provision of the Personal Health Information Protection Act, 2004 (PHIPA) or its regulations has been or is about to be contravened;
- The privacy provisions of the [Applicable Agreements] or any other agreement in respect of [the EHR Solution]have been or are about to be contravened;
- The privacy policies, procedures and practices implemented in respect of [the EHR Solution]have been or are about to be contravened;
- Personal health information (PHI) in [the EHR Solution] is lost or stolen or has been or is about to be accessed by an unauthorized person; or
- Records of PHI in [the EHR Solution] have been or are about to be copied, modified or disposed of in an unauthorized manner.

Shall/Must: Used for absolute requirements, i.e., they are not optional.

Should: Used when valid reasons exist in certain circumstances not to implement the requirement; however, the implementer must understand the implications before choosing a different course and must consider implementing compensating controls.

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

Standard Requirements

1. Requirements for Health Information Custodians

1.1. HICs must implement an information security incident ("incident") management process that covers all phases of the incident management process to deal with incidents related to [the EHR Solution]:

- Identification/Triage
- Response
- Recovery
- Follow-up

1.2. If at any point in the incident management process a HIC realizes that the incident has resulted in a privacy breach, then the incident must be handled in accordance with the Privacy Breach Management Policy.

Identification/Triage

1.3. HICs must establish a point of contact to whom actual or suspected incidents related to [the EHR Solution] are reported. Most often, the point of contact is a service desk.

1.4. HICs must ensure that their agents and Electronic Service Providers are aware of their responsibility to immediately report actual or suspected incidents to the established point of contact.

1.5. The point of contact must generate an incident ticket or log for all reported incidents related to [the EHR Solution]. At a minimum, the incident ticket must contain the following elements:

1.5.1. The time and date of the reported incident.

1.5.2. The name and contact information of the agent or Electronic Service Provider that reported the incident.

1.5.3. Details about the reported incident (e.g., type and how it was detected).

1.5.4. Any impacts of the reported incident.

1.5.5. Any actions that are undertaken to contain the incident either by the agent or Electronic Service Provider that reported the incident or the point of contact.

1.6. HICs must appoint an incident response lead or team who is responsible for initiating the triage, response, recovery, and follow-up activities for incidents related to [the EHR Solution]. The incident response lead or team may be the same as the point of contact.

1.7. The point of contact must send all incident tickets related to [the EHR Solution] to the incident response lead or team to review the incident ticket and any supporting information to verify whether or not an incident has occurred.

1.8. The incident response lead or team must classify all actual incidents related to [the EHR Solution] according to severity (See Appendix A: Incident Severity and Priority Ratings for severity ratings).

1.9. The incident response lead or team must initiate an incident report related to [the EHR Solution]. (See Appendix B: Incident Report Details)

1.10. HICs must ensure that their incident management process requires the incident response lead or team to notify [the EHR Solution] Program Office Privacy and Security Team by email or telephone and any affected HICs by the end of the next business day of confirmed incidents that are classified as Severity 1 or Severity 2 according to *Appendix A: Incident Severity and Priority Ratings.*

At a minimum, the notification must contain the following elements:

1.10.1. The time and date of the reported incident.

1.10.2. The name and contact information of the agent or Electronic Service Provider that reported the incident.

1.10.3. Details about the reported incident (e.g., type and how it was detected).

1.10.4. Any known or suspected impacts of the reported incident.

1.10.5. Any actions that are undertaken to contain the incident either by the agent or Electronic Service Provider that reported the incident, the point of contact, or the incident response lead or team.

1.11. If an incident that originates at a HIC affects multiple HICs or [the EHR Solution], HICs must allow [the EHR Solution] Program Office to assume leadership of incident management activities if requested.

1.12. The team that leads the incident management activities (i.e. HIC or [the EHR Solution] Program Office) must notify Ontario Health who will notify the Connecting Security Committee and Applicable Oversight Body:

1.12.1. Within 72 hours of notification for any incident related to [the EHR Solution] and classified as a Severity 1; or

1.12.2. Within one week of notification for any incident related to [the EHR Solution] and classified as a Severity 2.

1.13. HICs should prioritize incidents related to [the EHR Solution] in accordance with their severity rating.

Response

1.14. The incident response lead or team must take steps to limit the scope and magnitude of an incident. Mitigation or containment activities may include:

1.14.1. Backing up the information system;

1.14.2. Discontinuing operations;

1.14.3. Changing passwords or modifying access control lists on the compromised information system; or

1.14.4. Restricting connectivity.

NOTE: Depending on the severity of an incident it may be necessary to activate the organization's business continuity plans.

Recovery

1.15. HICs must remediate affected information systems so that they return to full and normal operations. Remediation activities may include:

1.15.1. Eradicating the cause of the incident (e.g., removing malware).

1.15.2. Restoring and validating the information system.

1.15.3. Deciding when to restore operations.

1.15.4. Monitoring information systems to verify normal operations without further information system or data compromise.

Follow-up

1.16. HICs must investigate incidents related to [the EHR Solution] to identify the cause of the incident (e.g., by performing a root causes analysis).

1.17. Once an incident related to [the EHR Solution] has been resolved (i.e., all remediation activities have been implemented and affected information systems and information technology have returned to full and normal operations), the incident response lead or team must complete the incident report. During longer investigations led by HICs, [the EHR Solution] Program Office or affected HICs may request status updates on the incident investigation in the interim.

1.18. HICs must archive their incident reports related to [the EHR Solution] for a minimum of 24 months.

1.19. HICs must provide [the EHR Solution] Program Office and impacted HICs with an incident report related to [the EHR Solution] within 72 hours of the incident report being requested.

1.20. The final incident reports should be reviewed by the Connecting Security Committee and if necessary the Applicable Oversight Body. Ontario Health will facilitate this review when the report is submitted by the HIC.

1.21. HICs should implement a mechanism to review their incidents related to [the EHR Solution], at a minimum, monthly to identify trends and to determine whether any preventative actions can be taken to reduce the likelihood of similar incidents from occurring in the future.

Evidence Gathering

1.22. HICs should develop procedures for collecting evidence for the purposes of disciplinarily or legal action against agents or Electronic Service Providers. These procedures should require:

1.22.1. Forensics work to be performed on copies of the evidential material.

1.22.2. The creation of copies be witnessed

1.22.3. Details of the creation should be logged, including:

1.22.3.1. When and where the copying process was executed;

1.22.3.2. Who performed the copying activities; and

1.22.3.3. Which tools or programs were utilized for the copying process.

1.22.4. The integrity of all evidential material is protected.

2. Requirements for [the EHR Solution]

2.1. [The EHR Solution] Program Office must implement an information security incident ("incident") management process that covers all phases of the incident management process:

- Identification/Triage
- Response
- Recovery
- Follow-up

2.2. If at any point in the incident management process [the EHR Solution] Program realizes that the incident has resulted in a privacy breach, the incident must be handled in accordance with the Privacy Breach Management Policy.

Identification/Triage

2.3. [The EHR Solution] Program must establish a point of contact to whom actual or suspected incidents are reported. Most often, the point of contact is a service desk.

2.4. [The EHR Solution] Program must ensure that all its agents and Electronic Service Providers are aware of their responsibility to immediately report actual or suspected incidents to the established point of Contact.

2.5. The point of contact must generate an incident ticket for all reported incidents. An automated incident management system is recommended to support the recording of incidents. The incident ticket must contain the following elements:

2.5.1. The time and date of the reported incident.

2.5.2. The name and contact information of the patient, HIC, Agent or Electronic Service Provider that reported the incident.

2.5.3. Details about the reported incident, (e.g., type and how it was detected).

2.5.4. Any impacts of the reported incident.

2.5.5. Any actions that are undertaken to contain the incident either by the agent or Electronic Service Provider that reported the incident or the point of contact.

2.6. [The EHR Solution] Program must appoint an incident response lead or team who is responsible for initiating the triage, response, recovery and follow-up activities for all incidents. The incident response lead or team may be the same as the point of contact.

2.7. The point of contact must immediately send all incident tickets to the incident response lead or team.

2.8. The incident response lead or team must review the incident ticket and any supporting information to verify whether or not an incident has occurred.

2.9. The incident response lead or team must classify all actual incidents according to severity (See Appendix A: Incident Severity and Priority Ratings for severity ratings).

2.10. The incident response lead or team must initiate an incident report. (See Appendix B: Incident Report Details)

2.11. All completed or partially completed incident reports must be handled, at a minimum, in accordance with the protection requirements for information classified as Confidential.

2.12. If an incident that originates at a HIC affects multiple HICs or [the EHR Solution], [the EHR Solution] Program Office may assume leadership of the incident management activities.

2.13. [The EHR Solution] Program Office must ensure that their incident management process requires the incident response lead or team to notify any affected HICs and/or Ontario Health by email by the end of the next business day of any incident that [the EHR Solution] Program classifies as a Severity 1 or Severity 2.

At a minimum, the notification must contain the following elements:

2.13.1. The time and date of the reported incident.

2.13.2. The name and contact information of the agent or Electronic Service Provider that reported the incident.

2.13.3. Details about the reported incident (e.g., type and how it was detected).

2.13.4. Any impacts of the reported incident.

2.13.5. Any actions that are undertaken to contain the incident either by the agent or Electronic Service Provider that reported the incident, the point of contact, or the incident response lead or team.

2.14. [The EHR Solution] Program Office must notify Ontario Health (who will notify the Connecting Security Committee and the Applicable Oversight Body):

2.14.1. Within 72 hours of notification for any incident classified as a Severity 1.

2.14.2. Within one week of notification for any incident classified as a Severity 2.

2.15. [The EHR Solution] Program Office must prioritize all incidents in accordance with their severity and priority rating.

Response

2.16. The incident response lead or team must take steps to limit the scope and magnitude of an incident. Mitigation or containment activities may include:

2.16.1. Backing up the information system.

2.16.2. Discontinuing operations.

2.16.3. Changing passwords or modifying access control lists on the compromised information system.

2.16.4. Restricting connectivity.

NOTE: Depending on the severity of an incident it may be necessary to activate [the EHR Solution] Program's business continuity plans.

2.17. [The EHR Solution] Program Office should create containment strategies for each major incident type, with criteria clearly documented to facilitate decision-making. Criteria for determining the appropriate strategy may include:

2.17.1. Potential damage to and theft of resources.

2.17.2. Need for evidence preservation.

2.17.3. Service availability (e.g., network connectivity, services provided to external parties).

2.17.4. Time and resources needed to implement the strategy.

2.17.5. Effectiveness of the strategy (e.g., partial containment, full containment).

2.17.6. Duration of the solution (e.g., emergency workaround to be removed in four hours, temporary workaround to be removed in two weeks, permanent solution).

NOTE: Depending on the severity and type of an incident, it may be necessary to activate [the EHR Solution] Program's business continuity plans; therefore, criteria should be defined to provide the incident response lead or team with guidance on when to notify business continuity personnel.

Recovery

2.18. [The EHR Solution] Program must remediate all applicable information systems so that they return to full and normal operations. Remediation activities may include:

2.18.1. Eradicating the cause of the incident (e.g., removing malware).

2.18.2. Restoring and validating the information system.

2.18.3. Deciding when to restore operations.

2.18.4. Monitoring information systems to verify normal operations without further information system or data compromise.

Follow-up

2.19. [The EHR Solution]Program Office must investigate all incidents to identify the cause of the incident (e.g., by performing root cause analysis).

2.20. Once an incident has been resolved (i.e., all remediation activities have been implemented and affected information systems and information technology have returned to full and normal operations) the incident response lead or team must complete the incident report. During longer investigations, affected HICs may request status updates on the incident investigation in the interim.

2.21. [The EHR Solution] Program Office must archive their incident reports for a minimum of 24 months.

2.22. [The EHR Solution] Program Office must provide participating HIC with any [the EHR Solution] incident reports within 72 hours of the request.

2.23. The final incident reports should be reviewed by the Connecting Security Committee and if necessary the Applicable Oversight Body. Ontario Health will facilitate this review when the report is submitted by [the EHR Solution] Program Office.

2.24. [The EHR Solution] Program Office should implement a mechanism to review all of their incidents, at a minimum, monthly to identify trends and to determine whether any preventative actions can be taken to reduce the likelihood of similar incidents from occurring in the future.

Evidence Gathering

2.25. [The EHR Solution] Program Office should develop procedures for collecting evidence for the purposes of disciplinarily or legal action against agents or Electronic Service Providers. These procedures should require:

2.25.1. Forensics work to be performed on copies of the evidential material.

2.25.2. The creation of copies is witnessed.

2.25.3. Details of the creation should be logged, including:

2.25.3.1. When and where the copying process was executed

2.25.3.2. Who performed the copying activities, and

2.25.3.3. Which tools or programs were utilized for the copying process.

2.25.4. The integrity of all evidential material is protected.

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: Incident Severity and Priority Ratings

Severity Ratings

Severity	Category and Description	Recommended Maximum Time Frames		
		Triage	Containment	Recovery
1	**Critical** • Critical or multiple sites down • Loss of service poses substantial risk to participating HICs • Posing a public health safety, privacy or security risk • Causing significant adverse impact affecting a large number of internal and/or external systems, e.g., large scale malware outbreak. Immediate response and restore – "all hands on deck"	30min	6hrs	72hrs
2	**High** • Single, critical site down • Loss of non- mission-critical service • Help desk unavailable • Remedy Failure • Service degradation affecting HICs. • Application or component failure affecting multiple clients Response/restore as quickly as possible - within one business day	2hrs	12hrs	24hrs
3	**Medium** • Application or physical component slowdowns • Minor technical or function problems • Application or component failure affecting single client Restore within the next few business days	4hrs	36hrs	48hrs
4	**Low** • Minimal impact, not time- critical, or work-around exists. Restore within a week	24hrs	36hrs	15 days

Priority Ratings

Incident Type	Priority Rating	
	P2	P1
Access control: Reserved for security incidents related to a potential compromise of access control.		
Privilege account compromised E.g., a Privileged ID (such as system administrators, database administrators, firewall administrators) demonstrates unusual activities/behaviours (e.g., unexplained log-ins, unexplained file accesses)	X	
Phishing attack detected – targeting privileged users: E.g., numerous suspicious emails targeting users with privileged access	X	
Asset security: For incidents that involve lost or stolen assets and attacks to an asset causing disruption of service.		
Loss of unencrypted storage media E.g., loss of an unencrypted USB drive containing sensitive data is lost	X	
Denial of Service (DOS) attack against a critical asset detected E.g., a DOS attack has been initiated against a server hosting business critical applications	X	
Data security: For incidents that threaten the confidentiality of data.		
Unusually high volume of data access on server(s) hosting sensitive data/applications that process or store sensitive data E.g., a system alarm is triggered that there is a high volume of data transfer during non-business hours (not caused by data back-up)	X	
Malware / Virus infection detected– high impact E.g., an alarm is triggered that a virus outbreak was detected	X	
Data and System Integrity: Incidents related to a potential compromise of integrity of data and systems		
Major data breach that has attracted media attention: E.g., a major data breach that has attracted media attention		X
Tape back-up failed on over period of time E.g., A tape back-up failed for the past 5 sessions	X	

Appendix B: Incident Report Details

The following details are required in an information security incident report:

1. Contact Information of the agent or Electronic Service Provider that reported the incident, AND the incident response lead or team:
    - Name
    - Unit (e.g., department, division, team) (if applicable)
    - Email address
    - Phone number
    - Location (e.g., mailing address, building and room number)
2. Incident Details
    - Date/time when the incident was discovered
    - Estimated date/time when the incident started
    - Incident ticket number
    - Type of incident (e.g., denial of service, malicious code, unauthorized access, inappropriate usage)
    - Physical location of the incident (e.g., city)
    - Current status of the incident (e.g., ongoing attack)
    - Source/cause of the incident (if known), including hostnames and IP addresses
    - Description of the incident (e.g., how it was detected, what occurred)
    - Description of affected resources (e.g., networks, hosts, applications, data), including information systems' hostnames, IP addresses, and function
    - Operating system, version, and patch level
    - Antivirus software installed, enabled, and up-to-date (yes/no)
    - Mitigating factors
    - Estimated technical impact of the incident (e.g., data deleted, system crashed, application unavailable)
    - Actions performed by the agent or Electronic Service Provider who reported the incident (e.g., shut off host, disconnected host from network)
    - Other organizations contacted (e.g., software vendor)
    - Type of information compromised (if applicable)
3. General Comments (Recommended but not required)
4. Summary of the Incident
5. Contact information for all involved parties
6. Log of containment/mitigation actions taken by incident response lead/team
7. List of evidence gathered
8. Cause of the Incident (e.g., misconfigured application, unpatched host)
9. List of recommended and implemented remediation activities
10. Current Status of the Incident Response