| **Policy Title:** Data Use, Disclosures, and Protections | | | |
|---|---|---|---|
| **Department Responsible**: THN Compliance & Integrity | **Policy Number:** SEC-103 | **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.** SEC-103 outlines Triad HealthCare Network's (THN's) policies and procedures regarding data use, disclosures, and protections of protected health information (PHI) and personally identifiable information (PII).

II. **Policy.** THN will ensure that PHI or PII accessed by employees will be in accordance with all federal and state regulatory requirements and laws, and only the minimum information needed to treat patients, complete payment transactions, or conduct healthcare operations will be viewed. If PHI or PII must be disclosed to other employees, outside entities or individuals, or otherwise, providers are responsible for ensuring only authorized individuals are granted access and proper paperwork is completed and filed. Providers and employees should only send PHI or PII via secure e-mail or they must take the proper steps to de-identify the data before sending such information electronically.

III. **Procedure.**

A. THN employees should do the following to ensure beneficiary data is protected:

1. Execute the required CMS DUA agreement;
2. Treat all medical and financial information as confidential;
3. Share medical and financial information only with people authorized to receive or require such information;
4. Make reasonable attempts to limit the information shared to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. This does not apply to the following situations:
    a. Uses or disclosures to or requests by health care physicians or other providers;
    b. Uses or disclosures to the patient as provided in the regulations;
    c. Disclosures made to the Secretary of Health and Human Services that are permitted by the regulations;
    d. Uses or disclosures required by law; and
    e. Uses or disclosures required for compliance with regulations.
5. Investigate any potential unauthorized or non-permitted disclosures, following all

regulations and notification requirements, as required.

B. State and federal law permit and require certain receipts, uses, and disclosures of PHI such as those related to Business Associate agreements. Additional uses and/or disclosures are allowed or required that relate to public responsibility that require no agreement or authorization on the part of the patient who is the subject of the PHI. It is the policy of THN to obtain, use, and disclose PHI only as permitted and/or required by law or regulation including the following situations:
    1. *Treatment, Payment, or Healthcare Operations*: PHI may be used or disclosed for the purposes of providing billing services or healthcare operations. Such disclosures will be made only as allowed by and pursuant to prevailing state and federal law.
        a. Discussions involving PHI shall be conducted only in appropriate business areas including but not limited to offices, conference rooms, and other non-public areas;
        b. Conducted only for the purpose of fulfilling a legitimate business need; and
        c. Conducted with regard to and in compliance with the "minimum necessary provision."
    2. *Contained in a Business Associate Agreement*: For permitted and required uses or disclosures of PHI that are consistent with those authorized by the Covered Entity in a Business Associate Agreement.
        a. *Required by Law*: PHI may be used or disclosed to the extent such use or disclosure complies with and is limited to the requirements of such law.
            i. *Judicial Proceedings*: PHI may be disclosed in response to a court date.
            ii. *Law Enforcement*: PHI may be disclosed for the following law enforcement purposes and under the specified conditions:
                A. Pursuant to court order or as otherwise required by law, i.e., laws requiring the reporting of certain types of wounds or injuries; and
                B. Decedent's PHI may be disclosed to alert law enforcement to the death if the entity suspects that death resulted from criminal conduct.
        b. *Specialized Government Functions*:
            i. *National Security and Intelligence:* PHI may be disclosed to authorized federal officials for the conduct of lawful intelligence, counterintelligence, and other activities authorized by the National Security Act.
            ii. *Protective Services*: PHI may be disclosed to authorized federal officials for the provision of protective services to the President, foreign heads of state, and others designated by law, and for the conduct of criminal investigations of threat against such persons.
            iii. *Public Benefits:* PHI relevant to administration of a government program providing public benefits may be disclosed to another

governmental program providing public benefits serving the same or similar populations necessary to coordinate program functions or improve administration and management of program functions.

c. *Workers' Compensation:* PHI may be disclosed as authorized and to the extent necessary to comply with laws relating to workers' compensation and other similar programs.

3. The following procedures will be implemented to ensure that this policy is effectively enforced across all parts of the company:
    a. Any request for disclosure of PHI pursuant to a court order, warrant, or subpoena must be directed to the appropriate company employee for review and action.
    b. Any request for disclosure of PHI by a law enforcement agent must be directed to the appropriate company employee for review and action.
    c. Any request for disclosure of PHI by a public health authority must be directed to the appropriate company employee for review and action.
    d. Any request for disclosure of PHI by a national security, intelligence, or other federal agency must be directed to the appropriate company employee for review and action.
4. The Minimum Necessary Requirement does not apply to:
    a. Disclosures to or requests by a health care provider for treatment purposes;
    b. Uses or disclosures made to the individual who is the subject of the patient information (with possible exception of psychotherapy notes);
    c. Uses or disclosures made pursuant to a valid and HIPAA-compliant authorization;
    d. Disclosures requested;
    e. Disclosures made to the U. S. Department of Health and Human Services (DHHS) when disclosure of information is required for enforcement purposes (e.g., in response to a complaint filed with the Secretary of DHHS); and
    f. Uses and disclosures that are required by law (e.g., victims of abuse, neglect, or domestic violence; judicial administrative proceeding; and law enforcement purposes).
5. Each employee has a unique user ID and password combination to provide security and ensure accountability.
    a. Users, remote or internal, accessing THN networks and systems must be authenticated. The level of authentication should be appropriate to the data classification. Authentication includes but is not limited to:
        i. Biometric identification;
        ii. Passwords;
        iii. Personal Identification Numbers;
        iv. Telephone Callback Numbers; and
        v. Tokens.

b. All workstations used for THN business must use an access control system approved by THN. This process may involve password-enabled screen savers with a time-out-after-no-activity feature and a power-on password for the CPU and BIOS. Active workstations should not be left unattended unless properly locked by the user. Users are held responsible for any activity conducted under their logins.

6. A notice should be displayed when employees log on to the system saying it is private and that only the authorized user should have access, others should logout immediately.
7. THN will implement approved controls, such as user logon scripts, menus, session managers, and other access controls to limit user access to only those network applications and functions for which they have been authorized.
8. Users should only have access to information on a “need-to-know" basis, meaning users should not have access to applications or privileges beyond what is needed to perform their jobs.
9. Prior to receiving system access, THN employees must sign a compliance statement indicating that the user understands and agrees to abide by THN policies and procedures with confirmation required at least annually thereinafter.
10. Logins and auditing trails are based on the data classification of the systems. Logs of all THN internal network access shall be audited and maintained.
    a. To the extent possible, access to confidential systems will be logged and audited in a manner that allows the following information to be deduced:
        i. Access time;
        ii. User account;
        iii. Method of access; and
        iv. All privileged command must be traceable to specific user accounts.
    b. Audit trails for confidential systems shall be backed up and stored in accordance with THN back-up and disaster recovery policies. All logs must be audited on a periodic basis and results should be included in management reports.
    c. Employees who are not workforce members, contractors, consultants, or business partners must not be granted a user-ID or otherwise be given privileges to use THN computers or information systems unless the written approval of the Chief Information Officer has been first obtained.
    d. Workforce members are prohibited from gaining unauthorized access to any other information systems or in any way damaging, altering, or disrupting the operations of these systems.
    e. As corporate systems contain PHI and may contain claim recipient information, remote access must conform at minimum to statutory requirements.

C. THN Approved Method of De-identification.

1. The only approved method for de-identifying information at THN is the safe-harbor method, unless the Chief Compliance & Privacy Officer (or designee)

approves an exception.

2. If the information is de-identified and no means of re-identification is supplied to the recipient of the information, it is not subject to the HIPAA Privacy Rule.
3. If the information is re-identified, the information once again becomes PHI and is subject to HIPAA's privacy regulations.
4. Each THN provider of information, regardless of form, will be responsible for determining whether the information requested contains patient identifiers and is therefore subject to HIPAA's privacy regulations. A log of requests and decisions about providing PHI should be maintained by all formal and informal data providers, such as those areas that produce reports for decision support or receive report/data/information and pass it on to others.
5. Information is considered de-identified when THN has no reasonable basis to believe that the information can be used to identify an individual patient. To de-identify information, the following 18 data elements of the individual or of relatives, employers, or household members of the individual must be removed:
    a. Names;
    b. All geographic subdivisions smaller than a state;
    c. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death, encounter dates, and surgery date;
    d. Telephone numbers;
    e. Fax numbers;
    f. Electronic mail (e-mail) addresses;
    g. Social Security numbers;
    h. Medical record numbers;
    i. Health plan beneficiary numbers;
    j. Account numbers;
    k. Certificate/license numbers;
    l. Vehicle identifiers and serial numbers, including license plate numbers;
    m. Device identifiers and serial numbers;
    n. Web;
    o. Internet Protocol (IP) address numbers;
    p. Biometric identifiers, including finger and voice prints;
    q. Full face photographic images and any comparable images; and
    r. Any other unique identifying number, characteristic, or code that may identify an individual.

D. Special Circumstances De-identification

1. A limited data set may be used for research, public health, and health care operation activities provided the data does not include direct identifiable information (i.e., name, street address, etc.).
2. A Data Use Agreement, which is defined as a documented agreement between THN and the recipient of a limited data set, is required for use of the limited data set. Data Use Agreements must:

a. Establish the permitted uses and disclosures of the limited data set. The agreement may not authorize the limited data set recipient to use or further disclose the information in a manner that would violate the requirements set forth in this policy.
b. Establish who is permitted to use or receive the limited data set.
c. Provide that the limited data set recipient will:
    i. Not use or further disclose the information other than as permitted by the Agreement or as otherwise required by law;
    ii. Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the agreement;
    iii. Report to THN any use or disclosure in violation of the agreement of which the recipient becomes aware;
    iv. Ensure that any agents, including a subcontractor, to whom it provides the limited data set agrees to the same restrictions and conditions that apply to the limited data set recipient; and
    v. Not identify the information or contact the individuals.

3. The following elements may be used in a limited data set:
    a. Age (individuals 90+ years old must be aggregated to prevent potential identification);
    b. Race;
    c. Ethnicity;
    d. Marital status;
    e. Random or fictional codes that can be used to link cases or re-identify the health information at a later time. A code may not be a derivative of the Security number or other identifiable numerical code (i.e., birth date, fax number, etc.).
4. Questions concerning de-identification of patient information should be forwarded to THN's Compliance & Privacy Department.

E. Process for Re-identification
1. The THN information provider may assign a code to allow de-identified information to be re-identified. The code or mechanism used to re-identify information may not be derived from information related to the individual or otherwise information that could be translated to identify the individual.
2. The THN information provider is prohibited from disclosing the mechanism/codes for re-identification (i.e., tables, codes, or algorithms). If the THN user discloses a key or mechanism for re-identification of the health information, the information is no longer considered de-identified and the exemption to the HIPAA Privacy Rule no longer applies (i.e., patient consent and/or authorization is required prior to use).

F. Use of Patient Information
1. THN will identify the classes of persons or job titles within the THN workforce who need access to PHI to carry out their job duties and responsibilities described in

the THN job descriptions.

2. THN will authorize access to computerized health information. Use of this information will be limited based on reasonable determination regarding an individual's position and/or department.
3. An individual's access will be controlled via ID and password. The sharing of logon IDs and passwords is prohibited.

G. Routine or Recurring Requests and Disclosures for Patient Information
   1. Requests for patient information made on a routine or recurring basis shall be limited to the minimum amount of patient information necessary to meet the needs of the request/disclosure.
   2. Minimum necessary definitions and standard protocols will be established for routine and recurring requests/disclosures (e.g., patient information that is routinely disclosed to a medical transcription service).
   3. Individual review of the request will not be required for requests/disclosures made on a routine or recurring basis where standard protocols have been developed; however, periodic review should be made for routine or recurring requests to ensure the requests are still valid and necessary.

H. Non-routine Requests for Disclosure of Patient Information
   1. Non-routine requests for patient information will be reviewed on an individual basis to limit the patient information requested/disclosed to the minimum amount necessary to accomplish the purpose of the request/disclosure.
   2. Such requests will be reviewed on an individual basis unless the request/disclosure is to a health care provider for treatment purposes.
   3. Disclosures/requests authorized by the patient's legal representative will not be subject to the Minimum Necessary Standard but are subject to the terms of the authorization.
   4. THN may not use/disclose an entire medical record if it is determined, after conversation with the requestor or by established protocol, that the entire medical record is not justified as the amount that is reasonably necessary to accomplish the purpose of the use/disclosure.

I. Reasonable Reliance
   1. THN may rely on the judgement of the party requesting the disclosure as to the minimum amount of patient information reasonably necessary for the stated purpose, when:
      a. Making permitted disclosures to public officials, if the public official presents that the patient information is the minimum necessary for the stated purpose(s);
      b. The patient information is requested by another covered entity (i.e., health care provider, health plan or health care clearinghouse);
      c. The patient information requested is the minimum necessary for the stated purpose and requested by a professional who is requesting patient information for the purpose of providing professional services to THN (e.g.,

member of THN workforce or business associate of THN); or

d. The documentation or representations comply with the applicable provisions for using/disclosing patient information for research purposes and have been provided by a person requesting the patient information for such purposes (e.g., appropriate documentation from the Institutional Review Board).

1. THN workforce members should exercise judgement/discretion when making determinations about disclosures and limit the disclosure to the amount of patient information necessary to satisfy the purpose of the request.

***Do you believe a data breach has occurred, and you need to report it? Please reference SCE-112 for specific instructions on how to report your concerns.***

| Date | Reviewed | Revised | Notes |
|---|---|---|---|
| January 1, 2022 | | | Originally Published for DCE |
| May 2023 | X | | Reveiwed for REACH – no changes |
| | | | |
| | | | |
| | | | |
| | | | |