

Policy Title: Compliance with Privacy Requirements			
Department Responsible: THN Compliance & Integrity	Policy Number: SEC-001	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-001 is to outline (1) Triad HealthCare Network's (THN's) policies for ensuring compliance with all privacy requirements, and (2) procedures to ensure that THN's practices are consistent with its stated policies.
- II. **Policy.** It is the policy of THN to maintain the privacy and security of all THN-Related Information in accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules, Accountable Care Organization (ACO) Realizing Equity, Access and Community Health (REACH) model requirements and the HIPAA-Covered Data Disclosure Request Form submitted to the Centers for Medicare and Medicaid Services (CMS), all relevant HIPAA Privacy and Security guidance applicable to the use and disclosure of protected health information, as well as applicable state laws and regulations.
- III. **Procedure.**
 - A. THN requires that all THN-Related Activities comply with all elements of applicable federal and state laws, regulations and standards governing privacy of health care information in accordance with HIPAA and Privacy Rules, the Health Information Technology for Economic and Clinical Health (HITECH) Act, part of the American Recovery and Reinvestment Act (ARRA) of 2009, Gramm-Leach-Bliley Act (GLBA), the ACO REACH Model PA, and the HIPAA-Covered Disclosure Request Form submitted to the Centers for Medicare and Medicaid Services (CMS).
 - B. THN is the Business Associate of each ACO Participant. Any data shared by THN will be done only in accordance with the Business Associate Agreement signed by each ACO Participant.
 - C. THN's Compliance and Privacy Officer is responsible for ensuring compliance with this privacy policy and utilizes THN's Monitoring & Oversight program to ensure that THN is compliant with all applicable privacy regulations and standards.
 - D. THN requires all Related Individuals to use the best practices listed below in an effort to protect Beneficiaries' personally identifiable information (PII), protected health information (PHI), and other sensitive data:



1. Avoid sharing PII, PHI, or sensitive data by e-mail. If data must be e-mailed, it is sent as an encrypted file.
 2. Passwords for encrypted files are not sent via e-mail.
 3. Passwords are not shared.
 4. Work information is not sent to or from personal e-mail accounts.
- E. Privacy concerns are reported to the Compliance Officer and investigated according to THN's CIT policies. The report, investigation and any follow-up activities are documented in the Compliance Log, as required by CIT-003
- F. THN's Compliance Officer (or his or her designee) is responsible for reporting violations as required by the regulations, and in accordance with AMO-001 policy regarding reporting to law enforcement.
1. THN shall take reasonable steps to mitigate, to the extent practicable, any harmful effect (that is known to THN) of a use or disclosure of PHI by THN in violation of an agreement with a ACO Participant, or the HIPAA-Covered Data Disclosure Request Form submitted to the Centers for Medicare and Medicaid Services (CMS).
- G. As part of its participation in the ACO REACH Model, THN has signed a Participate Agreement with CMS. THN will only use and share data in accordance with the terms of and for the purposes described in that agreement.
1. Information received from CMS as part of THN's participation in the ACO REACH Model may only be shared and used within the legal confines of THN and its ACO Participants and Preferred Providers to enable THN to improve care integration and be a patient-centered organization.
 2. THN will disclose, use, and reuse the data only as specified in the ACO REACH Model PA and not for any other purpose, including, but not limited to conducting communications or activities related to Medicare Advantage or any other Medicare managed care plan.
 3. THN may not sell, rent, lease, loan or otherwise grant access to the data covered by the ACO REACH Model PA,
 4. CMS data files may not be moved, transmitted, or disclosed in any way from or by the site of the custodian indicated in the HIPAA Covered Disclosure Request Attestation and Data Specification Worksheet except that:
 - a. THN may reuse original or derivative data without prior written authorization from CMS for clinical treatment, care management and coordination, quality improvement activities and provider incentive design and implementation but shall not disseminate individually identifiable original or derived information received from CMS to anyone who is not a:

- i. HIPAA Covered Entity (CE) Participant or Preferred Provider in a treatment relationship with the Beneficiary(ies);
 - ii. HIPAA Business Associate (BA) of such a CE Participant or Preferred Provider;
 - iii. Sub-BA to THN, which is hired by THN to carry out work on behalf of the CE Participants or Preferred Providers; or
 - iv. Non-Participant HIPAA CE in a treatment relationship with the Beneficiary(ies).
 5. Use of any CMS data in the creation of any document concerning the purposes of the ACO REACH Model must adhere to CMS' current cell size suppression policy. No cell representing 10 or fewer beneficiaries may be displayed, and no use of percentages or other mathematical formulas may be used if they result in the display of a cell representing 10 or fewer Beneficiaries.
- H. THN has designated a Custodian of the CMS data files who is responsible for the observance of all conditions of use and disclosure of data received from CMS and any derivative data files, and for the establishment and maintenance of security arrangements as specified in the ACO REACH Model PA to prevent unauthorized use or disclosure. This individual is responsible for contractually binding any downstream recipients of such data to the terms and conditions of this agreement.
 1. Requests to share data with any vendors or contractors are submitted to THN's Compliance Officer. Once appropriate documentation is received, the Compliance Officer provides notification to the appropriate individual within THN to allow for the sharing of data, as necessary.
 2. THN shall notify CMS within 15 days of any change of custodianship.
- I. **Access to Information:** Within fifteen (15) business days of a written request by a Participant, Preferred Provider, or a Beneficiary for access to PHI, THN shall make available such PHI.
- J. **Availability of PHI for Amendment:** Within fifteen (15) business days of receipt of a written request from a Participant or Preferred Provider for the amendment of an Individual's PHI maintained by THN, THN shall provide such information for amendment and incorporate any such amendments in the PHI as required by 45 C.F.R. §164.526. If THN receives a request for amendment to PHI directly from a Beneficiary, THN shall forward such request to the Participant or Preferred Provider within ten (10) business days.
- K. **Accounting of Disclosures:** Within thirty (30) business days of written notice by a Participant or Preferred Provider that it has received a request for an accounting of disclosures of PHI (other than disclosures to which an exception to the accounting requirement applies), THN shall make available such information as is in THN's possession and is required for



the Participant or Preferred Provider to do the accounting required by 45 C.F.R. §164.528.

- L. Each THN-Related Individual is required to complete Compliance Training, including HIPAA and Privacy training, upon hire or contracting and at least annually thereafter. THN’s Compliance Officer is responsible for ensuring the appropriate documentation of training completions and retention of training records. THN’s Compliance Officer is also responsible for ensuring that this training is reviewed and updated as needed, but no less than annually.
- M. All data requests, uses and disclosures are limited to the minimum necessary to achieve the purposes of THN and the ACO REACH Model.

IV. **Reporting.** THN’s Compliance Officer reports on any privacy issues to the Compliance and Privacy Committee at least quarterly. Any breach of PHI or PII derived from data files received from CMS, loss of these data or improper use or disclosure of such data will be reported to the CMS Action Desk by telephone at (410) 786-2850 or by e-mail notification at cms_it_service_desk@cmsahhs.gov within one hour.

V. **Enforcement.** Any workforce member found to have deliberately violated this policy shall be subject to disciplinary action up to and including termination of employment. In the case where inappropriate access, use, or disclosure of PHI was or may have been involved, such workforce members may additionally be reported to the appropriate enforcement agencies.

Date	Reviewed	Revised	Notes
January 2022			Originally published for DCE
May 2023		X	Converted to REACH