	Guideline: ITS Data Classification and Handling 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.). 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.).

To comply with regulatory requirements, Cone Health has established internal corporate governance for safeguarding the confidentiality, integrity, and availability of covered information the workforce creates, receives, maintains, or transmits. Cone Health will have in place appropriate administrative, technical, and physical safeguards to protect covered information. It is the policy of Cone Health to ensure that covered information is protected against misuse, loss, tampering, or use by unauthorized persons.

The purpose of this procedure is to define Cone Health's data classification schema and associated handling procedures to ensure that the organization is properly safeguarding covered information in accordance with internal and regulatory requirements.

This procedure provides guidelines that are associated with the different means of transmitting, communicating, and storing data.

Scope and Goals:
The goal of data classification and handling is to ensure that Cone Health's workforce understands the criticality and sensitivity of the data they work with and what type of security protection they need to apply when working with the data. The goal of this procedure defines the different classification levels and the type of security control that needs to be applied for each classification based on how it is being used and communicated.

Data classification transcends to media, computing devices, medical equipment, business machines, applications, systems, etc. Depending on the type of data being processed, stored or transmitted, the

asset being used takes on the same classification, until it can be sanitized in accordance with the organization's information security policy/procedure.

Responsibilities:

Chief Information Security Officer (CISO):

The CISO is responsible for working with organizational leaders to assign classification labels to data handled by the organization. The classification labels must be reviewed periodically and updated when necessary. The CISO is also responsible for providing ongoing workforce education and awareness as it pertains to data classification and handling.

Management:

The Cone Health leadership team will provide support through active enforcement, funding, and resources needed to meet the requirements of this procedure.

Workforce:

Workforce members are responsible for complying with this procedure and reporting deviations and non-compliance to the CISO. Workforce means employees, physicians, volunteers, students, trainees, and other persons whose conduct, in the performance of work for Cone Health, is under our direct control, whether or not they are paid by Cone Health.

Third-Party Contractual Relationships:

Third parties performing work on behalf of Cone Health that requires them to have access to covered information will comply with this procedure. Cone Health personnel responsible for contractual oversight will ensure requirements of this procedure are included in all contractual agreements to include a statement that non-compliance is grounds for contract termination.

Data Classifications:

All data created, processed, received, transmitted, and stored by Cone Health workforce will fall under one of the following classifications:

- Public
- Internal
- Confidential
- Protected Health Information

If you are uncertain about what classification of data you are handling, speak with your manager. If the manager is not sure of the classification, bring it to the attention of Cone Health's CISO. When the classification is unknown, the data must be classified as "Confidential."

Public:

Any data that can be given to the general public and can be distributed outside of Cone Health without any risk, through the various mediums. This is often general information about Cone Health for marketing or product purposes. Examples of public data are:

- Information that can be obtained from publicly accessible resources, in other words, anything that can be obtained from public websites, newspapers, etc.

- Internal correspondence, memoranda, or documentation that doesn't merit security classification (e.g., social event flyers, marketing material that is going to the general public, ads meant for the public, etc.)
- Press releases

Internal:
Data which if disclosed may cause the organization some financial, legal, or reputational damage. This data is typically used by workforce members during the ordinary course of business. Examples of internal data are:

- General competitive strategies (e.g., comparative matrixes, external positioning statements, PowerPoint presentations, etc.)
- Progress and status reports (e.g., weekly reports from departments and individuals to management)
- General business plans, strategies, and tactics (e.g., PowerPoint presentations for analysts).
- Any identifiable information on people interviewing with the company that could be considered covered
- Employee handbook
- Policies, standards, procedures, etc.

Confidential:
Data which if disclosed is likely to cause the organization severe financial, legal or reputational damage. Examples of confidential data are:

- Source code, internal internet protocol (IP) addresses, internal system/application security configuration
- Negotiation strategies/contracts
- Human Resources data (e.g., employee evaluations, phone listings, employee's home phone, address, medical history, social security number, etc.)
- Payroll data
- Confidential data received from or generated for Cone Health or other business partners (e.g., security assessments)
- Passwords, passcodes, key-codes, etc.
- Internal network topology/architecture and addresses
- Business financials (e.g., profit and loss, annual revenue goals, etc.)
- Data covered under any non-disclosure or confidentiality agreements, especially those with other business partners

Protected Health Information (to include electronic):
HIPAA protected health information (PHI) is any piece of information in an individual's medical record that was created, used, or disclosed during the course of diagnosis or treatment that can be used to personally identify them.

Examples of PHI are as follows:

- Prescription refills
- Instructions on how to take medications or apply dressings

- Appointment scheduling
- Appointment reminders
- Normal test results (other than HIV test results) with interpretation and advice
- Care and treatment recommendations
- Pre- and postoperative instructions
- Insurance and billing questions
- As a secondary means of attempting to have patients call the provider to discuss important test results and/or prognosis of a condition
- STD and HIV test results and/or treatment
- First means of notification for confusing or abnormal diagnostic results
- Mental health issues
- Drug and alcohol abuse and/or treatment
- Child abuse and/or neglect
- Domestic abuse
- Peer review or risk management information

FOR COVERED ENTITY: PHI can be in the form of various different media. This information will be used internally within Cone Health and received by the patient, guardian, and/or authorized personal representatives (refer to Cone Health Release of Information policy for appropriate release processes). Unauthorized disclosure could seriously and adversely impact Cone Health or our patients. Always obtain appropriate authorization for disclosures of PHI.

FOR BUSINESS ASSOCIATE: PHI can be in the form of various different media. Unauthorized disclosure could seriously and adversely impact Cone Health and our clients and their patients. Always obtain appropriate authorization for disclosures of PHI. A BAA must be in effect for third parties to receive PHI.

Management will assign responsibility to an individual(s) to manage the identification, periodic inventory (at least annually), and tracking the status of PHI stored on portable media and devices. Individual(s) assigned responsibility for managing the status of electronic PHI will track data based on the following attributes:

- Owner/person responsible for control of device or media
- Status/location
- Whether the data is encrypted or unencrypted
- Chain of custody when devices/media is transferred to a different owner
- Disposition records when devices/media is destroyed

PHI and other covered information will be stored in an encrypted format (encryption at rest). This includes information stored on servers, workstations, and other types of electronic media (e.g., laptops, tablets, smartphones, etc.). The minimum standard used for encryption will be 256 AES. If encryption is not possible or plausible, the CISO will perform a risk analysis to determine if the risk is acceptable and what additional controls will be needed. However, in the event that covered information is being stored in a non-secure area, then encryption IS required with no exceptions allowed. Risk management activities will be performed in accordance with the organization's

Information Security Risk Management procedure. The same encryption standard will also be utilized for the transmission (e.g., sFTP, email, instant messaging, etc.) of covered information (encryption in transit).

Cone Health will train workforce members on the appropriate systems and devices for the storage and transmission of covered information. This shall be technically enforced through system configuration in addition to training. However, Cone Health will also ensure that the storage and transmission of covered information is kept to a minimum. Any workforce members found using an unapproved system or device for the storage or transmission of covered information will be consider non-compliant with this procedure and be subject to disciplinary action. with this procedure and be subject to disciplinary action.

Portable media containing PHI will be properly identified in a manner that individuals handling the media understand the sensitivity of the data stored on the device.

Portable media/devices containing PHI will be properly secured with encryption and physically safeguarded against theft, loss, and unauthorized access/modification when transferring outside of the organization and its facilities, to include in between facilities. All transfers of covered information outside of controlled areas will also require management approval.

In the event that mail services are utilized for the transport of PHI or other covered information, both internally and externally, it will be sent in a secured fashion. Some examples of protecting physical mail are:

- Authorized, trained personnel must handle all mail
- Clearly label with recipient's name and verify that address information is correct
- Store all unattended mail in a closed, secure area
- Place all types of media containing any form of PHI in secured, confidential envelopes and/or containers (internal and external)
- Return address on external mail consists of Cone Health address only. There must be no mention of the contents.
- Opaque envelopes will be utilized for external mail and internal distribution of PHI to prevent viewing of information. Ensure that all envelopes are properly sealed (internal and external). PHI may be faxed to another provider for continuity of care (review the Release of Protected Health Information and Reportable Cases policy for guidelines).

Cone Health will train workforce members on the following:

- Not discussing or leaving critical information in the open or areas where unauthorized individuals could overhear or see the information
- Not leaving information on answering machines through:
  - People in their immediate vicinity, particularly when using mobile phones
  - Wiretapping, and other forms of eavesdropping through physical access to the phone handset or the phone line, or using scanning receivers; or
  - People at the recipient's end
- Not registering demographic data in software that could be collected later for unauthorized use
- Addressing the problems with printers, facsimile, and copy machines, such as:

- Unauthorized access to built-in message stores to retrieve messages
- Deliberate or accidental programming of machines to send messages to specific numbers
- Sending documents and messages to the wrong number either by misdialing or using the wrong stored number
- Registering demographic data, e.g., email address or other personal information, in any software to avoid collection for unauthorized use
- Page caches and store page functionality that modern facsimile machines and photocopiers have in case of a paper or transmission fault, which will be printed once the fault is cleared.

Release of Information:
Cone Health's Marketing and Communications Department will ensure information planned for release to the public has been reviewed to ensure regulatory requirements have been met, appropriate consent has been obtained (if applicable), information has been properly sanitized (i.e., reclassified as Public), and source (i.e., authorship) is clearly stated.

Related to the release of information, Cone Health's Health Information Management department will permit an individual (patient) to request the restriction of the disclosure of their covered information to a business associate for purposes of carrying out payment or health care operations and is not for purposes of carrying out treatment. All restriction requests will be responded to.

Covered Information Document Retention:
Cone Health's management will ensure covered information (i.e., PHI, PII, and other sensitive or protected information) adheres to the following document retention requirements:

- Data will be stored in an encrypted active, offline archived, secured physical location for 50 years after the death of an individual. Only after that can it be purged from the system/disposed of.
- Related to covered information usage notice requirements, all versions of this notice issued to patients will be retained for a period of 6 years. Any written acknowledgements of the usage notice from patients must also be retained for at least a 6-year period.
- All restrictions related to covered information usage will be documented as an organizational record for at least 6 years.
- The designated record sets that are subject to access by individuals and the Cone Health workforce members responsible for receiving and processing requests for access by individuals will be retained for at least 6 years.
- All records and documentation related to disclosures of covered information, including the information required for disclosure, the written account provided to the individual, and the Cone Health workforce member involved will be retained for at least 6 years.
- All formal policies and procedures, other critical records, and records for disclosures of protected health information are retained for a minimum of 6 years; and, for electronic disclosures of health records, including information to carry out treatment, payment, and health care operations, for a minimum of 3 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 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.