

	Guideline: ITS Disposal of Covered Information Procedure	
	Department Responsible: SW-ITS-Administration	Date Approved: 05/15/2024
	Effective Date: 05/15/2024	Next Review Date: 05/15/2025

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. 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.

The purpose of this procedure is to define Cone Health’s roles, responsibilities, and processes associated with the proper disposal of hard copy (i.e., paper) covered information.

Scope and Goals:

This procedure applies to all workforce members who work with hard copy covered information. The goals of this procedure are as follows:

- Define methods for proper disposal of hard copy covered information.
- Define when hard copy covered information must need to be retained.

Responsibilities:

Chief Information Security Officer (CISO) and Chief Privacy Officer:

The CISO and chief privacy officer are responsible for, but not limited to, the following activities:

- Revisions, implementation, workforce education, interpretation, and enforcement of this procedure.
- Ensure that mechanisms/methods utilized for disposing of paper documents render covered information unusable, unreadable, or indecipherable.
- Ensure an adequate number of shred bins or containers are obtained and located in a central location for workforce members to use.
- Retain destruction documentation provided by the shredding vendor.
- Ensure the shredding vendor has the appropriate security controls in place to prevent information leakage and signs a business associate agreement.

Management:

Management will provide the budget for contracting with a National Association for Information Destruction (NAID) certified onsite shredding service.

Guideline: ITS Disposal of Covered Information Procedure

General Disposal:

Cone Health workforce members will shred all paper documents, records, etc., as soon as it has been determined they are no longer needed, in accordance with the organization's record retention guidelines.

Cone Health has contracted with a national onsite shredding company. Located throughout all of Cone Health's facilities, shred bins are provided for secure disposal of hard copy covered information and other business-related documentation. *NOTE: Newspapers, magazines, and food wrappers can be recycled or disposed of as normal waste. Do not use the secure shred bins for disposal of these items.*

In situations where work related documents cannot be disposed due to teleworking or travel, documents will be protected in a manner that prevents unauthorized access and disposed of in a shred bin at the Cone Health facility as soon as possible.

Documents deposited in shred bins do not require a Certificate of Destruction/Sanitization. The shredding service will provide their own at the time of destruction.

Destruction/Sanitization by Shredding Services:

Contracts with shredding services will specify the following:

- Destruction method(s) used.
- Safeguards in place to prevent unauthorized access to documents awaiting destruction and in transit to a destruction facility.
- Protection of Cone Health from damages due to loss, theft, or unauthorized disclosure due to the fault of the vendor.
- Liability insurance requirements.
- Requirements for providing proof of destruction/sanitization in a timely manner to Cone Health.

Retention of Records for Investigations/Audit/Litigation:

In the event of a pending investigation, audit, or ongoing litigation, Cone Health's record retention schedule shall be suspended for all paper records related to the topic in question until the situation has been resolved. If records have been requested in the course of a judicial or administrative hearing, a qualified protective order will be obtained to ensure that the records are returned to Cone Health for disposition or properly destroyed/disposed of by the requesting party, in which case the requesting party will provide a record of disposition/destruction to Cone Health.

Third Party Relationships:

All contracts between Cone Health and third-party entities must state that, upon termination of their contract with Cone Health, that they will return all covered information to Cone Health for proper disposal. The contract will also include a requirement that if the return of hard copy covered information is not feasible, the third-party entity must refrain from using or disclosing the information and return or destroy the information as soon as feasibly possible. If the entity chooses to destroy the information, they are to be required by contract to provide Cone Health with a record of disposition/destruction.

Guideline: ITS Disposal of Covered Information Procedure

Storage of Records:

Records scheduled for destruction/disposal will be secured against unauthorized or inappropriate access until the destruction/disposal of patient information is complete.

Documentation Retention:

Retain all documentation associated with the destruction of covered information for a minimum of 6 years.

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.