Policy Title: Breach Notification			
Department Responsible: THN Compliance & Integrity	**Policy Number:** SEC-112	**THN's Effective Date:** January 1, 2022	**Next Review/Revision Date:** September 30, 2024
Title of Person Responsible: THN Director of Compliance & Privacy	**THN Approval Council:** THN Compliance and Privacy Committee	**Date Committee Approved:** **June 9, 2023**	**Date Approved by THN Board of Managers:** August 15, 2023

I. **Purpose.** The purpose of SEC-112 is to provide instruction to all Triad HealthCare Network (THN) workforce members regarding the requirements for notification to the HIPAA Privacy Officer in the event of the unauthorized use, disclosure, theft, or loss of unsecured PHI and to articulate company policies and procedures related to breach notification as required under HITECH.

II. **Policy.** It is the policy of THN that all workforce members of THN and its current and future subsidiaries give notice to the HIPAA Privacy Officer if there is an inadvertent disclosure of PHI about a patient to a third party in any form. This notice must be given within 1 business day, if not sooner, of discovery of unauthorized use, loss, theft, or disclosure.

III. **Procedure.**

A. *Step 1 – Discovery.*

1. A breach of PHI will be deemed "discovered" as of the first day THN knows of the breach or, by exercising reasonable diligence, would or should have known about the breach.

B. Step 2 – Reporting.

1. If a breach of PHI or PII from or derived from the CMS data files, loss of these data or improper use or disclosure of such data , you must immediately notify the HIPAA Privacy Officer. The Privacy Officer is required to report the breach to the CMS Action Desk by telephone at (410) 786-2580 or by e-mail notification at cms_it_service_desk@cms.hhs.gov.
2. Enter a report into Navex at www.conehealth.ethicspoint.com Please provide all the information that you have available to you regarding the potential breach, including names, dates, the nature of the PHI potentially breached, the manner of the disclosure (e.g., fax, e-mail, mail, verbal), all employees involved, the recipient, all other persons with

knowledge, and any associated written or electronic documentation that may exist.

3. Notification and associated documentation may itself contain PHI and should only be given to the HIPAA Privacy Officer.
4. Please do not discuss the potential breach with anyone else and do not attempt to investigate. These tasks will be performed by the THN HIPAA Privacy Officer.

C. *Step 3 – Investigation.*

1. Upon receipt of notification of a potential breach, the THN HIPAA Privacy Officer (or his/her designee) shall promptly investigate.
2. The investigation shall include interviewing employees involved, collecting written documentation, and completing all appropriate documentation.
3. The THN HIPAA Privacy Officer shall retain all documentation related to potential breach investigations for a minimum of 10 years.

D. *Step 4 – Risk Assessment.*

1. After the investigation is complete, the THN HIPAA Privacy Officer will perform a Risk Assessment. The purpose of the Risk Assessment is to determine if use or disclosure of PHI constitutes a breach and requires further notification to the Covered Entity.
2. A "reasoned judgment" standard will be applied to the Risk Assessment, which shall be fact-specific, and shall include consideration of the following factors:
    a. Did the disclosure involve unsecured PHI in the first place?
    b. Who impermissibly used or disclosed the unsecured PHI?
    c. To whom was the information impermissibly disclosed?
    d. Was it returned before it could have been accessed for an improper purpose?
    e. What type of unsecured PHI is involved and in what quantity?
    f. Was the disclosure made for any improper purpose?
    g. Is there the potential for significant risk of financial, reputation, or other harm to the employee whose PHI was disclosed?
    h. Was immediate action taken to mitigate any potential harm?
    i. Do any of the specific breach exceptions apply?

E. *Step 5 – Final Determination by the THN HIPAA Privacy Officer.*

1. The THN Privacy Officer shall have final authority to determine whether a breach of unsecured PHI occurred and what, if any, further action is warranted.

F. *Step 6 – Documentation*.
   1. All phases of the process must be documented in detail on a case-specific basis, in a manner sufficient to demonstrate that all appropriate steps were completed. All supporting documentation associated with the potential breach shall be kept on file for a period of 10 years.

G. Step 7 – Notice to Affected Individuals.
   a. If a breach has occurred requiring notice to affected individuals, that notice shall be sent in a timely manner, as required by the HITECH provisions of the American Recovery and Reinvestment Act, and in the manner prescribed therein.

Date	Reviewed	Revised	Notes
January 1, 2022			Originally Published for DCE
May 2023		X	Converted to REACH