CONE HEALTH	**Policy:** Breach Notification	
	Department Responsible: SW-Corp Compliance Audit	**Date Approved:** 12/19/2022
	Effective Date: 12/19/2022	**Next Review Date:** 09/20/2025

PURPOSE:
This policy defines a breach pursuant to the HIPAA Privacy Rule and provides guidance pertaining to the steps team members and affiliates of Cone Health should take in the event they become aware of a breach. Further, the policy stipulates the steps to be taken with regard to determining the extent and nature of the protected health information (PHI) that was breached and the procedures to notify affected parties.

This policy applies to all Cone Health team members, which include employees, board members, vendors, independent contractors, students, trainees, medical professionals and specialists, volunteers, business partners and workforce members. Workforce members include all of the above listed team members (and any other persons) whose conduct, in the performance of work for Cone Health, is under Cone Health's direct control, whether or not they are paid by Cone Health.

DEFINITIONS:

- **Breach:** The acquisition, access, use, or disclosure of unsecured PHI in a manner that compromises the security or privacy of that information. Examples include loss or theft of unsecured PHI, and unauthorized access or receipt of PHI.
- **Individually identifiable health information (IIHI):** Information that is a subset of health information, including demographic information collected from an individual, and is created or received by Cone Health; and relates to the past, present or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present or future payment for the provision of health care to an individual (a) that identifies the individual or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.
- **Protected health information (PHI):** Information that is "individually identifiable health information" and is transmitted by electronic media, or transmitted or maintained in any other form or medium; except education and other records covered by the Family Educational Right and Privacy Act, and employment records held by a covered entity (Cone Health) in its role as an employer.
- **Unsecured PHI:** Information that is not unusable, unreadable, or indecipherable through technology or other means, such as by encryption or proper shredding.

POLICY:
It is the policy of Cone Health to maintain the confidentiality of PHI, and to safeguard against the unauthorized use or disclosure of PHI. Cone Health team members will report any suspected breach as soon as possible to the Cone Health Privacy team. In the event Cone Health discovers a breach of any unsecured PHI, then Cone Health will take action as required by law to notify the necessary parties, mitigate against potential harm of the breach, and take appropriate action to safeguard against the breach from recurring.

PROCEDURE:

Exceptions to Breach:

The following situations are not considered breaches and are not subject to this policy:

1. A Cone Health team member unintentionally acquires, accesses, or uses PHI and:
    a. Was made in good faith;
    b. Was acting within the scope of his/her authority at the time; and
    c. Does not further use or disclose the PHI in an impermissible manner.
2. A Cone Health team member authorized to access the PHI:
    a. Inadvertently discloses it to another person who is also authorized to access PHI at Cone Health (or at an organized health care arrangement in which Cone Health participates); and
    b. The PHI is not further used or disclosed in an impermissible manner.
3. The PHI is disclosed to an unauthorized person, but Cone Health has a good faith belief that the person could not reasonably retain the PHI.
4. Deidentified information (information that does not contain any elements of PHI) is not PHI and is not subject to this policy.

Safeguards Against Potential Breach:

Cone Health team members are expected to follow privacy and security policies, procedures, and practices to safeguard against the unauthorized use or disclosure of PHI. Failure to do so may result in corrective action and sanctions.

Discovery of Potential Breach:

1. In the event a Cone Health team member has a good faith concern that PHI has been impermissibly used, accessed, acquired, or disclosed, she/he should immediately do any of the following:
    a. Contact his/her supervisor and alert them to the concern;
    b. Report the concern to the Compliance & Privacy Helpline (1-855-809-3042);
    c. Contact the Cone Health Privacy team or anyone with Cone Health Audit and Compliance Services.
2. At a minimum, the following information should be provided in the initial report:
    a. Name of patient(s), if known, including the total number of patients affected
    b. Department/facility/practice name where the incident occurred
    c. Type of information disclosed
    d. Circumstances of the incident
    e. Date of discovery
    f. Contact information of the person making the report
3. Time is of the essence. If the incident is determined to be a breach, timely notifications to the patient and possibly others must take place in very short time frames. All notifications must be approved by Cone Health Audit and Compliance Services; departments and team members are not to notify patients, unless specifically directed to do so by Cone Health Audit and Compliance Services.

4. Business associates are required to notify Cone Health of any potential breaches of Cone Health PHI. Once a Cone Health team member is notified by a business associate of a potential breach, this policy applies.

Immediate Action in Response to Potential Breach:

1. Cone Health team members will take steps to immediately stop the unauthorized use, access, acquisition, or disclosure and mitigate any potential harm or misuse.
2. Response steps include the following:
    a. All affected PHI will be secured and recovered from the third party to the extent possible.
        i. If the PHI is with a third party, attempt to recover the PHI.
        ii. Written confirmation from the third party will be secured, if possible.
    b. If the third party has the PHI but does not or cannot return it (such as with an email), then the third party will be asked to permanently destroy the PHI.
        i. The PHI will also be permanently deleted off all electronic storage devices or media.
        ii. Written confirmation from the third party will be secured, if possible.

Determination of a Breach:

1. Cone Health Audit and Compliance Services will review the incident and conduct an investigation. Relevant Cone Health team members, departments, facilities, and practices will be notified of the potential breach and will cooperate in the investigation.
2. Cone Health Audit and Compliance Services will determine whether the unauthorized acquisition, access, use, or disclosure of PHI constitutes a breach, or whether there is a "low probability" that the PHI has been compromised, based on at least the following considerations:
    a. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
    b. The unauthorized person who used the PHI or to whom the disclosure was made;
    c. Whether the PHI was actually acquired or viewed; and
    d. The extent to which the risk to the PHI has been mitigated.
3. Cone Health Audit and Compliance Services is authorized to engage resources both within and outside of Cone Health to assist with the investigation and evaluation of the potential breach.
4. The investigation, evaluation, and breach determination will be documented.

Breach Notification:

1. Time Period: Unless law enforcement has directed otherwise, notification of a breach must occur without unreasonable delay, but no later than within 60 calendar days of discovery by Cone Health, including by its team members.
2. Patient Notification Letters:
    a. If the incident is determined to be a breach, Cone Health Audit and Compliance Services will prepare the required notifications in conjunction with Legal Services and Information Technology Services, as appropriate. No other departments are to issue communications to the patients, the media, or any other agency, unless specifically directed by the Cone Health chief privacy officer or designee.

b. At a minimum, patient notification letters will include the following:
    i. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
    ii. A description of the unsecured PHI involved in the breach (i.e., whether full name, Social Security Number, date of birth, home address, account number, diagnosis, disability code, or other types of identifying information were involved);
    iii. Any steps individuals should take to protect themselves from potential harm resulting from the breach;
    iv. A brief description of what Cone Health is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and,
    v. Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, e-mail address, web site, or postal address.
    vi. Depending on the nature of the breach, credit monitoring may be offered.
c. Notifications are to be written in plain English.
d. If the breach is determined to originate from a Cone Health business associate, the business associate may be responsible for providing the notices, subject to the decision and approval of Cone Health.
e. A third party contractually engaged by Cone Health may be used to prepare and send the notification letters, and other duties as assigned.

3. Parties to Be Notified:
    a. The following notifications will take place for breaches of under 500 patients located in one state, as required:
        i. To the patient or his/her authorized representative within 60 days of discovery.
        ii. To the Office for Civil Rights in the annual report submitted by Audit and Compliance Services.
        iii. To the state Attorney General as required by law.

    b. The following notifications will take place for breaches of over 500 patients located in one state, as required:
        i. To the patient or his/her authorized representative within 60 days of discovery.
        ii. To prominent media outlets serving the state of the 500 or more patients
            a) Media notification is to be issued at, or close to, the same time as the patient letters are issued.
            b) Media notification is to be handled by Media Relations.
        iii. To the Office for Civil Rights (OCR)
            a) OCR notification is to be issued contemporaneously with patient letters.
            b) OCR notification is to be handled by Audit and Compliance Services.
        iv. To the state Attorney General as required by law.
4. Methods of Patient Notification:
    a. Written notice is to be provided by first-class mail to the patient at the last known address (or that of his/her representative). Notification may also be provided by secure email if the patient has agreed to electronic notice and has not withdrawn that agreement.

b. If there is insufficient or out-of-date contact information for the patient, then substitute notice can be provided as follows:
    i. If fewer than 10 patients have insufficient contact information, then substitute notice may be done by an alternative form of written notice, telephone, or other means.
    ii. If 10 or more patients have insufficient contact information, then substitute notice will be as follows:
        a) A conspicuous posting of information about the breach on the Cone Health and facility home page of the web site for a period of 90 days, or
        b) A conspicuous notice in major print or broadcast media in geographic areas where the patients affected by the breach likely reside for a period of 90 days.

    Both methods will include a toll-free phone number that remains active for at least 90 days through which the patient can learn whether their information was included in the breach.
c. If there is a good faith concern that the breach could result in imminent misuse of the unsecured PHI, then the patient may be notified by telephone or other means in addition to the other forms of notice.
d. No patients are to be specifically identified in any public notifications or information about the breach.

5. Inquiries Following Notification:
    a. Any inquiries from the media are to be directed to Media Relations; only Media Relations is authorized to speak to the media.
    b. Any inquiries from patients or other parties are to be directed to the point of contact designated by Audit and Compliance Services for the specific breach. This may include the department/facility/practice leader, a third-party vendor, an administrator, Office of Patient Experience, or the Cone Health Chief Privacy Officer, depending on the nature of the breach.
6. Remediation and Documentation:
    a. Cone Health will take appropriate action to remediate the breach, including but not limited to:
        i. Appropriate and relevant education
        ii. Review of processes and practices for possible additional safeguards
        iii. Corrective action, as appropriate
        iv. Other actions and safeguards as appropriate and relevant
    b. Documentation related to the breach will be maintained for at least 6 years.

Burden of Proof:
Cone Health or its business associate, if applicable, will have the burden of demonstrating that all notifications were made as required, or that the use or disclosure did not constitute a breach based on the low probability that the PHI was compromised.

REFERENCE DOCUMENTS/LINKS:
HIPAA Privacy Rule, 45 C.F.R. § 164.400 through 164.414