

# State of Tennessee

## Department of Health



### HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) Policies and Procedures Manual

Effective January 4, 2022

State of Tennessee  
Department of Health  
Health Insurance Portability and Accountability Act (HIPAA)  
Policies and Procedures Manual  
(Effective January 4, 2022)

Table of Contents

---

<u>Policy No.</u>	<u>Title of Policy</u>	<u>Eff./Rev. Date</u>	<u>Page in PDF</u>
101	HIPAA Hybrid Entity Designation	January 4, 2022	3
102	HIPAA Definitions	January 4, 2022	8
103	Administrative Requirements for the Implementation of HIPAA	January 4, 2022	11
104	Clients Privacy Rights	January 4, 2022	16
105	Uses and Disclosure of Client Information	January 4, 2022	28
106	Minimum Necessary Information	January 4, 2022	40
107	Administrative, Technical, and Physical Safeguards	January 4, 2022	44
108	Use and Disclosure for Research Purposes and Waivers	January 4, 2022	46
109	De-identification of Client Information and Use of Limited Data Sets	January 4, 2022	52
110	Business Associates	January 4, 2022	57
111	Enforcement, Sanctions, and Penalties for Violations of Individual Privacy	January 4, 2022	62
112	Mitigation Efforts	January 4, 2022	64
113	Breach Notification of Unsecured Protected Health Information	January 4, 2022	65

Tennessee Department of Health

HIPAA Policies

Privacy

**Policy Title:** HIPAA Hybrid Entity Designation

**Policy Number:** 101

**Effective Date:** January 4, 2022

**PURPOSE:**

To define the State of Tennessee, Department of Health (“TDH”) as a hybrid entity and designate its HIPAA covered health care components, in accordance with the privacy regulations promulgated pursuant to the Health Insurance Portability and Accountability Act (“HIPAA”), Public Law 104-191 and the Health Information Technology for Economic and Clinical Health Act (“HITECH Act”), Public Law 111-5. This HIPAA Hybrid Entity Designation Policy addresses the requirements of 45 C.F.R. §§ 164.103 and 164.105.

**POLICY:**

**General:**

1. Scope. This policy applies to all offices, divisions, programs, and workforce members of TDH health care components identified under Section 3 of this policy.
2. Background.
  - a. TDH is a public health authority as defined at 45 C.F.R. § 164.501.
  - b. County health departments in Tennessee, operating under the direct supervision of TDH, are HIPAA covered entities. Some larger urban counties, including Madison, Shelby, Knox, Davidson, Hamilton and Sullivan, have health departments that operate under local governance and are separate legal entities.
  - c. A single legal entity that is a HIPAA covered entity, whose activities and services include both HIPAA covered and non-covered functions, may elect to be a hybrid entity by designating its HIPAA covered components. Health care components are any TDH component that, if a separate legal entity, would meet the definition of a covered entity or business associate.
  - d. By choosing to be a hybrid entity, a legal entity may limit application of HIPAA to only its health care components. For example, an agency that includes a health clinic that conducts HIPAA covered transactions electronically (*e.g.*, electronic

claim submission) is a covered entity component, and the legal entity must designate the clinic as part of the hybrid entity's health care component. The single legal entity must also include the claims submission department that handles the clinic's billing as a health care component because the claims submission department serves as a business associate to the clinic.

- e. A single legal entity may choose to include a non-covered health care provider as part of the health care components. For example, an agency may decide to include its laboratory in its health care components, even though its laboratory does not conduct any covered transactions.

3. Designation of Health Care Components. TDH designates the following Divisions/Offices as health care components:

a. Covered entity components:

- i. Community Health Services, Regional and Local Health Departments
- ii. Community Health Services, Office of the Medical Director
- iii. Laboratory Services, Office of the Knoxville Regional Lab Director
- iv. Laboratory Services, Office of the Clinical Division Director
- v. Laboratory Services, Office of Laboratory Services Director

b. Business associate components:

- i. Community Health Services, Office of the Assistant Commissioner
- ii. Community Health Services, Office of the Fiscal Administrator
- iii. Community Health Services, Business Solutions
- iv. Community Health Services, EMR Solutions
- v. Community Health Services, Administrative Services
- vi. Family Health & Wellness, Reproductive & Women's Health Section
- vii. Laboratory Services, Administration
- viii. Laboratory Services, Office of the Administrative Director
- ix. Communications & Media Relations

- x. Compliance & Ethics
  - xi. Office of the General Counsel, Non-Health Licensure, Regulation Attorneys & Staff
  - xii. Office of the Chief Medical Officer
  - xiii. Core Informatics, Office of Informatics and Analytics\*
  - xiv. Quality Improvement
  - xv. Office of the Deputy Commissioner for Population Health
  - xvi. Administrative Services
  - xvii. Information Technology Services
- c. This designation is based upon the “Tennessee Department of Health’s HIPAA Hybrid Assessment Findings and Recommendations, Final Report” dated June 7, 2021.
  - d. Whenever TDH policies, procedures, or guidelines refer to TDH as covered under HIPAA, they refer *only* to the health care components listed above.
4. General Procedures and Responsibilities. As a hybrid entity, TDH must ensure that:
- a. Its health care components do not use or disclose PHI to another component of the covered entity in circumstances in which the HIPAA Privacy Rule would prohibit such disclosure if the health care component and the other component were separate and distinct legal entities.
  - b. Its health care components protect access to electronic PHI by TDH’s non-covered components within the hybrid entity, in compliance with the HIPAA Security Rule, as if the health care components and the non-covered components were separate and distinct legal entities.
  - c. If a workforce member performs duties for **both** the health care component in the capacity of a member of the workforce of such component **and** for another non-covered component of the entity in the same capacity with respect to that component, such workforce member must not use or disclose PHI created or received in the course of, or incident to, the member's work for the health care component in a way prohibited by HIPAA.

---

\* Advanced Analytics & Visualization and Data Governance, Office of Informatics and Analytics are designated as non-covered components.

5. Health Care Component Procedures and Responsibilities. TDH has the following responsibilities with respect to its health care components:
  - a. Compliance with the HIPAA Security Rule.
  - b. Compliance with the HIPAA Privacy Rule including implementation of policies and procedures to ensure compliance, and the safeguard requirements.
  - c. Compliance with the HIPAA Privacy Rule regarding business associate arrangements and other organizational requirements.
  - d. Designation of health care components in compliance with the HIPAA Privacy Rule. TDH must maintain documentation of its designation for six years from the date of its creation or the date when it was last in effect, whichever is later.
  
6. Disclosures for Public Health Activities. For public health functions pursuant to TDH's activities as a public health authority:
  - a. A health care component may disclose PHI to a non-covered component without written patient authorization if the disclosure is made for a specified public health purpose, such as preventing or controlling disease, injury, or disability, or as required by state or local law.
  - b. A health care component may reasonably rely on a minimum necessary determination made by the non-covered component in requesting the PHI.
  - c. For routine and recurring public health disclosures, a health care component may develop standard protocols that address the types and amount of PHI that may be disclosed for such purposes.
  
7. Sanctions. Failure to comply with this policy may subject individuals to sanctions, up to and including disciplinary action, suspension, termination of employment, dismissal from TDH, and legal action. Some violations may constitute criminal offenses under local, state, and federal laws. TDH will carry out its responsibility to report such violations to the appropriate authorities.

**Reference(s):**

- 45 C.F.R. § 164.103
- 45 C.F.R. § 164.105
- 45 C.F.R. § 164.501
- 45 C.F.R. § 164.512(b)(1)(i)
- 45 C.F.R. § 164.514(d)(3)(i)
- 45 C.F.R. § 164.514(d)(3)(iii)(A)

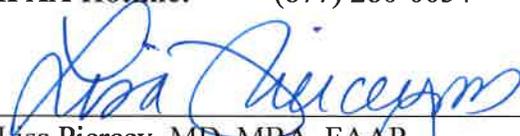
**Related policies:**

HIPAA Policies #102 - #113

**Contact(s):**

- **Privacy Program Office:** (615) 741-1969
- **Security Officer:** [security.health@tn.gov](mailto:security.health@tn.gov)
- **TDH HIPAA Hotline:** (877) 280-0054

**Approved by:**

  
\_\_\_\_\_  
Lisa Piercey, MD, MBA, FAAP  
Commissioner, Tennessee Department of Health

**Approved on:**

November 10, 2021

**Review/change history:**

**Review cycle:** Annual

Tennessee Department of Health

HIPAA Policies

Privacy

**Policy Title:** HIPAA Definitions

**Policy Number:** 102

**Effective Date:** January 4, 2022

**PURPOSE:**

This policy defines common terms used in the Tennessee Department of Health's (TDH) HIPAA Policies.

**POLICY:**

**Breach** means the acquisition, access, use, or disclosure of PHI in a manner that violates the HIPAA Rules and compromises the security or privacy of the PHI.

**Business Associate** means, with respect to TDH, a person or entity who, other than in the capacity of a TDH workforce member:

1. Performs or assists in the performance of a function or activity involving the use or disclosure of PHI, including claims processing or administration, data analysis, utilization review, quality assurance, billing benefit management on behalf of TDH; or
2. Provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for TDH, where the provisions of the service involve the disclosure of PHI from TDH, or from another business associate of TDH, to the person.

**Client** means an individual for whom TDH uses or maintains PHI to carry out health care component functions.

**Covered entity** means a health plan, a health care provider who conducts electronic transactions, or a health care clearinghouse.

**De-identified information** means client information from which TDH or another entity has deleted, redacted, or blocked identifiers, so that the remaining information cannot reasonably be used to identify a person.

**Health care component** means a component or combination of components of a hybrid entity designated by the hybrid entity in accordance with § 164.105(a)(2)(iii)(D) to provide HIPAA covered services.

**HIPAA Privacy Rule** means the regulatory rule that establishes national standards for the protection of certain health information, located at 45 CFR Part 160 and Subparts A and E of Part 164.

**HIPAA Security Rule** means the regulatory rule that establishes a national set of security standards for protecting certain health information that is held or transferred in electronic form, located at 45 CFR Part 160 and Part 164, Subparts A and C.

**Hybrid entity** means a single legal entity:

1. That is a covered entity;
2. Whose business activities include both covered and non-covered functions; and
3. That designates health care components in accordance with paragraph §164.105(a)(2)(iii)(D).

**Limited data set** means protected health information that excludes 16 categories of direct identifiers of an individual or of relatives, employers, or household members of the individual and may be used or disclosed, for purposes of research, public health, or health care operations, without obtaining either an individual's Authorization or a waiver or an alteration of Authorization for its use and disclosure, with a data use agreement.

**Protected health information (PHI)** means individually identifiable health information, including genetic information that is created, maintained, transmitted, or received in any medium by a health care provider, health plan, employer, or health care clearinghouse. PHI does not include information contained in employment records held by a covered entity or records regarding a person who has been deceased for more than fifty (50) years.

**Provider** means a person or entity who may seek reimbursement or payments from TDH as a provider of services to TDH clients.

**Public official** means any employee of a government agency who is authorized to act on behalf of that agency in performing the lawful duties and responsibilities of that agency.

**Research** means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalized knowledge.

**Treatment, payment, and health care operations (TPO)** includes all the following:

- *Treatment* means the provision, coordination, or management of health care and related services, consultation between providers relating to an individual, or referral of an individual to another provider for health care.
- *Payment* means activities undertaken to obtain or provide reimbursement for health care, including determinations of eligibility or coverage, billing, collection activities, medical necessity determinations and utilization review.
- *Health Care Operations* include functions such as quality assessment and improvement activities, reviewing competence or qualifications of health care professionals, conducting or arranging for medical review, legal services, and auditing functions, business planning and development, and general business and administrative activities.

**Unsecured PHI** means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the United States Department of Health and Human Services.

**Workforce member** means employees, volunteers, trainers, contractors, and other persons whose conduct, in the performance of work for the department, its offices, or programs is under the direct control of the department, office or program regardless of whether they are paid by the by the TDH.

**Reference(s):**

- 45 CFR Parts 160 and 164. *Note: please refer to the regulations for the complete definitions.*

**Contact(s):**

- Privacy Program Office: (615) 741-1969
- TDH HIPAA Hotline: (877) 280-0054

## Tennessee Department of Health

### HIPAA Policies

#### Privacy

**Policy Title:** Administrative Requirements for the Implementation of HIPAA

**Policy Number:** 103

**Effective Date:** March 26, 2013

**Revised Date:** January 4, 2022

#### **PURPOSE:**

To issue instructions to all offices, programs and workforce members regarding the Department of Health's (TDH) obligations relating to the implementation of the Health Insurance Portability and Accountability Act (HIPAA). 42 U.S.C. §§1320d-1329d-8, and regulations promulgated thereunder, 45 CFR Parts 160 and 164. This policy outlines TDH general guidelines and expectations for the necessary collection, use, and disclosure of protected health information (PHI) about clients in order to provide services and benefits to individuals while maintaining reasonable safeguards to protect the privacy of their information.

#### **POLICY:**

##### **General Overview**

TDH may, collect, maintain, use, transmit, share, and/or disclose information about clients, and providers to the extent required to administer TDH programs, services, and activities. TDH will safeguard all PHI about clients and providers, inform clients and providers about TDH's privacy practices, and respect clients' and providers' privacy rights, to the full extent required under this policy.

This policy identifies two types of individuals of whom TDH is most likely to obtain, collect, or maintain individual information:

- i) TDH clients
- ii) Providers

TDH, its workforce, and business associates will respect and protect the privacy of records and information about clients who request or receive services from TDH and providers. All information must be safeguarded in accordance with TDH privacy policies and procedures.

TDH has adopted reasonable policies and procedures for administration of its programs, services, and activities. If any state or federal law or regulation or order of a court having appropriate jurisdiction imposes a stricter requirement affecting any TDH policy regarding

the privacy or safeguarding of information, TDH shall adopt and comply with the stricter standard.

TDH workforce members shall act in accordance with established TDH policy and procedures regarding the safeguarding of client PHI. In the event that more than one policy applies but compliance with all such policies cannot reasonably be achieved, TDH employees will seek guidance from supervisors according to established TDH policy and procedures. TDH workforce members should consult with their Subsidiary Privacy Officer or the Department Privacy Officer in appropriate circumstances.

### **TDH Notice of Privacy Practices**

- A. The current “**TDH Notice of Privacy Practices**” shall be available in all offices of TDH.
- B. TDH will provide a copy of the current “**TDH Notice of Privacy Practices**” to any client requesting a copy. However, when TDH is a client’s direct provider, TDH is required to give a copy of the notice to the client on the first date the client receives services. TDH must have each client who receives direct care from TDH to sign an acknowledgement of receiving the notice on their first date of service. If TDH cannot get a signed acknowledgement, then TDH will document the reason why one was not received in the client’s record. Acknowledgement of receipts of the notice, and/or documentation of good faith effort to obtain written acknowledgement must be maintained for six years.
- C. The “**TDH Notice of Privacy Practices**” shall contain all information required under federal regulations regarding the notice of privacy practices for PHI under HIPAA.
- D. The “**TDH Notice of Privacy Practices**” shall also be available at the TDH website.
- E. Whenever the notice is revised, it should be made available upon request, posted at the TDH website, and posted in a prominent location on TDH premises on or after the effective date of the revision.
- F. Copies of the notice and all revisions shall be maintained by the Department Privacy Officer.

### **Administrative Requirements**

Due to HIPAA requirements, TDH has implemented certain administrative requirements as specified below:

#### **A. Personnel Designations**

1. Department Privacy Officer. TDH must designate an individual to be the Department Privacy Officer, responsible for the development and implementation of TDH-wide policies and procedures relating to the safeguarding of PHI.
2. Subsidiary Privacy Officers will be appointed to represent offices, each regional office and local health departments and to act in support of the Department Privacy Officer.

## **B. Privacy Officer Duties**

1. The Department Privacy Officer will oversee: all ongoing activities related to the development, implementation, maintenance of, and adherence to TDH's policies concerning privacy; establish and administer a process for receiving, documenting, tracking, investigations, and taking action on all complaints; and ensure that TDH is 1) in compliance with its privacy practices, and 2) consistently applies sanctions for failure to comply with privacy policies for all workforce members and business associates.
2. Subsidiary Privacy Officers will be responsible for providing information about TDH's privacy practices and receiving complaints relating to PHI and forwarding complaints to the Department Privacy Officer.

## **C. Workforce Training Requirements**

TDH and, as applicable, its offices must document the following training actions:

1. All TDH workforce members must receive HIPAA awareness training. Training regarding appropriate policies and procedures relating to PHI will be given as necessary and appropriate for those employees whose jobs are impacted by HIPAA.
2. Each new workforce member shall receive training as described above within a reasonable time after joining or re-joining the workforce.
3. After training as described above has been given to all the current workforce, TDH shall require every workforce member to sign a revised "Confidentiality Statement" (Form PH 3131). All new workforce members shall sign the "Confidentiality Statement" as soon as they have received the appropriate training outlined above.
4. Each workforce member must receive training as described above within a reasonable time when:
  - a. a material change in the policies and procedures relating to PHI occurs and it impacts his/her work, or
  - b. a change in jobs or position responsibilities occurs.

## D. Policies and Procedures

TDH and, as applicable, its offices must document the following actions relating to its policies and procedures:

1. TDH shall design and implement policies and procedures to assure appropriate safeguarding of PHI in its operations to be followed by all workforce members.
2. TDH must revise its policies and procedures as necessary and appropriate to conform to changes in law or regulation. TDH may also make changes to policies and procedures at other times as long as the policies and procedures are still in compliance with applicable law. When necessary, TDH must make correlative changes in its privacy notice. TDH may not implement a change in policy or procedure before the effective date of the revised privacy notice when required.
3. TDH and each office must maintain the required policies and procedures in written or electronic form and must maintain written or electronic copies of all communications, actions, activities or designations as are required to be documented hereunder or otherwise under the HIPAA regulations, for a period of six (6) years from the later of the date of creation, or the last effective date, or such longer period that may be required under state or other federal law.
4. Policies and procedures have been developed for the following administrative requirements.
  - a. Safeguarding PHI from intentional or unintentional unauthorized use or disclosure as outlined in **TDH HIPAA Policy #107**. *“Administrative, Technical, and Physical Safeguards.”*
  - b. Complaint process for documenting and referring complaints received by clients as outlined in **TDH HIPAA Policy #104**. *“Clients’ Privacy Rights.”*
  - c. Application of sanctions and documentation of the application of appropriate sanctions against workforce members as outlined in **TDH HIPAA Policy #111**. *“Enforcement, Sanctions, and Penalties for Violation of Individual Privacy.”*
  - d. Each office must mitigate, to the extent practical, any inappropriate use or disclosure of PHI by TDH or any of its business associates as outlined in **TDH HIPAA Policy #113**. *“Mitigation Efforts.”*
  - e. Neither TDH nor any office or workforce member shall intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any

individual for the exercise of his/her rights relating to HIPAA compliance, nor will TDH require clients to waive their right to file a complaint as a condition for providing treatment, payment, or receiving a service, as outlined in **TDH HIPAA Policy #104**, “*Clients’ Privacy Rights.*”

5. Policies and procedures for other aspects of HIPAA have been developed to address operational issues as follows:
  - a. Clients’ rights to access their own information, with some exceptions, as well as the client’s right to request restrictions or amendments to their information is outlined in **TDH HIPAA Policy #104**, “*Clients’ Privacy Rights.*”
  - b. The requirements TDH needs to follow regarding the uses and disclosures of client information is outlined in **TDH HIPAA Policy #105**, “*Uses and Disclosures of Client Information.*”
  - c. TDH will use or disclose only the minimum necessary information necessary to provide services and benefits to clients as outlined in **TDH HIPAA Policy #106**, “*Minimum Necessary Information.*”
  - d. TDH may use or disclose client’s information for research purposes as outlined in **TDH HIPAA Policy #108**, “*Use and Disclosure for Research Purposes and Waivers.*”
  - e. TDH workforce members will follow standards under which client information can be used and disclosed if information that can identify a person has been removed or restricted to a limited data set as outlined in **TDH HIPAA Policy #109**, “*De-identification of client information and Use of Limited Data Sets.*”
  - f. TDH may disclose PHI to business associates with whom there is a written contract, business associate agreement or memorandum of understanding as outlined in **TDH HIPAA Policy #110**, “*TDH Business Associates.*”

**Reference(s):**

- 45 CFR Parts 160 and 164

**Contact(s):**

- Privacy Program Office: (615) 741-1969
- TDH HIPAA Hotline: (877) 280-0054

## Tennessee Department of Health

### HIPAA Policies

#### Privacy

**Policy Title:** Clients Privacy Rights

**Policy Number:** 104

**Effective Date:** March 26, 2013

**Revised:** January 4, 2022

#### **PURPOSE:**

The policy establishes TDH client privacy rights regarding the use and disclosure of a client's Protected Health Information (PHI) held by TDH and describes the process for filing a complaint if a client feels those rights have been violated.

#### **POLICY:**

##### **General:**

TDH will use the “**TDH Notice of Privacy Practices**” to inform clients about how TDH may use and/or disclose their information. The “**TDH Notice of Privacy Practices**” also describes the actions a client may take or request TDH to take with regard to the use and/or disclosure of their information.

The policies related to the “**TDH Notice of Privacy Practices**” and distribution of the notice is addressed in **TDH HIPAA Policy #103**, “*Administrative Requirements for the Implementation of HIPAA.*”

##### **A. TDH clients have the right to, and TDH may not deny:**

###### **1. Access to their own information, consistent with certain limitations:**

- a. Clients have the right to access, inspect, and obtain a copy of the client's health information in TDH files or records, consistent with federal and Tennessee law. TDH recognizes the right of a decedent's personal representative. Death certificates listing cause of death will only be released in accordance with T.C.A. §68-3-205.
- b. All requests for access must be made in writing in accordance with appropriate office policy and procedure.
- c. If TDH maintains information about the client in a record that includes information about other people, the client is only authorized to access information about him or her, unless:

- i) If the person identified in the file is the client's minor child, and the client is authorized under Tennessee law to access the minor's information or act on behalf of the minor for making decisions about the minor's care, TDH will release the minor's information to the client.
  - ii) If the person requesting information is the client's legal guardian or legal custodian under Tennessee law and is authorized by Tennessee law to access the client's information or act on behalf of the client for making decisions about the client's services or care, TDH will release information to the requestor.
  - iii) A covered entity may, in the exercise of professional judgment, disclose to a client's family member, other relative or a close personal friend, the protected health information related to the client's health care or payment related to the client's health care.
- d. TDH must act on a client's request for access no later than 30 days after receiving the request.
- i) If TDH is unable to act within the 30-day limit, TDH may extend this limitation by up to an additional 30 days, subject to the following:
    - TDH must notify the client in writing of the reasons for the delay and the date by which TDH will act on the request.
    - TDH will use only one such 30-day extension to act on a request for access.
- e. If TDH grants the client's request, in whole or in part, TDH must inform the client of the access decision and provide the requested access.
- i) If TDH maintains the same information in more than one format (such as electronically and in a hard-copy file) or at more than one location, TDH need only provide the requested protected information once.
  - ii) TDH must provide the requested information in a form or format requested by the client, if readily producible in that form or format. If not readily producible, TDH will provide the information in a readable hard-copy format or such other format as agreed to by TDH and the client.
  - iii) TDH may provide the client with a summary of the requested information, in lieu of providing access, or may provide an explanation of the information if access had been provided. If:
    - The client agrees in advance; and

- The client agrees in advance to pay any fees.
- iv) TDH must arrange with the client to provide the requested access in a time and place convenient for the client and TDH. This may include mailing the information to the client if the client so requests or agrees.
- v) Fees: TDH may impose a fee for these records, in accordance with departmental regulations and/or policies.
- vi) If TDH does not maintain the requested information but knows where such information is maintained (such as by a medical provider, insurer, other public agency, private business, or other non-TDH entity), TDH must provide the client with that information (where to direct the request access).
- vii) If requested client information is maintained by a TDH business associate, TDH must forward the request directly to the business associate. Requests for information held by a business associate are subject to the same 30-day limit which begins when TDH receives the request.

**2. TDH may deny a client access to his PHI under the following limitations:**

- a. TDH may deny a client access to his own health information if federal law prohibits the disclosure. Under federal law, a client has the right to access, inspect, and obtain a copy of his own health information in TDH files or records **except for:**
  - i) Psychotherapy notes;
  - ii) Information that, in good faith, TDH believes can cause harm to the client, or to any other person;
  - iii) Information that was obtained from someone other than a health care provider under a promise of confidentiality, and access would reveal the source of the information;
  - iv) Information compiled for use in civil, criminal, or administrative proceedings;
  - v) Information that is subject to the federal Clinical Laboratory Improvement Amendments of 1988, or exempt pursuant to 42 CFR493.3(a)(2);
  - vi) Documents protected by attorney work-product privilege; and
  - vii) Information prohibited from release by state or federal laws.

- b. Only a licensed health care professional or TDH designated workforce member may deny a client or his personal representative access to the client's health information because there is a good faith belief that its disclosure could cause harm to the client or to another person. TDH must provide a review of the denial available to the client. If the client wishes to have this denial reviewed, the review must be done by a health care professional who is part of the TDH workforce and who was not involved in the original denial decision.

TDH must promptly refer a request for review to the designated reviewer within the time frame of this policy.

The reviewer must determine, within a reasonable time, whether or not to approve or deny the client's request for access, in accordance with this policy.

The Department Privacy Officer must then:

- i) Promptly notify the client in writing of the reviewer's determination; and
- ii) Take action to carry out the reviewer's determination.

If TDH denies access, in whole or in part, to the requested information, TDH must:

- i) Give the client access to any other requested client information, after excluding the information to which access is denied;
- ii) Provide the client with a timely written denial.

The denial must:

- i) Be sent or provided within the time limits specified in this policy;
- ii) State the basis for the denial, in plain language;
- iii) If the reason for the denial is due to danger to the client or another, explain the client's review rights as specified in this policy, including an explanation of how the client may exercise these rights; and
- iv) Provide a description of how the client may file a complaint with TDH, and if the information denied is protected health information, with the United States Department of Health and Human Services, Office for Civil Rights, pursuant to this policy.

## **B. Rights of clients to an accounting of disclosures of PHI**

1. Clients have the right to receive an accounting of disclosures from TDH for PHI disclosed for any period of time, but not to exceed six years preceding the date of requesting the accounting.
2. An accounting is only required to include health information NOT previously authorized by the client for use or disclosure, and not collected, used, or disclosed for treatment, payment, or health care operations for the client.
3. Clients may request an accounting of disclosures at any TDH office-- the central office, a regional office or a local office. The office receiving the request is required to provide an accounting of the disclosures made by that office. When the accounting is provided to the client, each office should include a statement indicating that this it is an accounting of disclosures for their particular office only, *i.e.*, “This is an accounting of the disclosures made only by the Wilson County Health Department. If you are interested in whether other disclosures may have been made by TDH, please contact the Tennessee Department of Health Privacy Officer at . . .”
4. The Department Privacy Officer will be responsible for compiling an accounting of disclosures received by his office. The Department Privacy Officer will assure the accounting includes disclosures for the entire TDH and will provide the accounting to the client or the client’s legal representative.
5. All requests for an accounting of disclosures must be made in writing.
6. Disclosures that TDH is not required to track or account for are:
  - a. Made between TDH health care components;
  - b. Authorized by the client;
  - c. Made to carry out treatment, payment, and health care operations (“TPO”);
  - d. Made to the client;
  - e. Made a part of a limited data set in accordance with TDH **HIPAA Policy #109: “De-identification of Client Information and Use of Limited Data Sets”**;
  - f. For national security or intelligence purposes;
  - g. Required by law; or



- iii) Limit the temporary suspension to no longer than 30 days from the date of the oral request, unless the agency or official submits a written request specifying a longer time period.
10. TDH must act on a client's request for an accounting of disclosures no later than 60 days after receiving the request, subject to the following:
- a. If unable to provide the accounting within 60 days after receiving the request, TDH may extend this requirement by another 30 days. TDH must provide the client with a written statement of the reasons for the delay within the original 60-day time-period and inform the client of the date by which TDH will provide the accounting.
  - b. TDH will use only one such 30-day extension.
  - c. In lieu of an accounting of disclosures provided to a client, a copy of any disclosure protocol may be provided to the client for disclosures made for research purposes rather than an individualized accounting of each actual disclosure, for studies involving 50 or more individuals.

### **C. Rights of clients to file complaints regarding disclosure of information**

1. Clients have a right to submit a complaint if they believe that TDH has improperly used or disclosed the client's PHI, or if the client has concerns about the privacy policies of TDH or concerns about TDH compliance with such policies.
2. Complaints may be filed with any of the following:
  - a. The Department Privacy Officer
  - b. The U.S. Department of Health and Human Services, Office for Civil Rights.
  - c. The Subsidiary Privacy Officers may receive complaints and then forward them to the Department Privacy Officer.
3. The TDH workforce will not intimidate, threaten, coerce, discriminate against, or take any other form of retaliatory action against any person filing a complaint or inquiring about how to file a complaint.
4. TDH workforce may not require clients to waive their rights to file a complaint as a condition of providing treatment, payment enrollment in a health plan, or eligibility for benefits.

5. The Department Privacy Officer will review and determine action on complaints filed with TDH. The Department Privacy Officer will also perform these functions when TDH is contacted about complaints filed with the U.S. Department of Health and Human Services – Office for Civil Rights.
6. The Department Privacy Officer will review and determine the action to be taken on all complaints. The Department Privacy Officer will document and maintain all complaints, the findings form reviewing each complaint, and TDH actions resulting from the complaint. For each specific complaint, this documentation shall include a description of corrective actions that TDH has taken, if any are necessary, or why corrective actions are not needed.

**D. Clients may make specific requests regarding the use and disclosure of their information and TDH may either approve or deny the request. Specifically, clients have the right to request:**

1. Restricted use and disclosure of their information
  - a. Clients have the right to request in writing restrictions on the use and/or disclosure of their information for:
    - i) Carrying out treatment, payment, or health care operations; or
    - ii) Disclosure of health information to a relative or other person who is involved in the client's care.
    - iii) TDH is not obligated to agree to a requested restriction and may deny the request or may agree to a restriction more limited than what the client requested. However, **TDH MUST comply with requests to restrict disclosure of PHI to a health plan for payment or health care operations IF the PHI pertains to health care items or services which were paid in full out of pocket by the patient or his/her representatives.**

**Exception:** Certain programs can only use information that is authorized by the client, such as alcohol and drug programs (42 CFR Part 2). For those program clients, TDH shall honor their requests for restriction by making sure that the authorization clearly identifies the authorized recipients of the information.

2. TDH is not required to agree to a client's requested restriction.
  - a. TDH will not agree to restrict uses or disclosures of information if the restriction would adversely affect the quality of the client's care or services.

- b. In an emergency situation, TDH may use or disclose such information to the extent needed to provide the emergency treatment to the client.
- c. TDH will document the reasons for granting or denying the requested restriction in the client's medical record.
- d. Before any use or disclosure of client PHI, TDH workforce member must confirm that such use or disclosure has not been granted a restriction by reviewing the client's medical file.
- e. TDH may terminate its agreement to a restriction if:
  - i) The client agrees to or requests termination of the restriction in writing;
  - ii) The client orally agrees to or requests termination of the restriction. TDH will document the oral agreement or request in the client's TDH medical record file; or
  - iii) TDH informs the client in writing that TDH is terminating its agreement to the restriction. Information created or received while the restriction was in effect shall remain subject to the restriction.

**E. Rights of clients to request to receive information from TDH by alternate means or at alternate locations**

- a. TDH must accommodate reasonable requests by clients to receive communications by alternate means, such as by mail, e-mail, SMS or telephone; and
- b. TDH must accommodate reasonable requests by clients to receive communications at an alternate location.
- c. In some cases, sensitive health information or health services must be handled with strict confidentiality under Tennessee state law. For example, information about substance abuse treatment and certain sexually transmitted diseases may be subject to specific handling. TDH will comply with the more restrictive requirements.

**F. Rights of clients to request amendments to their information.**

- a. Clients have the right to request that TDH amend their information in files held by TDH health care components.

- b. All requests for amendments must be in writing and a justification must be provided supporting the request for the amendment in accordance with the appropriate office policy and procedure.
- c. TDH is not obligated to agree to any amendment and may deny the request or limit its agreement to amend. Before any decision, based on a client's request for TDH to amend a previously documented health or medical record, the office director shall review the request and any related documentation. The licensed health care professional may be a TDH workforce member involved in the client's case.
- d. Before any decision to amend any other information that is not a health or medical record, a TDH workforce member designated by the program administrator shall review the request and any related documentation.
- e. If TDH grants the request, in whole or in part, TDH must:
  - i) Make the appropriate amendment to the protected information or records, and document the amendment in the client's file or record;
  - ii) Provide timely notice to the client that the amendment has been accepted, pursuant to the time limitations of this policy;
  - iii) Seek the client's agreement to notify other relevant persons or entities with whom TDH has shared or needs to share the amended information; and
  - iv) Make reasonable efforts to inform and to provide the amendment within a reasonable time to:
    - Persons identified by the client as having received PHI and who need the amendment; and
    - Persons, including TDH business associates, which TDH knows have the PHI that is the subject of the amendment and that may have relied, or could rely, on the information to the client's detriment.
- f. TDH may deny the clients request for amendment if:
  - i) TDH finds the original information to be accurate and complete;
  - ii) The information was not created by TDH, unless the client provides a reasonable basis to believe that the originator of such information is no longer available to act on the requested amendment;

- iii) The information is not part of TDH records; or
  - iv) If it would not be available for inspection or access by the client pursuant to this policy.
- g. If TDH denies the requested alteration, in whole or in part, TDH must:
- i) Provide the client with a timely written denial. The denial must:
    - Be sent or provided within the time limits specified in this policy;
    - State the basis for the denial, in plain language;
    - Explain that if the client does not submit a written statement of disagreement, the client may ask that if TDH makes any future disclosures of the relevant information, TDH will also include a copy of the client's original request for amendment and a copy of the TDH written denial; and
    - Explain the client's right to submit a written statement disagreeing with the denial and how to file such a statement. If the client does so:
      - TDH will enter the written statement into the client's TDH case file;
      - TDH may also enter a TDH written rebuttal of the client's written statement into the client's TDH case file. TDH will send or provide a copy of any such written rebuttal to the client;
      - TDH will include a copy of the statement and of the written rebuttal by TDH if any, with any future disclosures of the relevant information; and
      - Provide information on how the client may file a complaint with TDH, or with the U.S. Department of Health and Human Services, Office for Civil Rights.
- h. TDH must act on the client's request no later than 60 days of receiving the request. If TDH is unable to act on the request within 60 days, TDH may extend this time limit by up to and additional 30 days, subject to the following:
- TDH must notify the client in writing of the reasons for the delay and the date by which TDH will act on the receipt; and
  - TDH will use only one such 30-day extension.

**G. Decisions related to any other requests made to TDH under this policy shall be handled in a manner consistent with federal and state statutes, rules and regulations, and/or TDH policies and procedures applicable to the program, service or activity and shall be coordinated with TDH's Privacy Officer.**

**Reference(s):**

- 45 CFR Part 164.522 – 164.528

**Contact(s):**

- Privacy Program Office: (615) 741-1969
- TDH HIPAA Hotline: (877) 280-0054

**Tennessee Department of Health**

**HIPAA Policies**

**Privacy**

**Policy Title:**           **Uses and Disclosure of Client Information**

**Policy Number:**       **105**

**Effective Date:**       **March 26, 2013**

**Revised Date:**       **January 4, 2022**

**PURPOSE:**

This policy specifies when a client’s Protected Health Information (PHI) may be used or disclosed without the client’s prior authorization. It also specifies how to use or disclose PHI when there is a client’s authorization.

**POLICY:**

**General – Client Authorization**

TDH may disclose information for purposes of treatment, payment, and health care operations (“TPO”) without client authorization unless otherwise provided by office policy.

TDH shall not use or disclose any PHI about a client of TDH’s programs or services without a signed authorization for release of that information from the client, or the client’s personal representative, unless authorized by this policy, or otherwise authorized by state or federal law.

A. A signed authorization is required:

1. Before a client’s enrollment in a TDH health service, if necessary to determine eligibility or enrollment;
2. For disclosure of psychotherapy notes;
3. For disclosure to an employer (or potential employer) for use in employment-related determination;
4. For research purposes unrelated to the client’s treatment;
5. For marketing purposes;
6. For the sale of PHI; and
7. For any other purpose in which state or federal law requires a signed authorization.

B. TDH may obtain, use, or disclose information only if the written authorization includes all required elements of a valid authorization. The required elements are:

1. A description of the information to be used or disclosed identifying the information in a specific and meaningful fashion;
  2. The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure;
  3. The name or other specific identification of the person(s), class of persons, to whom TDH may make the requested use or disclosure;
  4. A description of each purpose of the requested use or disclosure.
  5. An expiration date, or an expiration event that relates to the client or to the purpose of the use or disclosure;
  6. Signature of the client, or of the client's personal representative, and the date of signature; and
  7. If the client's personal representative signs the authorization form, a description of the representative's authority to act for the client, including a copy of the legal court document (if any) appointing the personal representative.
- C. Uses and disclosures must be consistent with those authorized by the client on the signed authorization form.
- D. TDH may not require the client to sign an authorization as a condition of providing treatment services or obtaining payment for health care services.
- E. Each authorization for use or disclosure of a client's information must be fully completed jointly by a workforce member and the client, whenever possible, with the workforce member taking reasonable steps to ensure that the client understands why and how the information is to be used or released.
- F. TDH must document and retain each signed authorization form for a minimum of six (6) years.
- G. When TDH receives a signed authorization from an outside entity, TDH must verify that it is a valid authorization and contains all the required information before TDH releases or discloses any PHI.

### **Uses and Disclosures without a Client's Authorization**

#### **A. Public Health Authority/Activity**

For the purpose of carrying out duties in its role as a public health authority, TDH does not need to obtain a client's authorization to lawfully receive, use, disclose or exchange PHI for public health activities, including PHI from TDH's health care components. Public health activity is defined as those duties necessary to, but not limited to, prevent or control disease or injury; report vital events, such as births or deaths; and conduct public health surveillance or interventions.

1. Information about clients received or held by TDH as a governmental public health authority shall be safeguarded against loss, interception or misuse as required by law or TDH policy.
2. Allowable uses and disclosures for public health activities are:
  - a. A governmental public health authority authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability. This includes, but is not limited to, reporting disease, injury, vital events such as birth or death, and conducting public health surveillance, investigations, survey and certification, inspections, and interventions. Some of these types of disclosures may be covered in a disclosure protocol developed by each office and are included in the TDH's accounting protocol;
  - b. An official of a foreign government agency that is acting in collaboration with a lawful governmental public health authority;
  - c. A governmental public health authority, or other appropriate governmental authority authorized by law to receive reports of child abuse or neglect;
  - d. A person subject to the jurisdiction of the federal Food and Drug Administration (FDA), regarding an FDA-regulated product or activity for which that person is responsible, for activities related to the quality, safety, or effectiveness of such FDA-related product or activity. Such persons include:
    - i. To collect or report adverse events, product defects or problems (including product labeling problems), or biological product deviations;
    - ii. To track FDA-related products;
    - iii. To enable product recalls, repairs, replacements, or look back; or
    - iv. To conduct post market surveillance.
3. A person who may have been exposed to a communicable disease or may be at risk of contracting or spreading a disease or condition. If TDH or other public health authority is authorized by law to notify such person as necessary in conducting a public health intervention or investigation.
  - a. As a public health authority, TDH is authorized to use and disclose a client's PHI in all cases in which TDH is permitted to disclose such information for the public health activities listed above.
  - b. Public health research will be conducted consistent with **TDH HIPAA Policy #108**, *"Use and Disclosure for Research Purposes & Waivers."*
4. Operation of the Public Health Laboratory
  - a. This section applies only to those components of the public health laboratory designated as health care components.

- b. State law establishes that for the “protection of the public health,” a public health laboratory is created within TDH to conduct tests and examinations at the request of any state, county, or city institution or officer, and at the request of any licensed physician.
  - c. Laboratories are health care providers with an “indirect treatment relationship” as defined in federal regulations 45 CFR 164.501 and in accordance with 45 CFR 164.506(a)(2)(i).
  - d. TDH is authorized to use and disclose PHI for purposes of the operation of the public health laboratory consistent with HIPAA and applicable law.
5. Verifying the authority of a public health officer

Health care providers and health care payers may request TDH to verify the authority of a TDH employee or contractor to conduct a public health activity. TDH employees or contractors must be prepared to explain and provide documentation to the provider or payer about their legal authority to collect or obtain information and be prepared to identify themselves.

#### B. Other Disclosures without Authorization

To the extent not otherwise prohibited or limited by federal or state requirements applicable to the TDH program or activity, TDH may use or disclose PHI without written authorization of the client in the following circumstances:

1. Required by law. TDH may use or disclose PHI without client authorization if the law requires such use or disclosure, and the use or disclosure complies with, and is limited to, the relevant requirements of such law.
2. Internal TDH communications. Internal communication within TDH health care components is permitted without client authorization, in compliance with **TDH HIPAA Policy #106**, “*Minimum Necessary Information.*” However, disclosure of alcohol and drug abuse treatment records may be limited to particular program areas named on their authorization form. If such a limitation is noted on the authorization form, disclosure is limited to the parties named.
3. Client access. TDH clients may access their own PHI with certain limitation in compliance with **HIPAA Policy #104**, “*Clients’ Privacy Rights.*”
4. Treatment, payment and health care operations (“TPO”). TDH may disclose PHI for purposes of payment, treatment, and health care operations without client authorization unless otherwise required by office policy.
5. Child abuse. If TDH has reasonable cause to believe that a child is a victim of abuse or neglect, TDH may disclose PHI to appropriate governmental authorities authorized to receive reports of child abuse or neglect.

- a. Consistent with applicable law, TDH may make reports and records available to any person, administrative hearing officer, court, agency, organization, or other entity when TDH determines that such disclosure is necessary to:
    - i. Administer the State's child welfare services and is in the best interest of the affected child;
    - ii. Investigate, prevent, or treat child abuse and neglect; or
    - iii. Protect children from abuse and neglect.
  - b. TDH may not disclose the names, addresses, or other identifying information about the person who made the report.
6. Adult abuse. If TDH had reasonable cause to believe that an adult is a victim of abuse or neglect, TDH may disclose PHI, as required by law, to a governmental authority authorized by law to receive such reports.
- a. If the disclosure is required by law, and the disclosure complies with and is limited to the relevant requirement of such law; or
  - b. If the client agrees to the disclosure, either orally or in writing; or
  - c. When TDH workforce members, in exercise of professional judgment, and in consultation with an appropriate TDH supervisor, believes the disclosure is necessary to prevent serious harm to the client or other potential victims; or
  - d. When the client is unable to agree because of incapacity, a law enforcement agency or other public official authorized to receive the report represents that:
    - i. The PHI being sought is not intended to be used against the client, and
    - ii. An immediate law enforcement activity would be materially and adversely affected by waiting until the client is able to agree to the disclosure.
  - e. When TDH workforce members make a disclosure permitted above, TDH must promptly inform the client that such a report has been or will be made, except if:
    - i. A TDH workforce member, in the exercise of professional judgment and in consultation with an appropriate TDH supervisor, believes informing the client would place the client or another client at risk of serious harm; or
    - ii. A TDH workforce member would be informing a personal representative and the TDH workforce member reasonably believes the personal representative is responsible for the abuse, neglect or other injury, and that informing such person would not be in the best interest of the client, as determined by the TDH workforce members, in the exercise of professional judgment and in consultation with the appropriate TDH supervisor.

7. Duties as a health oversight agency. If a health oversight activity or investigation is conducted in conjunction with an oversight activity or investigation relating to a claim for public benefits not related to health, the joint activity is considered health oversight activity for the purposes of this section.
  - a. TDH may use or disclose PHI without authorization for the purpose of carrying out its duties in its role as a health oversight agency. Such activities may be authorized by law, and include audits of health care providers; civil, criminal, or administrative investigations; prosecutions or actions; licensing or disciplinary actions; Medicare/TennCare fraud; or other activities necessary for oversight.
  - b. If TDH has obtained PHI in performing its duties as a health oversight agency, nothing in this section supersedes TDH policies that otherwise permit or restrict uses or disclosures. For example, if TDH has obtained client PHI as a result of an oversight action against a provider, TDH may lawfully use that patient information in a hearing consistent with the other confidentiality requirements applicable to that program, service or activity.
8. Disclosure to health oversight agencies. TDH may disclose PHI to a health oversight agency to the extent the disclosure is not prohibited by state or federal law for its oversight activities of:
  - a. The health care system;
  - b. Government benefit programs for which the information is relevant to eligibility;
  - c. Entities subject to government regulatory programs for which the information is necessary for determining compliance with program standards; or
  - d. Entities subject to civil rights laws for which the information is necessary for determining compliance.
9. Law enforcement. As specified in HIPAA regulations 45 CFR 165.512, for limited law enforcement purposes to the extent authorized by applicable federal or state law, TDH may release PHI in the following circumstances:
  - a. TDH may report certain injuries or wounds;
  - b. provide information to identify or locate a suspect, victim, or witness;
  - c. alert law enforcement of a death if suspected it is a result of criminal conduct; and
  - d. provide information which in good faith constitutes evidence of criminal conduct on TDH premises.
10. Research. TDH may disclose PHI without authorization for research purposes, as specified in **TDH HIPAA Policy #108**, *“Use and Disclosure for Research Purposes & Waivers.”*

11. Serious threat to health or safety. To avert a serious threat to health or safety, TDH may disclose PHI without authorization if TDH believes in good faith that the PHI is necessary to prevent or lessen a serious or imminent threat to the health and safety of a person or the public; **and** the report is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat.
12. Government functions. TDH may disclose PHI without authorization for other specialized government functions, including authorized federal officials conducting lawful intelligence, counterintelligence, and other national security activities that federal law authorizes.
13. Health of inmates. TDH may disclose limited PHI without authorization to a correctional institution or a law enforcement official having lawful custody of an inmate, for the purpose of providing health care or ensuring the health and safety of clients or other inmates.
14. Emergency. In case of an emergency, TDH may disclose PHI without an authorization to the extent needed to provide emergency treatment.
15. Student records. The Family Educational Rights and Privacy Act (FERPA) and state law applicable to student records govern TDH access to, use, and disclosure of student records. TDH may disclose proof of immunization to a school where State or other law requires the school to have such information prior to admitting the student.
16. Prior client relationship. TDH may disclose PHI without authorization to another entity covered by federal HIPAA law and rules for the health care activities of that entity, if:
  - a. Both the entity and TDH has or has had a relationship with the client who is the subject of the information;
  - b. The information pertains to such relationship; and
  - c. The disclosure is for the purpose of:
    - i. Conducting quality assessment and improvement activities, including: outcome evaluation and development of clinical guidelines, provided that obtaining generalized knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs; protocol development; case management and care coordination; contacting health care providers and patients with information about treatment alternatives; and related functions that do not include treatment; or
    - ii. Reviewing the completeness or qualifications of health care professionals; evaluating practitioner and provider performance; conducting training programs in which students, trainees or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers;

training of non-health care professionals; accreditation, certification, licensing, or credentialing activities; or

iii. Detecting health care fraud and abuse or for compliance purposes.

- Use or disclosure by TDH in training programs where students and trainees learn under supervision to practice or improve skills;
- To the extent authorized under state law to defend TDH in a legal action or other proceeding brought by the client.

17. Judicial or administrative proceedings. Unless prohibited or otherwise limited by federal or state law applicable to the program or activity requirements, TDH may disclose PHI without authorization for judicial or administrative proceedings in which TDH or the State of Tennessee is a party, in response to an order of a court or a subpoena. TDH may use or disclose PHI without the written authorization of the client when TDH discloses PHI in a judicial or administrative proceeding subject to the following:

- a. The Office of General Counsel will address or respond to subpoenas, court orders, discovery requests, and other requests for documents made pursuant to litigation or law enforcement purposes. All subpoenas or other legal documents served on TDH should be forwarded to the Office of General Counsel for review within 2 business days.
  - i. An administrative hearing officer or administrative law judge lacks legal authority under Tennessee law, to require or authorize TDH to disclose information about a client that is confidential under federal or state law without appropriate subpoenas, orders, or similar lawful process. TDH workforce members should work with hearing officers to ensure that protective orders are used when appropriate in contested case hearing to prevent unauthorized use and disclosures of information.
  - ii. TDH workforce members will refer any questions or concerns regarding what is required by law, or by court order, to the TDH Privacy Officer, who will then consult with the Office of General Counsel to resolve the question.

18. Restrictions on disclosures in administrative or judicial proceedings. In any situation in which federal or state law prohibits or restricts the use or disclosure of PHI in an administrative or judicial proceeding, TDH shall assert the confidentiality of such confidential information, consistent with TDH policies applicable to the program, service, or activity, to the presiding officer at the proceeding. A HIPAA-authorized protective order may not be sufficient to authorize disclosure if it does not address other applicable confidentiality laws.

19. Disclosures pursuant to judicial or administrative orders. TDH may disclose PHI in compliance with, and limited to the relevant specific requirements of:

- a. A court order or warrant, summons or subpoena issued by a judicial officer;
- b. A grand jury subpoena;
- c. An administrative request, including administrative subpoena or summons, a civil or authorized investigative demand, or similar lawful process, provided that the information is relevant, material, and limited to a legitimate law enforcement inquiry.

**Exceptions:**

- i. Information on alcohol and drug treatment services can be disclosed only on the basis of a court order (42 CFR Part 2)
  - ii. Information regarding sexually transmitted disease services can only be disclosed with specific authorization from the patient or pursuant to T.C.A. § 68-10-113.
20. Lawsuit. If TDH is sued or if a suit is filed on behalf of TDH, the Office of General Counsel will address or respond to legal issues related to the use and disclosure of PHI. TDH will identify confidentiality issues for discussion with the assigned legal counsel, in consultation with the TDH Privacy Officer, when deemed appropriate.
21. National security. TDH may disclose PHI to authorized federal officials for conducting lawful intelligence, counterintelligence, and other national security activities, as authorized by the federal National Security Act (50 U.S.C. 401, *et seq.*) and implementing authority.
22. Protection of government officials. TDH may disclose PHI to authorized federal officials for the protection of the President or of other persons authorized by applicable federal law.

**Client's authorization that is not required if the client is informed in advance and given a chance to object.**

In some limited circumstances, TDH may use or disclose a client's PHI without authorization, but only if the client has been informed in advance and has been given the opportunity to either agree or refuse the use or disclosure. These circumstances are:

For disclosure of PHI to a family member, or relative, or close personal friend of the client, or any other person named by the client, subject to the following limitations:

- A. TDH may reveal only the PHI that directly relates to such person's involvement with the client's care or payment for such care.
- B. TDH may use or disclose PHI for notifying (including identifying or locating) a family member, personal representative, or other person responsible for care of the client, regarding the client's location, general condition, or death.

- C. If the client is present for, or available to, such a use or disclosure, TDH may disclose the PHI if it:
1. Obtains the client's agreement;
  2. Provides the client an opportunity to object to the disclosure, and the client does not express an objection; or
  3. Reasonably infers from the circumstances that the client does not object to the disclosure.
- D. If the client is not present, or the opportunity to object to the use or disclosure cannot practicably be provided due to the client's incapacity or an emergency situation, TDH may determine, using professional judgment, that the use or disclosure is in the client's best interests.
1. Any agreement, objection, refusal, or restriction by the client, may be oral or in writing. TDH will document any such oral communication in the client's case file.
  2. TDH will also document in the case file the outcome of any opportunity provided to object, the client's decision not to object, or the inability of the client to object.

**NOTE:** Verbal permission to use or disclose information for purposes described in this section is not sufficient if the client is referred to or receiving substance abuse treatment. *Written authorization is required.*

**Re-Disclosure of a Client's Information:**

- A. Unless prohibited by state and/or federal laws, PHI held by TDH and authorized by the client or by HIPAA or applicable state and federal law for disclosure to a third party may be subject to re-disclosure by the third party. In such cases, once disclosed by TDH to the third party, the information is no longer protected by TDH or covered by this policy.
- B. Alcohol and drug rehabilitation information: Federal regulations (42 CFR Part 2 and 34 CFR 361.38) prohibit TDH from making further disclosure of alcohol and drug rehabilitation information without the specific written authorization of the client to whom it pertains.

**Revocation of Authorization**

- A. A client may revoke an authorization at any time.
- B. Any revocation must be in writing and signed by the client and maintained in the file.

**Exception:** Alcohol and drug treatment clients may orally revoke authorization to disclose information obtained from alcohol and drug treatment programs. Oral authorizations must be documented and maintained in the client's record.

- C. No such revocation shall apply to PHI already released while the authorization was valid and in effect.

### **Verification of Client Requesting Information**

PHI about a client may not be disclosed unless the identity of the person requesting the information is verified in accordance with that appropriate office policy and procedure, if the TDH workforce member fulfilling the request does not know that person.

### **Denial of Requests for Information**

Unless a client has signed an authorization, or the information about the client can be disclosed pursuant to this policy, or as allowed by law, TDH shall deny any request for client PHI.

### **Prohibition of Use or Disclosure of Client's PHI**

**TDH shall not use or disclose any client's PHI for marketing purposes, unless: (1) the communication describes a prescription drug or biologic and TDH cannot receive compensation for the communication; or (2) the client has authorized such disclosure in writing. TDH shall not use or disclose psychotherapy notes or any disclosure that involves the sale of PHI without prior authorization by patient.**

### **Disclosures by Whistleblowers and Workforce Crime Victims**

- A. A TDH employee may disclose limited PHI about an individual to a law enforcement if the employee is the victim of a criminal act and the disclosure is:
  - 1. About only the suspected perpetrator or the criminal act; and
  - 2. Limited to the following information about the suspected perpetrator
    - a. Name and address;
    - b. Date and place of birth;
    - c. Social Security number;
    - d. ABO blood type and RH factor;
    - e. Type of any injury;
    - f. Date and time of any treatment; and
    - g. If applicable, death and time of death
- B. A TDH employee or business associate may disclose an individual's protected client information if:
  - 1. The TDH employee or business associate believes in good faith, that TDH has engaged in conduct that is unlawful or that otherwise violates professional standards or TDH

policy, or that the care, services, or conditions provided by TDH could endanger TDH workforce members, persons in TDH care, or the public; and

2. The disclosure is to:
  - a. An oversight agency or public authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of TDH.
  - b. An appropriate health care accreditation organization for the purpose of reporting the allegation of failing to meet professional standards or of misconduct by TDH; or,
  - c. An attorney retained by or on behalf of the TDH employee or business associate for the purpose of determining the legal options of the TDH employee or business associate with regard to this TDH policy.

**Reference(s):**

- 45 CFR 164.502(a)
- 45 CFR 164.508-164.512
- 45 CFR Part 2

**Contact(s):**

- Privacy Program Office: (615) 741-1969
- TDH HIPAA Hotline: (877) 280-0054

## Tennessee Department of Health

### HIPAA Policies

#### Privacy

**Policy Title:** Minimum Necessary Information

**Policy Number:** 106

**Effective Date:** March 26, 2013

**Revised date:** January 4, 2022

#### **PURPOSE:**

This policy limits the amount of protected health information (PHI) used or disclosed by TDH workforce members to the minimum necessary and ensures that TDH workforce members have access to the information required to accomplish TDH mission, goal, and objectives.

#### **POLICY:**

##### **General**

- A. TDH will use or disclose only the minimum amount of PHI necessary to provide services and benefits to clients, and only to the extent provided in TDH policies and procedures.
- B. This policy does not apply to:
  - 1. Disclosures to or requests by a health care provider for treatment;
  - 2. Disclosures made to the client about his or her own PHI;
  - 3. Uses or disclosures authorized by the client within the scope of the authorization;
  - 4. Disclosures made to the United States Department of Health and Human Services, Office for Civil Rights, in accordance with subpart C of part 160 of the HIPAA Privacy Rule;
  - 5. Uses or disclosures required by law; and
  - 6. Uses or disclosures required for compliance with the HIPAA Transaction Rule. The minimum necessary standard does not apply to the required or situational data elements specified in the implementation guides under the Transaction Rule.

### **Minimum Necessary Information**

- A. When TDH policy permits use or disclosure of a client's PHI to another entity, or when TDH requests a client's PHI from another entity, TDH employees must make reasonable efforts to limit the amount of PHI to the 'minimum necessary' needed to accomplish the intended purpose of the use, disclosure, or request.
- B. If TDH policy permits a particular disclosure to another entity, TDH may rely on a requested disclosure as being the minimum necessary for the stated purpose if:
  - 1. Making disclosures to public officials permitted under 45 DFR 164.512, and as stated in **TDH HIPAA Policy #105**, "*Uses and Disclosures of Client or Participant Information*," if the public official states the PHI requested is the minimum necessary for the stated purpose(s).
  - 2. The PHI is requested by another covered entity under the HIPAA Privacy Rule.
  - 3. The information is requested by a professional who is a member of the TDH workforce or is a business associate of TDH for the purpose of providing professional services to TDH, if the professional represents that the PHI requested is the minimum necessary for the stated purpose(s); or
  - 4. Documentation or representations that comply with the applicable requirements of **TDH HIPAA Policy #108**, "*Use and Disclosure for Research Purposes & Waiver*", have been provided by a person requesting the PHI for research purposes.

### **Access & Uses of PHI**

- A. TDH will make reasonable efforts to limit each workforce member's access to only the PHI required to carry out his/her duties. These efforts will include internal staff to staff use and disclosure of PHI.
- B. Each office will determine, by category of responsibilities or by individual responsibilities, what level of PHI the workforce members will have access to in order to carry out their duties. Once the determinations have been made, workforce members will be informed. The determinations will be documented and shall include their accessibility to all PHI formats (electronic, as well as, paper).

### **Routine and Recurring Disclosure of a Client's PHI**

- A. For routine and recurring disclosures (including disclosures in routine reports), TDH program areas will:
  - 1. Identify the entity or individual requesting the PHI and the purpose of the request. If the request is **not** compatible with the purpose for which it was collected, follow the "non-routine use" procedures in the following section.

2. Confirm that applicable TDH policies permit the requested use (disclosure is consistent with the program purposes), and that the nature or type of the use recurs (occurs on a periodic basis) within the program or activity;
  3. Identify the type and amount of information necessary to respond to the request; and
  4. If the disclosure is one that must be included in the TDH accounting of disclosures, include documentation required by the appropriate office.
- B. For the purposes of this policy, “routine and recurring” means the disclosure of PHI by TDH, including to TDH non-covered components, without the authorization of the client, for a purpose that is compatible with the reason for which the PHI was collected. The following identifies several examples of uses and disclosures that TDH has determined to be compatible with the purposes for which PHI is collected.
1. TDH will not disclose a client’s entire medical record unless the request specifically justifies why the entire medical record is needed.
  2. Routine and recurring uses include disclosures required by law.
  3. When federal or state agencies – such as US HHS Office for Civil Rights, the US HHS Office of Inspector General, the State of Tennessee Medicaid Fraud Unit, or the Tennessee Comptroller Office – have the legal authority to require TDH to produce PHI necessary to carry out audit, or oversight of TDH programs or activities, TDH will make such PHI available as a routine and recurring use.
  4. When the appropriate TDH official determines that PHI is subject to disclosure under Tennessee law, TDH may make the disclosure as a routine and recurring use.

#### **Non-routine Disclosure of a Client’s PHI**

- A. For the purpose of this policy, “non-routine disclosure” means the disclosure of PHI outside TDH, including to TDH non-covered components, (whether in an ad hoc report or record) that is not for a purpose for which it was collected.
- B. TDH will not disclose a client’s entire medical record unless the request specifically justifies why the entire medical record is required, and applicable laws and policies permit the disclosure of all PHI in the medical record to the requestor.
- C. Requests for non-routine disclosures must be reviewed on an individual basis to limit the PHI disclosed to only the minimum amount of information necessary to accomplish the purpose for which the disclosure is sought.

## **TDH Request for a Client's PHI from Another Entity**

When requesting a client's PHI from another entity, TDH workforce members must limit requests to those that are reasonably necessary to accomplish the purpose for which the request is made. TDH will not request a client's entire medical record unless TDH can specifically justify why the entire medical record is required.

### **Reference(s):**

- 45 CFR Parts 160 and 164

### **Contact(s):**

- Privacy Program Office: (615) 741-1969
- TDH HIPAA Hotline: (877) 280-0054

**Tennessee Department of Health**

**HIPAA Policies**

**Privacy**

**Policy Title:**           **Administrative, Technical, and Physical Safeguards**

**Policy Number:**       **107**

**Effective Date:**       **March 26, 2013**

**Revised Date:**       **January 4, 2022**

**PURPOSE:**

This policy establishes criteria for safeguarding PHI to minimize the risks of unauthorized access, use or disclosure.

**POLICY:**

**General:**

TDH must take reasonable steps to safeguard PHI from any intentional or unintentional use or disclosure in violation of TDH privacy policies.

PHI must be safeguarded in all formats and medium, including paper, electronic, verbal, and visual representations.

**Safeguarding PHI– TDH Workplace Practices**

**A. Paper:**

1. TDH workforce members must make reasonable efforts to ensure safeguarding of PHI including use of locked storage wherever available.
2. Each TDH workplace will ensure that disposal of files and documents is performed on a timely basis, consistent with record retention requirements, and subject to the same safeguarding requirements until destruction occurs.

**B. Verbal:**

1. TDH staff must take reasonable steps to protect the privacy of all verbal exchanges or discussions of PHI, regardless of where the discussion occurs.
2. Each TDH workplace must ensure workforce member’s awareness of the potential for inadvertent verbal disclosure of PHI.

C. Visual:

1. Each TDH workplace must make every effort to ensure that PHI is not visible to unauthorized persons. This includes PHI on desktops, computer screens, fax machines, photocopy machines, printers, other electronic devices, management reports or paper documents in accordance with the appropriate office policy and procedure.

**Safeguarding PHI – TDH Administrative Safeguards**

A. Each office or Program Area determines access to specific PHI by workforce position role, duties and responsibilities.

1. TDH managers and supervisors will determine the role of each of their workforce members and request exceptions based on the needs of their office.
2. Managers are responsible for allowing access to enough PHI for each workforce member to perform their job responsibilities within the minimum necessary standard.

B. TDH managers and supervisors will:

1. Safeguard PHI.
2. Conduct a thorough assessment of each category of responsibilities and/or individual workforce member.
3. Foster a more secure atmosphere and enhance the belief that PHI is important and that protecting privacy is key to achieving TDH goals.
4. Managers will review the safeguards in place and update as needed, seeking to maintain reasonable administrative, technical, and physical safeguards.

C. All TDH workforce members are required to sign a “confidentiality statement” that constitutes a formal commitment to adhere to TDH privacy and security policies concerning PHI.

**Reference(s):**

- 45 CFR § 164.308
- 45 CFR § 164.310
- 45 CFR § 164.312

**Contact(s):**

- Privacy Program Office: (615) 741-1969
- TDH HIPAA Hotline: (615) 280-0054

**Tennessee Department of Health**

**HIPAA Policies**

**Privacy**

**Policy Title:** Use and Disclosure for Research Purposes and Waivers

**Policy Number:** 108

**Effective Date:** March 26, 2013

**Revised Date:** January 4, 2022

**PURPOSE:**

This policy specifies when TDH may use or disclose a client's PHI for research purposes.

**POLICY:**

**General:**

Before TDH uses or discloses a client's PHI for research purposes it must consider the following:

- A. TDH may use or disclose a client's PHI for research purposes as specified in this policy.
- B. All such research disclosures are subject to applicable requirements of state and federal laws and regulations and to the specific requirements of this policy.

**NOTE:** This policy is intended to supplement existing research requirements of the Common Rule, 45 CFR Part 46. The Common Rule is the rule for the protection of human subjects in research promulgated by the U.S. Department of Health and Human Services, and adopted by other general government agencies, including the National Institutes for Health, for research funded by those agencies. In addition, some agencies have requirements that supplement the Common Rule that are applicable to a particular research contract or grant.

- C. De-identified information may be used or disclosed for purposes of research, consistent with **TDH HIPAA Policy #109**, "*De-identification of Client Information and Use of Limited Data Sets.*"
- D. A limited data set may be used or disclosed for purposes of research, consistent with the policies related to limited data set in **TDH HIPAA Policy #109**, "*De-identification of Client Information and Use of Limited Data Sets.*"

- E. TDH may also conduct public health studies, studies that are required by law, and studies or analysis related to its health care operations. Such studies will be discussed in sections of this policy.

### **Institutional Review Board (IRB) or Privacy Board Established by TDH**

TDH has established an IRB in accordance with 45 CFR Part 46 and may establish a privacy board in accordance with 45 CFR § 164.512(i) to perform the duties and functions specified in this policy regarding a research project being conducted, in whole or in part, by TDH or by a TDH office or program.

### **Uses and Disclosures for Research Purposes – Specific Requirements**

- A. TDH may use or disclose client PHI for research purposes with the client’s specific written authorization.
  - 1. Such authorization must meet all the requirements described in **TDH HIPAA Policy #105**, “*Uses and Disclosures of Client Information*.” TDH may indicate as an expiration date such terms as “end of research study,” or similar language.
  - 2. An authorization for use and disclosure for a research study may be combined with any other type of written permission for the same research study.
  - 3. If research includes treatment, the researcher may condition the provision of research related treatment on the provision of an authorization for use and disclosure for such research.
- B. TDH may use or disclose client PHI for research purposes without the client’s written authorization if:
  - 1. TDH obtains documentation that a waiver of a client’s authorization for release of information requirements has been approved by either:
    - a. An institutional review board (IRB); or
    - b. A privacy board which:
      - i. Has members with varying backgrounds and appropriate professional competency as needed to review the effect of the research protocol on the client’s privacy rights and related concerns;
      - ii. Includes at least one member who is not affiliated with TDH, not affiliated with any entity conducting or sponsoring the research, and not related to any person who is affiliated with any such entity; and

- iii. Does not have any member participating in a review of any project in which the member has a conflict of interest.
2. When granting approval of a waiver of a client's authorization for release of PHI, the IRB or privacy board must document:
    - a. A statement identifying the IRB or privacy board that approved the waiver of a client's authorization, and the date of such approval.
    - b. A statement that the IRB or privacy board has determined that the waiver of authorization, in whole or in part, satisfies the following criteria:
      - i. The use or disclosure of a client's PHI involves no more than minimal risk to the privacy of clients, based on at least the following elements:
        - An adequate plan to protect a client's identifying PHI from improper use or disclosure;
        - An adequate plan to destroy a client's identifying PHI at the earliest opportunity consistent with the conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; and
        - Adequate written assurances that the PHI will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research study, or for other research for which the use or disclosure of the PHI would be permitted under this policy;
        - The research could not practicably be conducted without the waiver;
        - The research could not practicably be conducted without access to and use of the client's PHI;
        - A brief description of the PHI for which use or disclosure has been determined to be necessary by the IRB or privacy board;
        - A statement that the waiver of a client's authorization has been reviewed and approved under either normal or expedited review procedures, by either an IRB or a privacy board, pursuant to federal regulations at 45 CFR 14.512(2); and
        - The privacy board chair must sign documentation of the waiver of a client's authorization, or other member as designated by the chair of the IRB or the privacy board, as applicable.

3. In some cases, a researcher may request access to client PHI maintained by TDH in preparation for research or to facilitate the development of a research protocol in anticipation of research. Before agreeing to provide such access to client PHI, TDH should determine whether federal or state law otherwise permits such use or disclosure without client authorization or review and approval of an IRB. If there is any doubt whether the use and disclosure of the information by the researcher falls within this HIPAA exception, review by an IRB or privacy board and formal waiver of authorization is required. If such access falls within this HIPAA exception to authorization and is otherwise permitted by other federal or state law, TDH will only provide such access if TDH obtains, from the researcher, written representations that:
  - a. Use or disclosure is sought solely to review a client's PHI needed to prepare a research protocol or for similar purposes to prepare for the research project;
  - b. No client PHI will be removed from TDH by the researcher in the course of the review;
  - c. The client PHI for which use or access is sought is necessary for the research purposes;
  - d. Researcher and his or her agent agree not to use or further disclose the information other than as provided in the written agreement, and to use appropriate safeguards to prevent the use or disclosure of the information other than is provided for by the written agreement;
  - e. Researcher and his or her agents agree not to publicly identify the information or contact the client whose data is being disclosed; and
  - f. Applicable federal or state law may require such other terms or conditions.
  
4. In some cases, a researcher may request access to PHI maintained by TDH for deceased clients. TDH should determine whether federal or state law otherwise permits such use or disclosure of information about decedents without the decedent's legal representative's authorization or approval of an IRB. There may be instances where it would be inappropriate to disclose information, even where the client that is the subject of the PHI is dead – for example, clients who died of AIDS may not have wanted such information to be disclosed after their deaths. If there is any doubt, whether the use and disclosure of the PHI by the researcher falls within this HIPAA exception, review by an IRB or privacy board and formal waiver of authorization is required. If such access falls within this HIPAA exception to authorization and is otherwise permitted by other federal or state law, TDH will only provide such access if TDH obtains the following written representations from the researcher:
  - a. Representation that the use or disclosure is sought solely for research on the PHI of deceased persons;

- b. Documentation, if TDH so requests, of the death of such persons;
- c. Representation that the client's PHI for which use or disclosure is sought is necessary for the research purposes;
- d. Researcher (and any agent) agree not to use or further disclose the PHI other than as provided in the written agreement, and to use appropriate safeguards to prevent the use or disclosure of the PHI other than is provided for by the written agreement;
- e. Researcher (and any agent) agree not to publicly identify the PHI or contact the personal representative or family members of the decedent; and
- f. Applicable federal or state law may require such other terms or conditions.

### **TDH Public Health Studies and Studies Required by Law**

When TDH operates as a public health authority, TDH is authorized to obtain and use client PHI without authorization for the purpose of preventing injury or controlling disease and for the conduct of public health surveillance, investigations, and interventions. In addition to these responsibilities, TDH may collect, use, or disclose information without client authorization, to the extent that such collection, use, or disclosure is required by law. When TDH uses information to conduct studies pursuant to such authority, no additional client authorization is required nor does this policy require IRB or privacy board waiver of authorization based on the HIPAA Privacy Rule. Other applicable laws and protocols continue to apply to such studies.

### **TDH Studies Related to Health Care Operations**

Studies and data analyses conducted for TDH's own quality assurance purposes and to comply with reporting requirements applicable to federal or state funding requirements fall within the uses and disclosures that may be made without client authorization as TDH health care operations. Neither client authorization nor IRB or privacy board waiver of authorization is required for studies or data analyses conducted by or on behalf of TDH for purposes of health care operations, including any studies or analyses conducted to comply with reporting requirements applicable to federal or state funding requirements.

"Health care operations" as defined in 45 CFR 164.512 includes:

- A. Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that obtaining generalized knowledge is not the primary purpose of any studies resulting from such activities.
- B. Conducting population-based activities relating to improving health care or reducing health care costs, protocol development, case management and care coordination, contacting health care providers and patients with information about treatment alternatives; and related functions that do not include treatment.

- C. Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, and conducting training programs, and accreditation, certification, licensing, or credentialing activities.
- D. Underwriting, premium rating, and other activities related to the creation renewal or replacement of a contract of health insurance or health benefits.
- E. Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs.
- F. Business planning and development, such as conducting cost-management and planning related analyses associated with managing and operating TDH, including improvement of administration or development or improvement of methods of payment or coverage policies; and
- G. Business management and general administrative activities of TDH, including management activities related to HIPAA implementation and compliance; customer services, including the provision of data analyses for other customers; resolution of internal grievances; and
- H. Creating de-identifiable information or a limited data set consistent with **TDH HIPAA Policy #109**, *“De-identification of Client Information and Use of Limited Data Sets.”*

**Exception:** HIV-AIDS information may not be disclosed to anyone without the specific written authorization of the client. Re-disclosure of HIV test information is prohibited, except in compliance with law or written permission from the client. T.C.A. § 68-10-113 limits the release of STD related medical records (including HIV) more stringently than federal law and regulations (HIPAA).

**Reference(s):**

- 45 CFR Part 64
- 45 CFR 164.512
- Tenn. Consolidated Statutes Annotated § 68-10-113.

**Contact(s):**

- Privacy Program Office: (615) 741-1969
- TDH HIPAA Hotline: (877) 280-0054

**Tennessee Department of Health**

**HIPAA Policies**

**Privacy**

**Policy Title:**           **De-identification of Client Information and Use of Limited Data Sets**

**Policy Number:**       **109**

**Effective Date:**       **March 26, 2013**

**Revised Date:**       **January 4, 2022**

**PURPOSE:**

This policy prescribes standards under which client PHI can be used and disclosed without authorization or tracking of disclosures because all information that could identify the client has been removed or restricted to a limited data set. This policy does not apply to PHI transmitted to a business associate.

**POLICY:**

**General:**

- A. De-identified information is client information from which TDH or another entity has deleted, redacted, or blocked identifiers, so that the remaining information cannot reasonably be used to identify a person.
- B. Unless otherwise restricted or prohibited by other federal or state law, TDH can use and share information as appropriate for the work of TDH, without further restriction, if TDH or another entity has taken steps to de-identify the information consistent with the requirements and restrictions defined in this policy.
- C. TDH may disclose PHI to a TDH business associate, acting as an honest broker, for the purpose of deidentifying the PHI of TDH clients.
- D. TDH may use or disclose a limited data set that meets the requirements for a limited data set as defined in this policy, if TDH enters into a data use agreement with the limited data set recipient (or with the data source, if TDH will be the recipient of the limited data set) in accordance with the requirements of a data use agreement as defined in this policy.
- E. TDH may disclose a limited data set for the purposes of research, public health, or health care operations. However, unless TDH has obtained a limited data set that is subject to a data use agreement, TDH is not restricted to using that limited data set for its own activities

or operations. PHI obtained under 45 CFR can be used or disclosed beyond a limited data set so long as it meets the minimum necessary standard.

- F. If TDH knows of a pattern or activity or practice of the limited data set recipient that constitutes a material breach or violation of a data set agreement. TDH will take reasonable steps to cure the breach or end the violation and, if such steps are unsuccessful, TDH will discontinue disclosure of information to the recipient and report the problem to the United States Department of Health and Human Services, Office of Civil Rights.

### **Requirements for De-identification of Client Information**

TDH may determine that the client information is sufficiently de-identified, and cannot be used to identify any individual, only if the requirements listed in *either* A or B (below) are met:

- A. A statistician or other person with appropriate knowledge of, and experience with, generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:
  - 1. Has applied such principles and methods, and determined that the risk is minimal that the information could be used alone or in combination with other reasonable available information, by a recipient of the information to identify the person whose information is being used; and
  - 2. Has documented that methods and results of the analysis that justify such a determination.
- B. TDH has ensured that:
  - 1. The following identifiers of the individual or of relatives, employers, and household members of the individual are removed:
    - a. Names;
    - b. All geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code, and their equivalent geo codes. However, the initial three digits of a zip code may remain on the information if, according to current publicly available data from the Bureau of the Census, the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and the initial three digits for all such geographic units containing 20,000 or fewer people is changed to 000.
    - c. All elements of dates (except year) for dates directly relating to an individual, including birth date, dates of admission and discharge from a health care facility, and date of death. For persons aged 90 and older, all elements of dates (including year) that would indicate such age must be removed, except that such ages and elements may be aggregated into a single category of "age 90 or older; "

- d. Telephone numbers;
  - e. Fax numbers;
  - r. Electronic mail addresses;
  - g. Social security numbers;
  - h. Medical record numbers;
  - i. Health plan beneficiary numbers;
  - j. Account numbers;
  - k. Certificate or license numbers;
  - l. Vehicle identifiers and serial numbers, including license plate numbers;
  - m. Device identifiers and serial numbers;
  - n. Web Universal Resource Locators (URLs);
  - o. Internet Protocol (IP) address numbers;
  - p. Biometric identifiers, including fingerprints and voiceprints;
  - q. Full face photographic images and any comparable images; and
  - r. Any other unique identifying number, characteristic, or codes, except as permitted under the Re-identification section below, of this policy; and
2. TDH has no actual knowledge that the information could be used alone or in combination with other information to identify an individual who is the subject of the information.
- C. TDH will designate the statistician or other person referred to in section A above, who may be either:
1. A TDH workforce member;
  2. An employee of another governmental agency; or
  3. An outside contractor or consultant, subject to TDH contract and personnel policy.

## **Re-identification of De-identified Information**

TDH may assign a code or other means of record identification to allow information to be de-identified under this policy to be re-identified by TDH, except that:

1. The code or other means of record identification is not derived from or related to information about the individual and cannot otherwise be translated to identify the individual; and
2. TDH does not use or disclose the code or other means of record identification for any other purpose and does not disclose the mechanism for re-identification.

## **Requirements for a Limited Data Set**

A limited data set is information that excludes the following direct identifiers of the individual, or of relatives, employers, or household members of the individual:

1. Names;
2. Postal address information, other than town city, state and zip code;
3. Telephone numbers;
4. Fax numbers;
5. Electronic mail addresses;
6. Social Security numbers;
7. Medical record numbers;
8. Health plan beneficiary numbers (such as Medicaid Prime Numbers);
9. Account numbers;
10. Certificate/ license numbers
11. Vehicle identifiers and serial numbers, including license plate numbers;
12. Web Universal Resource Locators (URLs);
13. Internet Protocol (IP) address numbers;
14. Biometric identifiers, including finger and voice prints;
15. Full face photographic images and any comparable images.

## **Contents of a Data Use Agreement**

- A. TDH may disclose a limited data set only if the entity receiving the limited data set enters into a written agreement with TDH in accordance with subsection (B) immediately below, that such entity will use or disclose the PHI only as specified in the written agreement.
- B. A data use agreement between TDH and the recipient of the limited data set must:
  1. Specify the permitted uses and disclosures of such information by the limited data set recipient. TDH may not use the agreement to authorize the limited data set recipient to use or further disclose the information in a manner that would violate the requirements of this policy if done by TDH.
  2. Specify who is permitted to use or receive the limited data set; and
  3. Specify that the limited data set recipient will:
    - a. Not use or further disclose the information other than as specified in the data set use agreement or as otherwise required by law;
    - b. Use appropriate safeguards to prevent use or disclosure of the information other than as specified in the data use agreement;
    - c. Report to TDH if the recipient becomes aware of any use or disclosure of the information not specified in its data use agreement with TDH;
    - d. Ensure that any agents to whom it provides the limited data set (including a subcontractor), agrees to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and
    - e. Not identify the information or contact the individuals whose data is being disclosed.

### **Reference(s):**

- 45 CFR 164.514

### **Contact(s):**

- Privacy Program Office: (615) 741-1969
- TDH HIPAA Hotline: (877) 280-0054

## Tennessee Department of Health

### HIPAA Policies

#### Privacy

**Policy Title:** Business Associates

**Policy Number:** 110

**Effective Date:** March 26, 2013

**Revised Date:** January 4, 2022

#### **PURPOSE:**

This policy specifies when TDH may disclose a client's PHI to a TDH business associate, and to specify provisions that must be included in TDH contracts with business associates.

#### **POLICY:**

##### **General**

- A. This policy only applies to contractors or business partners that meet the definition of a "business associate."
- B. If a contractor or business partner is a "business associate" those contracts that define the contractual relationship remain subject to all federal and state laws and policies governing the contractual relationship. A "business associate" relationship also requires additional contract provisions. The additional contract requirements are described in this policy. These provisions provide that Business Associates are directly liable to United States Department of Health and Human Services (HHS).
- C. "Business Associate" means (per 45 CFR 160.103):
  1. With respect to TDH, a person or entity who:
    - a. On behalf of TDH, but other than in the capacity of a TDH workforce member, performs or assists in the performance of a function or activity involving the use or disclosure of PHI, including claims processing or administration, data analysis, utilization review, quality assurance, billing benefit management; or
    - b. Provides, other than in the capacity of a TDH workforce member, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for TDH, where the provisions of the service involve the disclosure of PHI from TDH, or from another TDH business associate to the person.
  2. A covered entity may be a business associate of another covered entity.

- D. A business associate relationship is formed only if PHI is to be used, created, or disclosed in the relationship and it meets the definition of section C above.
- E. The following are not business associates or business associate relationships:
1. TDH workforce members;
  2. Medical providers providing treatment to clients;
  3. Enrollment or eligibility determinations, involving TDH clients, between government agencies;
  4. Payment relationships, such as when TDH is paying medical providers, or other entities for services to TDH clients when the entity is providing its own normal services that are not on behalf of TDH;
  5. When a client's PHI is disclosed based solely on a client's authorization;
  6. When a client's PHI is not being disclosed by TDH or created for TDH;
  7. When the only information being disclosed is information that is de-identified in accordance with **TDH HIPAA Policy #109**, "*De-identification of Client or Participant Information and Use of Limited Data Sets*;" and
  8. Persons or organizations (*e.g.*, janitorial services) whose duties do not involve the use or disclosure of PHI and where any access to PHI by such persons would be incidental, if at all.
- F. TDH may disclose a client's PHI to a business associate and may allow a business associate to create or receive a client's PHI on behalf of TDH, if:
1. TDH first enters into a written contract, or other written agreement or arrangement, with the business associate before disclosing a client's PHI to the business associate, in accordance with the contract requirements specified in this policy.
  2. The written contract or agreement provides satisfactory assurance that the business associate will appropriately safeguard the information.

### **Contract Requirements Applicable to Business Associates**

- A. A contract between TDH and a business associate must include terms and conditions that:
1. Establish the permitted and required uses and disclosures of PHI by the business associate. The contract may not authorize the business associate to further use or

disclose PHI obtained from TDH, except that the contract may permit the business associate to:

- a. Use and disclose PHI for the proper management and administration of the business associate; and
- b. Collect data relating to TDH operations.

2. Provide that the business associate will:

- a. Not use or further disclose PHI other than as permitted or required by the contract or as required by law;
- b. Use appropriate safeguards to prevent use or disclosure of PHI other than as provided for by the contract;
- c. Report to TDH any use or disclosure not allowed by the contract of which the business associate becomes aware;
- d. Ensure that any agents or subcontractors to whom it provides PHI agrees to the same restrictions and conditions that apply to the business associate under the contract;
- e. Ensure that business associates have mechanisms in place to protect clients' rights regarding PHI;
- f. Make its internal practices, books, and records relating to the use and disclosure of PHI available to TDH and to HHS for the purpose of determining TDH compliance with federal requirements; and
- g. At termination of the contract, if reasonably feasible, return or destroy all PHI that the business associate still maintains in any form, and keep no copies thereof. If not feasible the business associate will continue to protect the PHI.

3. Authorized termination of the contract if TDH determines that the business associate has violated a material term of the contract.

B. If the business associate of TDH is another governmental entity:

1. TDH may enter into a memorandum of understanding (MOU), rather than a contract, with the business associate if the MOU contains terms covering all objectives of the contract requirements outlined in this policy;
2. The written contract, agreement, or MOU does not need to contain specific provisions required under 2.a., above, if other law or regulations contain requirements applicable to the business associate that accomplish the same objective.

3. Business Associate shall require any agent, including a subcontractor, to agree to the same restrictions and conditions as applied to the Business Associate.
- C. If a business associate is required by law to perform a function or activity on behalf of TDH or to provide a service to TDH, TDH may disclose PHI to the business associate to the extent necessary to enable compliance with the legal requirement without a written contract or agreement if:
1. TDH attempts in good faith to obtain satisfactory assurances from the business associate that the business associate will protect PHI to the extent specific in 2.a., above; and
  2. If such attempt fails, TDH documents the attempt and the reasons that such assurances cannot be obtained.
- D. Other requirements for written contracts or agreements:

The written contract or agreement between TDH and the business associate may permit the business associate to:

1. Use information it receives in its capacity as a business associate to TDH, if necessary:
  - a. For proper management and administration of the business associate; or
  - b. To carry out its legal responsibilities.
2. Disclose information it receives in its capacity as a business associate if:
  - a. The disclosure is required by law; or
  - b. The business associate receives assurances from the person to whom the PHI is disclosed that:
    - i. It will be held or disclosed further only as required by law or for the purpose to which it was disclosed to such person; and
    - ii. the person notifies the business associate of any known instances in which the confidentiality of the PHI has been breached.

### **Responsibilities of TDH in Business Associate Relationship**

- A. TDH's responsibilities in business associate relationships include, but are not limited to, the following:

1. Receiving and logging a client's complaints regarding the uses and disclosures of PHI by the business associate or the business associate relationship;
  2. Receiving and logging reports from business associate of possible violations of the business associate contracts;
  3. Implementation of corrective action plans, as needed; and
  4. Mitigation, if necessary, of any known violations up to and including contract termination.
- B. TDH will provide the business associates with applicable contract requirements, and may provide consultation to business associates as needed on how to comply with contract requirements regarding PHI.

**Business Associate Non-compliance**

- A. If TDH knows of a pattern of activity or practice of a business associate that constitutes a material breach or violation of the business associate's obligation under the contract or other arrangement, TDH must take reasonable steps to cure the breach or end the violation, as applicable, including working with and providing consultation to the business associate.
- B. If such steps are unsuccessful, TDH must:
1. Terminate the contract or arrangement, if feasible; or
  2. If termination is not feasible, report the problem to US HHS.

**Reference(s):**

- 45 CFR 160 & 164

**Contact(s):**

- Privacy Program Office: (615) 741-1969
- TDH HIPAA Hotline: (877) 280-0054

**Tennessee Department of Health**

**HIPAA Policies**

**Privacy**

**Policy Title:**           **Enforcement, Sanctions, and Penalties for Violations of Individual Privacy**

**Policy Number:**       **111**

**Effective Date:**       **March 26, 2013**

**Revised Date:**       **January 4, 2022**

**PURPOSE:**

This policy specifies enforcement, sanction, penalty, and disciplinary actions that may result from violation of the HIPAA Privacy and Security Rule and provides guidelines on how to achieve the required standards.

**POLICY:**

**General:**

- A. All employees, volunteers, interns, and members of the TDH workforce must guard against improper uses or disclosures of a TDH client's PHI.
  - 1. If a TDH workforce member is uncertain if a use or disclosure is permitted, they are to consult with a supervisor in the TDH workplace. The Department Privacy Officer may also be consulted on any disclosure question.
  - 2. The Department Privacy Officer may consult with the Office of General on any disclosure question.
- B. All workforce members are required to be aware of their responsibilities under TDH HIPAA policies and will be expected to sign a "Confidentiality Statement" as part of the State of Tennessee's Code of Conduct.
- C. Supervisors are responsible for assuring that workforce members have appropriate access to PHI, whether electronic, hard copy, or verbally, and are informed of their responsibilities.
- D. TDH workforce members who violate TDH policies and procedures regarding the safeguarding of an individual's PHI are subject to appropriate disciplinary action by TDH up to and including immediate dismissal from employment. TDH workforce members may also be subject to legal action by the affected individual who may want to pursue a tort

claim against the State of Tennessee or a lawsuit against the state and the workforce member.

- E. TDH workforce members who knowingly or willfully violate state or federal law regarding improper use or disclosure of an individual's PHI may be subject to criminal investigation and prosecution or to civil monetary penalties as may be enforced by the Office for Civil Rights (OCR) within the United States Department of Health and Human Services (US HHS).
- F. If TDH, as a state agency, fails to enforce privacy safeguards, TDH may be subject to administrative penalties by OCR, including federal funding penalties.

### **Retaliation Prohibited**

Neither TDH as an entity, nor any TDH workforce member will intimidate, threaten, coerce, discriminate against, or take any other form of retaliatory action against:

- 1. Any individual for exercising any right established under TDH policy, including filing a complaint with TDH or OCR.
- 2. Any individual or other person for:
  - a. Filing a complaint with TDH or with OCR as provided in TDH's HIPAA policies;
  - b. Testifying, assisting, or participating in an investigation, compliance review, proceeding or hearing relating to TDH HIPAA policy and procedures; or
  - c. Opposing any unlawful act or practice, provided that:
    - i. The individual or other person (including a TDH workforce member) has a good faith belief that the act or practice being opposed is unlawful; and
    - ii. The manner of such opposition is reasonable and does not involve a use or disclosure of an individual's PHI in violation of TDH policy.

### **Reference(s):**

- 45 CFR 160.530

### **Contact(s):**

- Privacy Program Office: (615) 741-1969
- TDH HIPAA Hotline (877) 280-0054

# Tennessee Department of Health

## HIPAA Policies

### Privacy

**Policy Title:** Mitigation Efforts

**Policy Number:** 112

**Effective Date:** March 26, 2013

**Revised Date:** January 4, 2022

#### **PURPOSE:**

This policy specifies the extent that mitigation must take place, if TDH use or disclosure of client PHI in violation of the HIPAA Privacy Security Rules or TDH policy resulted in any known harmful effect.

#### **POLICY:**

##### **General:**

TDH has the duty to mitigate, to the extent practicable, any known harmful effects due to uses or disclosures of PHI in violation of the HIPAA Privacy and Security Rules or TDH policies.

The duty to mitigate arises only when TDH has actual knowledge of inappropriate use or disclosure of PHI either by TDH or a business associate. Offices are required to take reasonable steps to reduce the harmful effects of those actions about which they are aware.

TDH offices are obligated to undertake reasonable monitoring of the activities of workforce members. When unauthorized use or disclosure of PHI takes place, the incident(s) will be reviewed with the Department Privacy Officer, and actions to lessen the possibility that similar uses or disclosures do not occur in the future will be taken. Such actions may include revision of procedures, workforce education, business associate contract revision or other appropriate actions. If the use or disclosure is made by the TDH workforce, appropriate action should take place immediately.

The Department Privacy Officer must be notified immediately when unauthorized uses or disclosures of PHI take place or are discovered in order to determine if mitigation efforts are required. This includes both internal and external unauthorized uses or disclosure of PHI.

**Reference(s):** 45 C.F.R. § 164.530(f).

#### **Contact(s):**

- Privacy Program Office: (615) 741-1969
- TDH HIPAA Hotline: (877) 280-0054

**Tennessee Department of Health**

**HIPAA Policies**

**Privacy / Security**

**Policy Title:** Breach Notification of Unsecured Protected Health Information

**Policy Number:** 113

**Effective Date:** March 26, 2013

**Revised Date:** January 4, 2022

**PURPOSE:**

This policy establishes criteria for issuing a notification in the case of a breach of unsecured PHI.

**POLICY:**

TDH must notify clients promptly if their unsecured PHI has been or is reasonably believed to have been breached.

**Definitions:**

*A breach* is defined as "the acquisition, access, use, or disclosure" of PHI in a manner that violates federal law and regulations (HIPAA) and also, "compromises the security or privacy of the PHI." 45 C.F.R. § 164.402.

*"Unsecured" PHI* is PHI that is "not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by HHS." 45 C.F.R. § 164.402.

**Risk Assessment**

TDH shall perform a *Risk Assessment* to determine if notification is required. Breach notification under HIPAA is NOT required if TDH demonstrates through the Risk Assessment that there is a low probability that the PHI has been compromised.

In making this determination, the Risk Assessment must consider each of the following factors:

1. The nature and extent of the PHI involved, including types of identifiers and the likelihood of re-identification;

2. The unauthorized person who used the PHI or to whom the PHI was disclosed;
3. Whether the PHI was actually acquired or viewed; and
4. The extent to which the risk to the PHI has been mitigated.

Nothing prevents TDH from providing notification for each breach without performing the Risk Assessment.

TDH has the burden of proof to demonstrate that all notifications were provided or that an impermissible use or disclosure did not constitute a breach and to maintain documentation of the Risk Assessment performed. In the event of a breach by a Business Associate, TDH maintains the obligation to notify affected individuals of the breach. 45 CFR § 164.404.

### **Breach Exceptions**

Exceptions to the definition of a breach are:

1. Any unintentional acquisition, access, or use of PHI by a workforce member of TDH or person acting under TDH authority, if such acquisition, access, or use was in good faith, within that person's scope of authority, and did not result in further impermissible use or disclosure of the PHI;
2. Any inadvertent disclosure by a person who is authorized to have access to such PHI to another authorized person in TDH or a Business Associate and the PHI is not further used or disclosed in an impermissible manner; and
3. A disclosure of PHI where TDH has a good faith belief that the unauthorized person who received the PHI would not reasonably have been able to retain such PHI.

### **Notification to Privacy Officer**

Workforce members must immediately inform the Department Privacy Officer upon becoming aware or informed of any potential unauthorized use or disclosure of PHI. The Department Privacy Officer, upon learning of the potential unauthorized use or disclosure of PHI, will commence an investigation of the unauthorized use or disclosure within seven (7) days. The Department Privacy Officer will notify the TDH Security Officer, the Breach Response Team, and any other TDH workforce members as needed.

### **Breach Response Team**

A TDH Breach Response Team has been established by TDH for the purpose of receiving and reviewing the findings of Risk Assessments conducted by the Department's Privacy Officer and Security Officer and advising what further action, if any, is needed.

The Breach Response Team shall be made up of a representative from the TDH Office of

Human Resources, the Department Privacy Officer, the TDH Security Officer, the TDH Office for Information Technology Services, the TDH Office of General Counsel, the TDH Office of Internal Audit, and a representative from the TDH division or office in which the unauthorized use or disclosure of PHI occurred. In the event any member is absent or unavailable to serve, their designee may serve in their absence.

Following completion of the investigation by the Privacy and Security Officers, the Department Privacy Officer may convene the Breach Response Team within a reasonable time but no later than thirty (30) days following the completion of the initial investigation.

### **Notification to Individual**

TDH must notify the affected individual(s) "without unreasonable delay" and in no case later than 60 calendar days after TDH became aware of the unauthorized use or disclosure of PHI.

The notice shall be made in writing, except when TDH does not have the correct contact information for the individual or where there is particular urgency to the notification. The notice to the individual must contain the following five (5) elements:

1. A brief description of what occurred, including, to the extent known, the date of the breach and the date on which the breach was discovered;
2. A description of the types of unsecured PHI that were involved in the breach;
3. A description of the steps the individual should take in order to protect themselves from potential harm resulting from the breach;
4. A description of what TDH is doing to investigate and mitigate the breach, including any harm to affected individuals, and to prevent future breaches; and
5. Instructions for the individual to contact TDH to ask questions or learn additional information. Contact information must include a toll-free telephone number, an e-mail address, web site, or postal address.

The notice must be approved by the Breach Response Team before it is sent to the affected individual(s).

### **Other Notice Requirements**

If the breach of the unsecured PHI involves more than 500 clients of the department, TDH must notify media outlets within the state without unreasonable delay and no later than 60 calendar days after the discovery of the breach. The TDH must also notify the Secretary of US HHS of any breach involving 500 or more people at the time it notifies affected individual(s). The Department Privacy Officer will notify the Secretary of US HHS. The notification to the media outlet will be handled through TDH's Communications

Office in conjunction with the Department Privacy Officer. For breaches affecting less than 500 individuals, the Department Privacy Officer shall provide a copy of the log of all breaches to the Secretary of US HHS within 60 days after the end of each calendar year.

### **Training Employees**

The Department Privacy Officer must ensure that all current and new employees, including management, are trained on this policy consistent with the requirements of **Policy 103**, “*Administrative Requirements for the Implementation of HIPAA.*”

### **Reference(s):**

- 45 CFR 160 & 164, Subpart D

### **Contact(s):**

- Privacy Program Office: (615) 741-1969
- Security Officer: [security.health@tn.gov](mailto:security.health@tn.gov)
- TDH HIPAA Hotline: (877) 280-0054