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

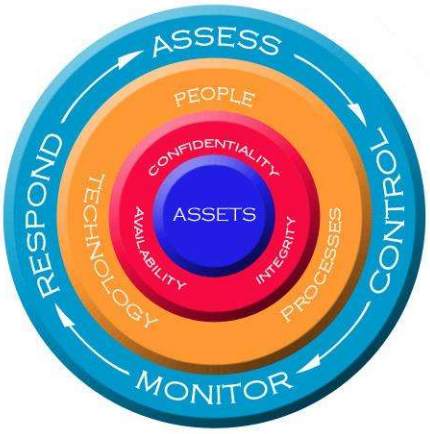
INTENDED AUDIENCE:
Entire workforce

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 risk management program. This policy outlines scope, responsibilities and the processes associated with risk identification, assessment/analysis, mitigation, acceptance, continuous monitoring, and revalidation.

Scope and Goals:
The principal goal of Cone Health's information security risk management program is to identify and mitigate risks to the confidentiality, integrity, and availability of covered information, to include the people, processes, and technology that use, support, or manage covered information. The information security risk management program is not a technical function carried out exclusively Information and Technology Services (ITS), but rather a business process that requires involvement from many different people (e.g., senior leadership, middle management, ITS, People and Culture, Legal, Privacy, etc.) in the organization.

The objective of the risk management program is to continually assess, control, monitor, and respond to the risks to Cone Health's assets, clients, workforce, and covered information that Cone Health is entrusted with and required to protect. Additionally, risk management ensures that controls/safeguards are not applied unnecessarily, and that risk is evaluated based on likelihood and impact from a loss of confidentiality, integrity, and availability of covered information and associated assets. The following figure encompasses all aspects of risk management.



The risk analysis is an integral part of the risk management program. Without risk analysis, the program cannot be successful. This procedure describes a number of different risk analysis approaches Cone Health utilizes to meet the specific situation.

The remainder of this procedure describes each of the following core risk management program processes:

- Risk Assessment/Analysis
- Risk Mitigation
- Risk Acceptance
- Continuous Monitoring
- Revalidation

Responsibilities:

Chief Information Security Officer:

Cone Health's chief information security officer (CISO) is responsible for maintenance, interpretation, and enforcement of this procedure and overall management of the information security risk management program. The CISO's responsibilities include, but are not limited to, the following:

- Providing training and awareness to applicable workforce members.
- Facilitating risk assessment and analysis activities at a set interval.
- Preparing risk analysis packages for designated approving authority (DAA) review.
- Assisting the DAA with risk mitigation and acceptance decisions.
- Monitoring plan of action and milestone activities.
- Annually reviewing all risk assessments and related mitigation decisions and working with the business and the DAA to update as needed.
- Working with Information and Technology Services (ITS) and other applicable resources to stay abreast of the threat environment.

Management:

Senior management is responsible for appointing an individual or group of individuals to act in the capacity of the DAA. Additional responsibilities include, but are not limited to, the following:

- Provide resources and funding as needed to support the organization's information risk management program.

- Provide guidance to the DAA as needed.
- Assist the CISO with enforcement.

Designated Approving Authority:
The DAA is responsible for making risk mitigation decisions on behalf of the organization. The DAA approves or denies risk mitigation strategies based on his or her knowledge of the business, regulatory/statutory requirements, and the recommendations of the CISO. The DAA's responsibilities include, but are not limited to, the following:

- Evaluate risk analysis packages with the assistance of the CISO and make risk mitigation decisions.
- When necessary, consult senior management for risk acceptance decisions that could significantly impact the organization.

Workforce:
Workforce members involved in performing or assisting with information security risk management activities are responsible for maintaining proficiency with risk management processes and complying with requirements in accordance with this procedure.

Third Party Contractual Relationships:
Third party contractors/vendors/consultants working on behalf of Cone Health, will be required to comply with the organization's information security risk management program. Some contractual relationships will warrant the third party to have and maintain their own risk management program that will include reporting applicable risk mitigation decisions to Cone Health.

Risk Assessment/Analysis:
Whether performing a risk assessment or an analysis, the following need to be taken into consideration:

- Type of information created, received, transmitted, or maintained (sensitivity of the data, criticality to the organization, value to an unauthorized user, etc.).
- Amount of information (number of records, number of individuals).
- Number of access points to the assets containing the information.
- Number of end-users, vendors, business associates, etc., who have access to the information.
- Lessons learned from prior security incidents or breaches.
- Safeguards/controls against all types of cyber-attacks, social engineering, insider threat, etc.
- Existing security measures in place.
- Level of security provided by business associates, service providers, etc.

A risk assessment is the first phase of the risk management process. A risk assessment typically takes the form of an activity that identifies risks: vulnerability assessment, audit, etc., or technical control (e.g. IDS, audit logs, etc.). It is important to know that not all risks will be determined by a risk assessment. Risks can also be identified as the result of an event, incident or breach.

A risk analysis is the next step in the risk management process but can also be the first step if a risk is identified by means other than a risk assessment. The primary purpose of a risk analysis is to evaluate

the risk and determine if existing controls are sufficient or if additional controls need to be implemented to mitigate risks to an acceptable level.

Under Cone Health's risk management program, a risk assessment and/or risk analysis will be performed as the prelude to, during or as a follow-up activity for the following:

- *Breach Notification:* As required by HIPAA's breach notification requirement, a breach risk assessment will be performed upon the discovery of a security incident by Cone Health or its business associates involving protected health information. The purpose of the breach risk assessment will be to determine if the incident is a reportable breach. See Cone Health's Breach Notification policy for additional guidance and the procedures on how to complete a risk analysis for breach notification.
- *Business Associates:* Risk assessments performed on business associates will be conducted prior to signing any contracts and annually thereafter. If a risk analysis is needed, then it will be performed in accordance with Cone Health's Third-Party Assurance procedure.
- *Incident/Disaster Follow-Up:* A risk analysis will be performed after an incident, breach or disaster to determine if any risks need to be mitigated. The form identified in the Information Security Risk Analysis will be used to document this risk analysis.
- *Policy/Standard/Procedural Exceptions:* When an exception to a Cone Health's security policy/procedure is requested, a risk analysis will be completed as a part of the exception decision making process. The purpose of the risk analysis is to ensure that the exception does not undermine existing security controls. If necessary, identifying and implementing compensating controls will be needed as a temporary solution until the exception is no longer needed. The form identified in the Information Security Risk Analysis, will be used to document this risk analysis. NOTE: Approved exceptions will be formally reviewed annually until the exception is no longer needed. This review will be documented.
- *Regulatory and Policy Compliance:* Risk assessments/analyses for regulatory and organizational policy and procedure compliance are managed under Cone Health's compliance program. Cone Health utilizes the Health Information Trust Alliance (HITRUST) to perform an annual risk analysis to measure compliance with regulatory and statutory requirements. Upon completion of this risk analysis, risks are identified in a corrective action plan, which Cone Health uses to document remediation activities through completion and acceptance by the DAA.
- *System Development or Acquisition*: Risk assessments/analyses will be conducted at various stages of new system acquisition or development projects. Risk assessments are meant to identify controls that need to be considered before acquisition or development and pre/postproduction. These control specifications must consider and state the automated and manual controls that will be required. Due to the number of changes that can occur during system acquisition or development, a risk analysis needs to be done at different stages of the process. The same risk analysis can be used as long as each phase is addressed in the risk analysis documentation. These phases are as follows:
    - Initiation Phase (e.g., planning/proposal stage): Risk assessments/analyses in this phase are meant to ensure that required minimum security controls have been addressed as early in the process as possible to avoid unnecessary costs later in the project or trying to retrofit after the system is in production.
    - Acquisition/Development Phase: During this phase, the risk assessment/analysis process is designed to be an extension of the initiation phase by ensuring that controls are being

implemented and if necessary adjusted or additional controls are added as the situation warrants.

- Implementation Phase (e.g., post-production): This is the final stage of the post-production risk assessment/analysis. The purpose of this phase is to ensure that existing controls are adequate and known security risks are addressed. It is during this phase that acceptance of risk occurs. Cone Health's CISO will prepare a statement of system certification (e.g., ATO or IATO) that states what the risks are, controls that have been implemented (or planned to be implemented) to mitigate identified risks, and what activities will be performed to monitor these controls to ensure that they continue to effectively manage the risk(s). This is provided along with the POAM (if applicable) to the DAA. The ATO/IATO will be signed by the CISO, the business owner who supports the system, and the DAA.
    - Interim Approval to Operate (IATO): Is only good for a 90-day period before an IATO extension must be signed by the DAA. An IATO is only authorized to be extended one time, after which the system/application will be removed from the production environment.
- Operations/Maintenance Phase (continuous monitoring): This phase covers the life of the system. At planned intervals, not to exceed 6 months, system controls will be reviewed to ensure that they are operating as expected. The risk analysis will also be reviewed to ensure that no new risks are present that need to be mitigated. If necessary, a POAM will be created to track new remediation/mitigation activities. After each review, the risk analysis will be updated.
    - Within this phase, ATOs will review and be reapproved on an annual basis by the DAA (i.e. revalidation).
- Disposition/Disposal Phase: During this phase the purpose of the risk analysis is to determine the method by which the contents on asset's electronic storage (i.e., hard drive) will be removed to protect covered information from becoming compromised. This phase applies to disposal, repurposing, lease turn-in, resale and donation.

- *System Changes:* Risk assessments/analyses will be performed whenever a system is changed, upgraded, patched, etc. The intent of the risk analysis it to ensure that any changes being made to the system do not nullify or weaken existing security controls. This risk analysis will be included as a part of the previously mentioned operation/maintenance phase risk analysis. The form identified in the information security risk analysis will be used to document the risk analysis. Completion of a risk analysis is a requirement of change management. Change control requests will not be approved without the completion of a risk analysis.
- *Neighboring Premises:* When sharing a building with other tenants or there is a facility physically located close to another facility external to the organization, a risk assessment must be conducted to assess if there are any risks or security threats presented.
- *Vulnerability (Technical) Assessments:* This risk analysis is part of Cone Health's vulnerability management program. The risk analysis will be comprised of the activity performed, subsequent report and corrective action plan or POAM. Vulnerability assessments include but are not limited to:
    - Perimeter Vulnerability Assessment (PVA)
    - Internal Vulnerability Scan (IVS)
    - Web Application Assessment

- Network Security Assessment (NSA)
- Wireless Security Assessment (WSA)
- Application Security Assessment
- Security Test and Evaluation

The remaining portion of this section is designed to help individuals understand the different components of a risk analysis.

- Risk Identification (i.e., Risk Assessment): Creating a list of risks associated with the confidentiality, integrity and availability of covered information and the covered environment.
- Risk Likelihood (Probability) of Occurrence: As with any risk analysis, there will be a level of subjectivity which cannot be avoided. If factual evidence (i.e., historical data) exists that provides insight regarding the frequency that a risk occurs. That data must be used when determining likelihood. The following table can be used to help determine the likelihood of a risk occurring when completing a risk analysis.

Sample Risk Likelihood of Occurrence Scale	
Likelihood Scale	**Definition**
LOW	• Lack of opportunity • Requires significant expertise/knowledge to circumvent controls • Little motive or potential gain • Cone Health or another similar organization have not experienced this risk • Existing controls will significantly impede or even prevent success of the risk being exercised
MEDIUM	• Some exposure through weak controls • Requires only moderate expertise to circumvent controls • May be some motive or possible gain • Cone Health or another similar organization have previously been alerted to the risk and could take steps to prevent the occurrence of the risk or minimize the harmful effects • Controls are in place that “may” impede the success of the risk being exercised
HIGH	• Easy opportunity to exploit • Few, if any, controls to circumvent • Obvious motive(s)/potential gain • Cone Health or another similar organization have experienced one or more successful occurrences of the risk being exercised • Existing controls to eliminate the risk are not very effective

- Risk Impact: In addition to the likelihood, the impact to Cone Health must also be determined. Likelihood and impact play an important role in determining how much of an investment will be made to mitigate a risk to an acceptable level. When determining impact, it is important to take into consideration the importance or criticality of the asset, data, process, etc., that would be affected by the risk, if it were to occur. The following table can be used as a guide when determining risk impact.

Sample Risk Impact Scale	
Impact Scale	**Definition**
LOW	• Limited, isolated effects • Minimal loss of confidentiality, integrity, and/or availability • Minimal disruption to operations • Loss of some tangible assets • Compliant to Cone Health • Loss of productivity • Nuisance • Embarrassment
MEDIUM	• Moderate effects • Some nontrivial loss of confidentiality, integrity, and/or availability • Moderate disruption to operations, possible public relations and/or legal impact (minor lawsuit) • Human injury or harm • Compliant to federal government • Significant cost of recovery • Loss of tangible assets
HIGH	• Severe effects • Significant loss of confidentiality, integrity, and/or availability • Significant disruption to operations, possible public relations and/or legal impact (major lawsuit) • Human death or serious injury • High cost of recovery • Inability to recover critical and/or covered information

- Risk Mitigation: The final phase of the risk analysis process is determining what, if anything, needs to be done to mitigate identified risks to an acceptable level. Risks can be dealt with in one of four ways:
    1. Avoidance: This approach eliminates the risk by avoiding the activity which provides the risk. For example, the risk associated with utilization of wireless technologies can be mitigated by deciding not to use wireless technologies at all.
    2. Reduction: Risk can be mitigated with controls that reduce the likelihood or impact of a risk. An example would be encryption of network traffic to minimize risks that threaten the confidentiality of data.
    3. Transference: Risk can be mitigated by shifting it to an outside entity. An example would be the purchase of insurance against fire damage.
    4. Acceptance: Organizations can choose to accept risk by not selecting any of the aforementioned approaches. When acceptance is selected, management agreement with this approach must be documented.

Regardless of the risk mitigation approach, Cone Health must define and document the criteria to determine whether or not a risk shall be avoided, reduced, transferred, or accepted.
The risk mitigation phase is comprised of the following two processes:

- Control Selection: Identification of potential solutions that could be implemented to reduce likelihood or impact to an acceptable level. Factors that must be taken into account when selecting controls include the following:
    - Organizational laws, regulations and standards
    - Cultural fit
    - Patient/consumer/client reactions
    - Coherence with ITS, corporate risk acceptance, and clinical strategy cost
    - Effectiveness
    - Type of protection
    - Number of threats covered
    - Risk level at which the controls become justified
    - Risk level that led to the recommendation being made
    - Alternatives already in place
    - Proper mitigation of harmful effect(s) known by Cone Health of a use or disclosure of covered information by Cone Health or its business associates, in violation of its policies and procedures.
    - Additional benefits derived
- Cost-Benefit Analysis: Estimation of the strengths and weaknesses of potential controls that satisfy management's expectations (i.e., acceptable level of risk). It is a technique that is used to determine options that provide the best approach for the adoption and practice in terms of benefits in labor, time and cost savings etc. Cost-benefit analysis needs to take the following into consideration for estimating the costs of implementation:
    - Hardware and software purchases
    - Business impact due to reduced operational effectiveness if system performance or functionality is negatively affected
    - Cost of implementing additional policies, standards and procedures
    - Cost of hiring additional personnel to implement proposed policies, standards and procedures, or services
    - Training costs
    - Maintenance costs
    - Enforcement costs

The Information Security Risk Analysis Form provides an example of a worksheet that can be used during the cost benefit analysis process. Using the impact and implementation costs for each selected control and comparing them against the asset/data value (e.g., patient care/safety, cost of replacement, federal and statutory penalties, criminal/civil litigation, reputational/brand damage, etc.) aid in determining if the total cost/impact of a selected control is adequate, affordable, appropriate or if it is excessive, insufficient, or outweighs value of the asset/data.

Performing the cost-benefit analysis, helps the DAA determine which controls are reasonable, appropriate and acceptable, allowing him/her to decide whether to forgo or proceed with implementation of the selected control(s).

It is not possible to fully eliminate risk, even when agreed upon controls are implemented. This is referred to as residual risk, which means risks that remain after selected controls have been applied.

Residual risk is what the DAA has decided he/she is willing to accept. It is important to include a description of residual risk for each selected control to help the DAA make an informed risk acceptance decision.

Risk Acceptance – DAA Approval:
Risk acceptance is the final phase of the risk analysis process. It is during this phase that the DAA, or his/her representative, accepts the results of the risk analysis. By signing the risk analysis form (or other approved type of risk analysis), the DAA is stating that they accept the recommended controls and that any residual risk, including any conditions identified by the DAA.

When submitting the risk analysis documentation (i.e., package) to the DAA for review and approval, the package must include the following:

- Risk assessment form
- Cost benefit analysis worksheet
- Recommendations from the CISO
- Plan of Action and Milestones (POAM) (if applicable)

Continuous Monitoring:
Exposure to new or evolving threats, changes in business processes and technology, etc., warrant the need for continuous monitoring. The primary purpose of continuous monitoring is to:

- Ensure controls are operating as expected and continue to protect against known threats
- Adjust, replace or remove controls when applicable (e.g., new threats are discovered, changes to business processes, etc.)
- Implemented controls remain cost-effective

Continuous monitoring can be accomplished through the use of technology (e.g., intrusion detection, audit logs, etc.) and in the form of informal audits, assessments and tests. An appropriate level of independence will also be maintained for the management of any tools or assessor teams being used to conduct these activities

Revalidation:
All risk analyses will be revalidated each year by the CISO and reapproved by the DAA for as long as the risk analysis is needed. Revalidation will be required more often when there is a significant change to an information system or the operational environment.

HIPAA Addressable Implementation Specifications:
For HIPAA Security Rule requirements that are classified as “addressable” that Cone Health cannot currently comply with, the CISO will do the following:

- Perform a risk analysis to determine if there are currently existing compensating controls in place that mitigates risk to an acceptable level until the organization can comply with the addressable implementation specification requirements. If existing controls are not adequate, the CISO, with the assistance of the DAA will determine what controls need to be implemented to adequately mitigate identified risks to acceptable level until Cone Health can fully comply with the addressable requirements.

- Establish a POAM to track mitigation activity associated to complying with the addressable implementation specification requirements.

Documentation Retention:
Risk assessments, analyses, and associated documentation will be retained for a minimum of 6 years from date of completion or revalidation, whichever is the most current.

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 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.