CONE HEALTH	**Guideline:** ITS Information Security Exception 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), and corporate internal and confidential data (hereafter all three will be referred to as covered information) it creates, receives, maintains, and/or transmits.

The purpose of this procedure is to define roles, responsibilities, and processes associated with Cone Health's information security policy exception management.

Scope and Goals:
Inability to comply with information security policies will happen from time to time and can occur for a variety of reasons beyond the control of the people involved. As a result, there may need to be an exception of a policy/procedure. This procedure was created to address how these exceptions will be reviewed, approved, and monitored while the exception remains in effect. This procedure allows management to make an informed decision about whether to grant an exception based on the understanding of the risks involved and alternatives to mitigating risk until the exception is no longer needed. Goals of this procedure are as follows:

- Assign responsibility for exception management.
- Ensure exceptions are evaluated based on formal risk management principles.

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

- Revisions, implementation, workforce education, interpretation, and enforcement of this procedure.
- Manage the exception process.
- Work with the exception requestor and gather the information needed to perform a risk analysis.
- Perform exception-based risk analyses.
- Review, approve, or deny low-risk exception requests.
- Provide recommendations to the designated approving authority to approve or deny the request for all exceptions, except those determined to be low risk.
- Notify the exception requester of conditions related to approvals or if denied, an explanation why.
- Documents specific conditions or requirements for approved exception(s).

- Continually monitor approved exceptions and at least annually, validate whether or not the exception is still required and if adequate progress is being made to eliminate the need for the exception. If it is determined the exception is still needed, document reasons why.
- Exception revocation resulting from incidents, breaches, or abuse.
- Reevaluate exceptions that significantly change from the original request.
- Maintains exception documentation.

Designated Approving Authority (DAA):
The DAA is responsible for the following:

- Review exception-specific risk analyses and approve or deny exception requests.
- Define low-risk exceptions that may be approved by the CISO.

Requestor:
Exception requestors are responsible for:

- Complete the exception request form and provide information needed to perform a risk analysis.
- Implement and maintain conditions associated with approved exception requests.
- Work toward compliance with policy/procedure and eliminating the need for the exception.
- Report changes to the CISO that could result in an exception no longer being needed or if conditions surrounding the exception change.

Exception Process:
An exception to an information security policy/procedure will be submitted using the Information Security Exception Request Form and sent to the CISO security officer for processing.
Exception requests will be evaluated in accordance with Cone Health information security risk management policy/procedures. Requests that result in significant risk to the organization, where compensating controls cannot reduce the risk to an acceptable level, will not be approved. Also, refer to the Information Security Risk Management procedure when evaluating how to comply with HIPAA Addressable Implementation Specifications.

Unless otherwise specified, exceptions are valid for one year and will be reviewed by the CISO to determine whether the exception is still needed and if the requestor is making adequate progress towards eliminating the need for the exception.

If the exception conditions change, the requestor will notify the CISO and a decision will be made to determine if another risk analysis is needed.

Documentation Retention:
Retain all documentation associated with policy/procedure exceptions for the life of exception and then for a minimum of 6 years after the exception has been resolved.

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.