CONE HEALTH	**Guideline:** ITS Information Security Incident Management Procedure	
	Department Responsible: SW-ITS-Administration	**Date Approved:** 06/07/2024
	Effective Date: 06/07/2024	**Next Review Date:** 06/07/2025

INTENDED AUDIENCE:
Entire workforce

PROCEDURE:
In accordance with the standards set forth under federal and state statutory requirements (hereafter referred to as regulatory requirements), Cone Health is committed to ensuring the confidentiality, integrity, and availability of all protected health information (PHI/ePHI), sensitive, and confidential data (hereafter referred to as covered information) it creates, receives, maintains, and/or transmits.
The purpose of this procedure is to define roles, responsibilities, and processes for information security incident management.

Scope and Goals:
The scope of this procedure is to define the process for identification, response, reporting, assessment, analysis, and follow-up to information security incidents. This procedure applies to the following types of security incidents (also refer to Appendix 1 – Examples of Security Incidents/Breaches):

- Technical security incidents (e.g., computer/network intrusions, denial of service to authorized users, unauthorized access, etc.)
- Non-technical security incidents (e.g., administrative and physical incidents including, but not limited to, theft, lost devices, unlocked doors, unauthorized facility entry, unauthorized computer access, etc.)

Goals of this procedure include, but are not limited to, the following:

- Define the relationship between a security incident and a reportable breach of ePHI/PHI.
- Describe activities associated with incident identification, containment, eradication, recovery, and post-incident remediation.
- Define members of the Security Incident Response Team (SIRT).

Responsibilities:
Chief Information Security Officer (CISO):
The CISO is responsible for, but not limited to, the following activities:

- Revisions, implementation, workforce education, interpretation, and enforcement of this procedure.
- Co-facilitate the Information Technology Incident Response Team.
- Coordinate efforts in respect to the vulnerability management program as applicable and needed to utilize network tools for IPS, IDS, forensics, vulnerability assessments, and validation (refer to the Vulnerability Management procedure).
- Investigation officer for all information security incidents.
- Advisor to the organization's Command Center and Incident Management Team.
- Assist chief privacy officer with breach management duties.

- Facilitate semiannual tabletop exercises with all members of the SIRT to ensure everyone understands their roles.
- Provide individuals with a process and method to report security issues and/or breaches anonymously.
- Maintain a list of third-party security contact information in the event an incident needs to be reported to an outside party.
- Ensure members of the Information Technology Incident Response Team and other workforce members that have significant responsibilities related to incident response are properly trained within 90 days of their hire date, or assuming an incident response role, and whenever there is significant change to the organization's environment, and within every three hundred sixty-five (365) days thereafter.
- Ensure members of the Information Technology Incident Response Team are properly trained to handle incidents that involve or are caused by insider threat.
- Ensure a duress alarm will be implemented in situations where they are warranted.

Chief Privacy Officer:

The chief privacy officer is responsible for, but not limited to, the following activities:

- Co-facilitate the Incident Response Team.
- Advisor to the organization's Command Center and Incident Management Team.
- Alternate investigation officer for all information security incidents.
- Breach management.

Security Incident Response Team (SIRT):

The SIRT is responsible for, but not limited to, the following activities:

- Keep the Command Center and Incident Management Team informed on all incident management activities.
- Ensure that all incidents are fully documented from discovery to remediation and include all individuals involved and the actions that were taken.
- Provide oversight and management of incident response and reporting activities.
- Review and approve the breach risk analysis.
- Specific duties outlined by the Command Center and Incident Management Team member roles and responsibilities in the Appendix 2.
- Ensure that incidents are promptly reported to external entities when necessary.

Command Center and Incident Management Team:

The Command Center and Incident Management Team is responsible for the process by which the organization deals with major events that threaten to harm the organization, its stakeholders/customers/clients, or the general public. The Command Center and Incident Management Team is responsible for keeping Cone Health's leadership team appraised on incident/breach management activities.

Information and Technology Services (ITS):

ITS is responsible for, but not limited to, the following activities:

- ITS will be responsible for performing activities associated with the containment, eradication, and recovery phases of this procedure.
- Maintain detailed internal procedures for performing containment, eradication, and recovery activities.

Incident Discovery/Notification:
Incident discovery/notification can come from, but not be limited to, the following:

- Workforce member
- Insider threat
- Anonymous call/email
- Firewall, intrusion detection/prevention, antivirus technology, etc.
- System audit log review
- Patient/client/customer
- Third party vendor/contractor/consultant
- Internal/external audit
- Business partner
- Third party security services (not associated with the organization)
- Third party threat notification services
- Media
- Duress alarm

Incident Response Process:
The incident response process begins immediately upon discovery or notification. The date/time is very important to the breach notification process if the incident is determined to be a breach of ePHI/PHI (see Breach Notification procedure).

The following phases represent the entire information security incident management process. These phases often happen quickly and do not necessary happen in the order listed in this procedure. It is also common for activities within each phase to occur simultaneously.

Identification Phase:

1. The CISO or chief privacy officer will determine if what is being reported is an event, precursor, or security incident.
2. If the issue is an event, the CISO/chief privacy officer will contact the appropriate internal resource for resolution.
3. If the issue is a precursor or security incident, the CISO/chief privacy officer will determine if it is technical or non-technical and at the same time activate the SIRT and Command Center and Incident Management Team, and begin to document background information related to the incident on an Information Security Incident Response/Investigation Form. Among other factors being noted in this form, special attention should be given to listing any and all employees involved with the security incident. The SIRT will proceed as follows:
    - Non-Technical Security Incident: The SIRT completes the investigation, implements preventative measures, and resolves the security incident. Upon completion of the investigation, the SIRT will move to the Post-Incident Remediation Phase.

- Technical Security Incident: Go immediately to the Containment Phase.

4. Other activities could include the following:
    - Contact law enforcement (if appropriate).
    - Contact media outlets: If a security incident has already garnered media attention the Command Center and Incident Management Team may choose to initiate contact with media outlets. Cone Health's media relations representative will serve as the sole point of contact for activities related to the news media.
    - Begin the breach risk analysis process if it is determined or suspected that ePHI/PHI may be involved.
    - Contract with a digital forensic analysis firm.
    - Contact cyber-insurance representative.

Containment Phase:

During this phase, Cone Health's Information and Technology Services (ITS) department will attempt to contain the security incident. Depending on the type of incident, actions performed by ITS will vary. It is extremely important to take detailed notes and protect the chain of custody when information technology assets are involved in the incident. This information will be very helpful to digital forensic analysis and can be used during civil and criminal litigation and/or disciplinary/termination action.

Eradication Phase:

This phase represents ITS's activities to remove the cause and patch/repair security vulnerabilities that resulted in the security incident.

Recovery Phase:

The Recovery Phase represents ITS's effort to restore the affected environment back to normal operation after security vulnerabilities have been remediated.

Post-Incident Remediation:

The post-incident remediation phase represents the review of the security incident by the SIRT to determine the following:

- What additional actions (if any) need to be taken.
- If breach notification is required (see Breach Notification procedure).
- Review incident and if applicable, breach related documentation to ensure that it is complete.
- Whether there are any recurring or high-impact incidents and any improvements to the existing incident response process that need to be implemented.
    - Prepare formal communication or arrange a meeting with senior leadership to brief them on the outcome of the incident.
    - Close the security incident.

Incident Response Training and Evaluation:

The SIRT will semiannually review and evaluate the processes outlined in this procedure. This activity will coincide with mandatory exercises to practice the effectiveness and maintain familiarity with the process by SIRT members. The business continuity, hospital incident command center, and disaster recovery teams (responsible for contingency planning activities for the organization) will also be part of these exercises. All lessons learned will be incorporated into an updated incident response plan.

Documentation Retention:
Records related to security incidents, risk analysis, and breach decisions will be retained for a period of no less than 6 years from the date of the documentation.

Exception Management:
Exceptions to this procedure will be evaluated in accordance with Cone Health's Information Security Exception Management procedure.

Applicability:
All employees, volunteers, trainees, consultants, contractors, and other persons (i.e., workforce) whose conduct, in the performance of work for Cone Health, is under the direct control of Cone Health, whether or not they are compensated by Cone Health.

Compliance:
Workforce members are required to comply with all information security policies/procedures as a condition of employment/contract with Cone Health. Workforce members who fail to abide by requirements outlined in information security policies/procedures are subject to disciplinary action up to and including termination of employment/contract.

REFERENCE DOCUMENTS/LINKS:
Appendix A: Examples of Security Incidents/Breaches
Appendix B: Command Center and Incident Management Team Members and Primary Responsibilities

APPENDIX A: Examples of Security Incidents/Breaches

Name	Description
Disposal Computer	Discovery of computers not disposed of properly
Disposal Document	Discovery of documents not disposed of properly
Disposal Drive	Discovery of disk drives not disposed of properly
Disposal Mobile	Discovery of mobile devices not disposed of properly
Disposal Tape	Discovery of backup tapes not disposed of properly
Email	Email communication exposed to unintended third party
Fax	Fax communication exposed to unintended third party
Fraud SE	Fraud or scam (usually insider-related), social engineering
Hack	Computer-based intrusion
Lost Computer	Lost computer (unspecified type in media reports)
Lost Document	Discovery of documents not disposed of properly, not stolen
Lost Drive	Lost data drive (unspecified if IDE, SCSI, thumb drive, etc.)
Lost Laptop	Lost laptop (generally specified as a laptop in media reports)
Lost Media	Media (e.g., disks) reported to have been lost by a third party
Lost Mobile	Lost mobile phone or device such as tablets, etc.
Lost Tape	Lost backup tapes
Missing Document	Missing document, unknown or disputed whether lost or stolen
Missing Drive	Missing drive, unknown or disputed whether lost or stolen
Missing Laptop	Missing laptop, unknown or disputed whether lost or stolen
Missing Media	Missing media, unknown or disputed whether lost or stolen
Other	Miscellaneous breach type arising primarily from data mishandling
Phishing	Masquerading as a trusted entity in an electronic communication to obtain data
Seizure	Forcible taking of property by a government law enforcement official
Skimming	Using electronic devices (such as a skimmer) to swipe victims' credit/debit card numbers
Snail Mail	Personal information in "snail mail" exposed to unintended third party
Snooping	Exceeding intended privileges and accessing data for unauthorized purposes
Stolen Computer	Stolen desktop (or unspecified computer type in media reports)
Stolen Document	Documents either reported or known to have been stolen by a third party
Stolen Drive	Stolen data drive, unspecified if IDE, SCSI, thumb drive, etc.
Stolen Laptop	Stolen laptop (generally specified as a laptop in media reports)
Stolen Media	Media generally reported or known to have been stolen by a third party
Stolen Mobile	Stolen mobile phone or device such as tablets, etc.
Stolen Tape	Stolen backup tapes
System Failure	System failure or loss of service
Unknown	Unknown or unreported breach type
Virus (Malware)	Exposure to personal information via virus or Trojan (possibly classified as hack)
Web	Web-based intrusion, data exposed to the public via search engines, public pages
Wireless Access Point	Installation / use of an unauthorized wireless access point

APPENDIX B: Command Center and Incident Management Team Members and Primary Responsibilities

Command Center and Incident Management Team Member	Role	Primary Responsibilities
Incident Commander for the Health System	Team Leader for Command Center and Incident Management Team	• Convenes team and chairs Command Center and Incident Management Team meetings • Manages an incident from response through recovery • Delegates recovery planning efforts as applicable
Chief Information Security Officer (CISO)	Team Leader for SIRT and Security advisor	• Convenes team and chairs SIRT meetings • Oversees the information security incident response process. • Assists the chief privacy officer with breach risk analysis activities. • Submits progress and final reports to senior leadership. • Submits final report and oversees debriefing. • Tracks and reports on security related changes that could impact business operations, resulting from incident.
Chief Privacy Officer	Alternate Team Leader for SIRT and Privacy advisor	• Provides information on privacy-related regulatory requirements. • Oversees discovery and investigation from a privacy perspective. • Recommends steps for privacy compliance and to mitigate the risk of penalties. • Oversees breach management program and is responsible for breach risk analysis and notification processes. • Advises team on privacy issues.

Command Center and Incident Management Team Member	Role	Primary Responsibilities
Legal	Legal advisor	• Provides information on major contracts and other obligations that may be relevant to incident and breach management. • Oversees discovery and investigation from an evidentiary perspective, in the case of civil or criminal litigation. • Provides advice on minimizing legal liability. • Coordinates with internal and external legal teams as needed.
Information Technology (CIO)	ITS advisor	• Assists in determining the existence, cause, and extent of an ITS-related incident (e.g., reviews firewall/IPS/sys logs for correlating evidence of unauthorized access). • Coordinates incident management activities assigned to ITS. • Coordinates with ITS to identify victims in Cone Health systems. • Coordinates with ITS organization to plan and implement actions to prevent similar future incidents.
Finance (CFO)	Financial advisor	• Assists with evaluating financial liability. • Provides financial assistance when needed. • Assists with cost/benefit analysis when applying controls.
Facilities/Physical Security	Facilities and physical security advisor	• Advises on matters related to physical, facility and environmental security. • Coordinates activities between the organization and law enforcement. • Remediates any physical facility changes.
Media Relations	Public relations advisor	• Coordinates activities between the organization and public media. • Prepares and issues press releases or statements, as needed.
Emergency Management Director	Emergency Management advisor	• Acts as liaison to outside agencies and Command Center operations. • Aligns with HICS model for best practice.

Command Center and Incident Management Team Member	Role	Primary Responsibilities
People and Culture	People and Culture advisor	• Advises on employment law issues. • If employee personal data is compromised, handles internal communications. • If employee misconduct is a factor, works with appropriate business managers, legal representatives and others to take appropriate employment action (e.g., termination of employment).