	Guideline: ITS Information Security Program 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), confidential, and sensitive data (hereafter referred to as covered information) it creates, receives, maintains, and/or transmits at a level which is reasonable and appropriate with the associated classification level, regardless of format (i.e., electronic, paper, voice, etc.).

The purpose of this procedure is to define Cone Health's information security program, assign organizational responsibility for managing and maintaining information security, and define the need for creating and maintaining organizational security governance (e.g., policies and procedures) that define leadership's expectations for safeguarding the confidentiality, integrity, and availability of covered information that is created, received, maintained, or transmitted by the organization and its business partners, through the use of reasonable and appropriate administrative, technical, and physical safeguards.

Scope and Goals:
Covered information at Cone Health exists in many forms. It can be in hard copy (i.e., paper), electronic (i.e., CD-ROM, hard-drives, phone, email, fax, flash/thumb drive, etc.), or spoken in conversation.

Regardless of the form covered information takes, or the method by which it is shared or stored, covered information requires protection against unintentional or intentional (unauthorized with malicious intent) access, manipulation, or destruction and requires an appropriate level of protection to minimize risk to consumer/client/patient safety, privacy, and quality of care. Therefore, the goal of Cone Health's information security program is to develop, apply, maintain, and test administrative, physical, and technical controls that protect covered information against unauthorized access, manipulation, and disruption (i.e., to availability). The identification and application of security controls will be governed by the organization's risk management program.

Cone Health's information security program is characterized under three core concepts:

- Confidentiality: Ensuring that information is accessible only to those authorized to have access;
- Integrity: Safeguarding the accuracy and completeness of information and processing methods;
- Availability: Ensuring that authorized users have access to information and associated assets when required, and
- Achieved through a combination of:

- People: Everyone understanding their role for protecting information as defined by the organization's policies, standards, and procedures.
- Process: Well defined, realistic, and enforceable policies, standards, and procedures
- Technology: Controls that help with the enforcement of information security processes, reduce human error, and reduce malicious activity

Cone Health's information security program is based on the following frameworks:

1. Health Information Trust Alliance (HITRUST)
2. National Institute of Standards and Technology (NIST)

Responsibilities:

Chief Information Security Officer:

Cone Health's chief information security officer (CISO) is responsible for facilitating the development, implementation, and oversight of all security activities pertaining to Cone Health's information security program. The CISO's responsibilities include, but are not limited to, the following:

- Maintain, interpret, and enforce of this procedure.
- Ensure that information security is integrated into all essential business activities.
- Ensure that information security delivers value and meets business requirements.
- Ensure regulatory, statutory, and contractual obligations are met, stakeholder expectations are managed, and civil and criminal penalties are avoided.
- Support business requirements by managing information risk and ensure that it is treated in a consistent and effective manner through the application of appropriate risk management principles (i.e., Risk Management program).
- Analyze and assess emerging information security threats so that informed, timely action to mitigate risk can be taken.
- Reduce costs, improve efficiency and effectiveness, and promote a culture of continuous improvement in information security.
- Prevent disclosure of covered information to unauthorized individuals.
- Ensure that information security-related activities are performed in a reliable, responsible and effective manner.
- Provide a positive information security influence on the behavior of end users, reduce the likelihood of information security incidents occurring, and limit their potential business impact through effective, ongoing information security education, training, and awareness.
- Oversee, verify compliance and enforce all activities necessary to comply with the regulatory, statutory and contractual requirements within Cone Health's policies and procedures.
- Create (when applicable) and maintain formal security policies and procedures, to include annual review and update, and evaluating/approving exceptions to information security policies.
- Manage policy/procedure exceptions and review at least annually to determine applicability and validate that sufficient corrective action is being taken to negate exception.
- Continually monitor, review and evaluate the effectiveness of the information security program and update as needed to ensure objectives continue to be met.
- Ensuring plans for system security testing, training and monitoring activities are developed, implemented, maintained and reviewed for consistency with the risk management strategy and response priorities.

- Perform or oversee technical and non-technical evaluations (i.e. assessments) to validate compliance with Cone Health's security policies and procedures.
- Document all activities and assessments completed to comply with the regulatory, statutory and contractual requirements and retain applicable documentation in accordance with federal and state record retention requirements.
- Document approved applications and application stores for mobile devices.
- Ensure that applicable security policies and procedures are read and understood by all workforce members (e.g., information security education, training and awareness).
- Implement an ongoing workforce improvement program that provides initial, recurring, and annual security training to all workforce members in accordance with Cone Health's Information Security Training and Awareness procedure. Also ensure that all appropriate measures are taken to avoid cases of identity theft targeted at patients, employees, and third parties.
- Proactive coordination and communication of security activities (e.g., implementing controls, correcting gaps) across the organization.
- Co-facilitate the Audit and Compliance Committee with the chief privacy officer.
- In cooperation with the chief privacy officer, ensure that covered information is only retained for as long as necessary and then properly disposed of or sanitized per Cone Health's applicable policy/procedure.
- Manage the Security Incident Response Team (SIRT).
- Ensure that all systems undergo an annual security review or when changes occur that could impact system security.
- Ensure that new systems undergo a thorough security review, prior to being put into production, to ensure that the confidentiality, availability, and integrity of ePHI is properly maintained.
- Assist Cone Health's People and Culture when necessary on matters pertaining to workforce background investigations and disciplinary action for noncompliance with security policies and procedures.
- Work with Cone Health's chief privacy officer on security matters that impact patient/consumer/client privacy.
- Oversee the vendor risk management program.
- Document a report and then present an annual "state of the information security program" briefing to Cone Health leadership on the overall posture of the information security program to include areas of risk that require attention and incidents that occurred during the calendar year and what actions were taken to prevent recurrence.
- Participate as a member of the organization's Command Center and Incident Management and business continuity/disaster recovery teams.
- Work with and advise facility management on matters pertaining to physical and environmental security.
- Ensure security requirements for information systems are identified in mission/business processes and resources allocated as part capital planning and investment control processes in a discrete budget line item.
- Meet with lead and business area/organizational unit security contacts on a monthly or near monthly basis for the purpose of coordinating security activities.
- Participate in industry trade associations, subscribe to thought leadership and market research organizations or establish some other reliable process to stay abreast of business sector, industry,

technology, infrastructure, legal, and regulatory environment trends that may impact the organization's security policies. See that changes are incorporated into development or updates to the organization's policies and procedures.
- Ensure that the organization's security and privacy practices are publicly accessible (i.e., on a public website).
- Be available to customers and business partners for questions and other security situations that require direct communication.
- Perform responsibilities outlined in other information security policies/procedures.

Management:

Key success factors for the successful implementation of Cone Health's information security program include the following of the organization's leadership:

- Direction and mandate for the information security initiative, to include visible ongoing commitment and support.
- Adequate funding and resource commitment.

Management's responsibilities include, but are not limited to, the following:

- Appointment of a qualified, experienced, senior-level information security official who is responsible for managing the organization's information security program, for ensuring appropriate security processes are in place, continually evaluating security risks and providing recommendations for mitigation to the appropriate level of management. If the security official is an outsourced resource, management will:
    - Assign an internal workforce member to manage that resource.
    - Require the third-party service to maintain a security program that protects Cone Health and complies with applicable regulatory requirements.
- Appointment of a qualified, experienced, senior-level data protection/privacy officer who is responsible for the privacy integrity of covered information. For applicants, examine the individual's resume and any other relevant materials to determine if the individual has the requisite knowledge, education and experience to fulfill the duties of the position. If appointed, ensure that the individual understands that as part of their job, responsibilities will include:
    - Development and implementation of privacy policies and procedures.
    - Serving as the point of contact for all privacy-related issues.
    - Providing guidance to managers, users, and service providers on their individual responsibilities and the specific privacy procedures that must be followed.
- For the data protection/privacy officer, ensure other tasks are kept to a minimum, such that they would not interfere with the performance of the data protection officer's primary responsibilities.
- Ensure adequate and qualified resources are available to manage and maintain the information security program.
- Provide clear direction and visible management support for security initiatives.
- Ensure that information security personnel receive adequate and recurring training to maintain their job proficiency and stay abreast of the current threats, vulnerabilities, and mitigation strategies.
- Support, promote, and assist with the enforcement of the information security program and the policies and procedures by which it is governed.

- Appoint a management-level individual (designated approving authority) to review and evaluate risk analyses submitted by the CISO and accept/deny risk mitigation recommendations.
- Establish and communicate the organization's priorities for organizational mission, objectives, and activities.
- Assign an internal management-level individual or group or contract a qualified external resource (e.g., security auditor) to annually review the effectiveness of the information security and risk management programs.
- Appoint additional security contacts in writing for each major organizational area or business unit to assist the CISO with the implementation and management of the organization's information security program.
- Formally approve all organizational security policies, including the information security program.
- Ensure an Information Security Committee or Audit and Compliance Committee is chartered and active.
- Ensure that annually (or when there is a material change to business practices that will implicate the security or integrity of covered information) an internal security/risk assessment is performed by the CISO and externally by an independent organization. Independent security program reviews:
    - Include an assessment of adherence to the organization's security plan;
    - Notify and coordinate with management the timing and nature of the assessment;
    - Address the need for changes to the approach to security in light of evolving circumstances, including the policy and control objectives and other opportunities for improvement, including those based on regular vulnerability assessments (e.g., network scans and penetration testing);
    - Carefully control information security tests to limit the risks to confidentiality, integrity, and system availability; and
    - Will be carried out by individuals who have the appropriate skills and experience and that are independent of the area under review (e.g., the internal audit function, an independent manager or a third-party organization specializing in such reviews).
- Take corrective action on any discrepancies or areas of non-compliance with regulatory/statutory/contractual requirements identified by internal and independent audits/assessments. The results of these assessments, including any correction actions performed, will be documented, approved, and maintained for at least 3 years.
- Evaluate the need for cyber-insurance to protect against cost associated with recovering from a data breach or other type of security incident. If cyber-insurance is purchased, ensure that the coverage is maintained.
- Perform responsibilities outlined in other information security policies/procedures.

Workforce:

All workforce members are responsible for being knowledgeable on, promoting, and complying with established information security policies and procedures.

Third Party Contractual Relationships:

All third party contractual relationships (i.e., business associates, contractors, consultants, vendors, etc.) that have or could have access to Cone Health's covered information, are responsible for complying with established Cone Health information security policies and procedures. The CISO, with

the assistance of the organization's contract management/procurement office, will ensure that all individuals employed/contracted by a third party that will have access to covered information read and acknowledge receipt and understanding of applicable Cone Health's information security policies and procedures.

Information Security Committee/Audit and Compliance Committee:
The purpose of the Information Security Committee or Audit and Compliance Committee is to ensure that there is clear direction and visible management support for security and privacy initiatives. This group is responsible for all duties identified in the group's charter as assigned by Cone Health's senior management. The CISO and Chief Privacy Officer will co-facilitate the committee.

Board of Directors/Trustees:
Cone Health's Board of Directors/Trustees is responsible for ensuring all senior management is fulfilling its responsibilities in accordance with organization information security policies/procedures.

Security Incident Response Team:
The Security Incident Response Team responsibilities are outlined in the Incident Management and Breach Management policies/procedures.

Business Continuity/Disaster Recovery Teams:
Personnel responsible for the management of business continuity and disaster recovery will work with the CISO to ensure information security is included in their processes and plans.

Command Center and Incident Management Team:
The organization's Command Center and Incident Management team will ensure that the CISO is a member of the team.

Governance Management:
The CISO is responsible for drafting all information security policies and procedures. Draft policies/procedures will be vetted with the Information Security Committee or Audit and Compliance Committee before submitting to senior management for approval.

The CISO will review policies/procedures at least annually and update as needed. The CISO will also update policies/procedures sooner if the situation warrants (e.g., regulatory, statutory and contractual changes, process changes, changes due to compliance problems, etc.). All changes to policies/procedures will warrant immediate communication

Compliance Testing:
Compliance testing will be performed using one or more of the following techniques. For those techniques that require sampling, selection will be performed using a method of randomly selecting areas/attributes to test. Test procedures are listed in order of most to least reliable.

Test Procedure	Description
Reperformance	Performing the activity *(Ex. I locked the door!)*
Inspection	Reviewing documented proof or evidence of item being audited *(Ex. I checked the door to make sure it was locked!)*
Observation	Watching an individual actually do the task *(Ex. I saw you lock your doors!)*
Inquiry	Interview an individual and taking them at their word *(Ex. Do you lock your doors?)*

Periodically the CISO will perform random compliance testing in relation to the established internal policy/procedures and the specific requirements contained within those documents.

Information security program areas subject to compliance testing include, but are not limited to, the following:

- Acceptable Use of Information Technology
- Facility and Environmental Security
- Business Continuity and Disaster Recovery
- Technical Vulnerabilities and Patch Management
- Security Incident and Breach Management
- Asset Management
- Auditing Logging and Monitoring
- Risk Management
- Change Management
- Data Classification and Handling
- Password Management
- Access Management
- Security Training and Awareness
- Network Security
- Security Configuration Management
- Personnel Security Management
- Teleworking
- Personal Devices
- Third Party Assurance

Exception Management:
Cone Health will ensure individuals can make complaints concerning the information security policies, procedures, or the organization's compliance with its policies and procedures. These complaints, also known as exceptions, will be documented and evaluated in accordance with the Information Security Exception Management procedure.

Guideline: ITS Information Security Program 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 directly compensated for services/work 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.