Data Security Policy - Incident Response and Reporting

PURPOSE

To provide principles and guidelines for incident response and reporting at Organization, including security incidents. To provide detailed instructions for conducting incident response and reporting activities.

SCOPE

This Incident Response and Reporting Policy will cover:

- Detection, identification, response, and reporting of incidents and potential incidents **(Incident Management)**
- Mitigation of incidents that occur (**Incident Response)**
- Documentation of incidents
- Incident Management Process
- Incident Documentation
- Incident Response Process
- Roles and Responsibilities
- Related Forms, Plans, and Documents
- Related Policies
- And Relevant Regulations, Standards and Criteria

POLICY

Organization defines a “security incident” or “incident” as any event that results in unauthorized access, usage, disclosure, alteration, or destruction of information; or any disruption of information systems, including physical tampering.

Organization encourages a security-aware culture, so if you suspect an incident has occurred, contact your supervisor, or use the reporting hotline. Organization has included incident response in security training.

If Organization decides to follow industry data security best practices beyond the Security Rule, like SOC2, it will also perform periodic tabletop (TTX) exercises to simulate incident response activities.

Organization makes this Incident Response Policy and Procedures available to employees.

Incident Management

Organization adopts and follows an incident management procedure that provides instruction on:

- Detecting a security incident
- Identifying a security incident
- Documenting a security incident
- Responding to a security incident
- And reporting a security incident

Security incidents that involve ePHI may need to be handled in a specific way. Refer to the Data Security Policy – HIPAA Incident Response, Reporting, and Breach Determination Policy.

Examples of Security Incidents:

- Unauthorized access to physical or electronic assets, data, information, facilities, or accounts
- Cyber attacks, such as DDoS attacks, malware, social engineering, and others.
- Loss or theft of Organization devices or media
- Outages or disruptions of information systems and technology

Incident Response

Organization maintains a formal “Incident Response Plan” that are documented below *Procedure* section. Confirmed incidents are documented, and appropriate personnel are contacted to handle the incident. The incident team convened to address an incident is known as the “Incident Response Team” or IRT. IRTs can consist of members from all departments, levels, and regions across the organization.

Organization incident response consists of:

- Convening the IRT, including contact information plans
- Investigating the incident, including root cause
- Containing the incident
- Eradicating the incident
- Recovering from the incident
- And applying lessons learned from the incident

Incident Documentation

Organization documents each incident through to completion. Documentation of an incident should include sufficient information to determine the following:

- When the incident occurred and for how long
- What caused the incident
- What **Organization** did to respond to the incident
- How the incident was resolved
- And lessons learned from the incident

PROCEDURES

Organization makes these Incident Response and Reporting Procedures available to employees and includes them as part of *Security Awareness and Training.*

If Organization decides to follow security industry best practices like SOC2, will follow an Incident Response Plan and test this plan annually. If any updates are needed, the plan will be updated and approved.

Employees can report suspected incidents to their supervisor, the Security Officer or use Organization's reporting tool.

Incident Management

Identification and Determination of Security incidents

Incident Detection and Identification Incidents can be detected through existing logging and monitoring controls, receiving reports from personnel or the public, or running into an operational disruption or problem. Suspected incidents should be documented in Organization's ticketing system or similar tracking mechanism and triaged by the appropriate team.

Once an incident has been triaged and confirmed, attempts should be made to identify the type of incident, if possible. The identification process may take some investigation and collaboration across business units.

At this time, the Security Official must be notified if the incident affects PHI or ePHI for further action. The Security Official will contact the Privacy Official and collaborate to respond to the incident. Organization may need to consult with legal counsel if the incident calls for it. Security incidents that involve ePHI need to be handled in a specific way and have additional responses, like breach determinations and notifications. Refer to the Data Security Policy– HIPAA Incident Response, Reporting, and Breach Determination to handle Security Incidents involving ePHI*.*

While the supervisor or Security Official takes appropriate actions, Organization will avoid making any updates or other modifications to software, data, or equipment involved in the incident. This preserves evidence if further investigation is needed.

Incident Documentation

Organization documents each incident through to completion. Documentation of an incident should include details like:

- When the incident occurred and for how long
- What caused the incident
- How widespread the vulnerability is
- What Organization did to respond to the incident
- How the incident was resolved
- Lessons learned from the incident

Examples of details to include are:

- Hardware address
- System name
- IP address
- *ePHI* data processed by the system
- Applications installed on the system
- Location of the system

Organization will also document which systems were impacted, and what access was used, if possible.

The Incident management module in the Guard can be used to document incident and incident response including investigations.

Incident Response

Incidents come in many forms and may require different response approaches. In order to respond to an incident, Organization will convene an Incident Response Team (IRT) to tackle the incident, exept for those involving ePHI will be handled under the Data Security Policy– HIPAA Incident Response, Reporting, and Breach Determination. The IRT will then begin incident response using the *Incident Response Plan.*

Incident Response Plan

When responding to an incident, the IRT must perform and document the following:

- Investigation of the incident, including determining root cause
- Measures taken to contain the incident
- Eradication of the incident, which can include:
- Deletion, removal, or replacement of malicious or infected files
- Modification, re-creation, or termination of user accounts, if there is evidence of unauthorized access
- Restoration from a clean backup
- Incident recovery, which can include:
- Restoring data from a clean backup
- Bringing systems back online
- Enabling user access and accounts
- The IRT must document lessons learned from the incident and work with Organization to adopt any improvements that are necessary.

The *Incident Response Plan* will be tested annually and updated as needed.

ROLES AND RESPONSIBILITIES

Security Officer: Coordinates with Privacy Officer to address any incidents that affect PHI or ePHI. Determines if any laws or regulations may have been violated.

Incident Response Team (IRT): Team(s) responsible for responding to other security incidents.

VIOLATIONS

Organization may take disciplinary action should evidence show that an internal user caused or contributed to the incident.

RELATED FORMS/PLANS/DOCUMENTS

- Incident Response Plan

RELATED POLICIES AND PROCEDURES

- Data Security – Incident Response and Reporting Procedure
- Data Security – HIPAA Incident Response, Reporting, and Breach Determination
- Breach Notification Policy

RELEVANT HIPAA REGULATIONS

- § 164.308(a)(6)(i) *Security incident procedures*
- § 164.308(a)(6)(ii) *Response and reporting*

RELEVANT SOC 2 CRITERIA

- CC 7.3.1 *Responds to Security Incidents*
- CC 7.3.2 *Communicates and Reviews Detected Security Events*
- CC 7.3.3 *Develops and Implements Procedures to Analyze Security Incidents*
- CC 7.3.4 *Assesses the Impact on Personal Information*
- CC 7.3.5 *Determines Personal Information Used or Disclosed*
- CC 7.4.1 *Assigns Roles and Responsibilities*
- CC 7.4.2 *Contains Security Incidents*
- CC 7.4.3 *Mitigates Ongoing Security Incidents*
- CC 7.4.4 *Ends Threats Posed by Security Incidents*
- CC 7.4.5 *Restores Operations*
- CC 7.4.6 *Develops and Implements Communication Protocols for Security Incidents*
- CC 7.4.7 *Obtains Understanding of Nature of Incident and Determines Containment Strategy*
- CC 7.4.10 *Evaluates the Effectiveness of Incident Response*
- CC 7.4.11 *Periodically Evaluates incidents*
- CC 7.4.12 *Communicates Unauthorized Use and Disclosure*
- CC 7.4.13 *Application of Sanctions*