State of Tennessee

Department of Health

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

Policies and Procedures Manual

State of Tennessee
Department of Health
Health Insurance Portability and Accountability Act {HIPAA)
Policies and Procedures Manual

Table of Contents

HIPAA Privacy Policies and Procedures

Tennessee Department of Health

HIPAA Policies

Privacy

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

Policy Number: **101**

Effective Date: **March 26, 2013**

PURPOSE:

To issue instructions to all bureaus, 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.

Definitions:

Protected Health Information (PHI) "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."

Workforce Members means employees, volunteers, trainees, 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 TDH.

Client for the purpose of HIPAA is defined as an individual for whom the TDH uses or maintains PHI such as:

1. birth and death records,
2. infectious disease records,
3. health registries,

4. statistical data,

5. information obtained through an investigative or certification process of the TDH, etc., and

6. those who apply or receive health services through TDH.

Licensee is a person or entity that applies for or receives 1) a license, 2) a certification, or 3) a registration, or similar authority from TDH to perform or conduct a service, activity or function.

Provider is a person or entity who may seek reimbursement or payments from TDH as a provider of services to TDH clients. (Not pertaining to TDH when TDH is a direct provider of services.)

Treatment, Payment and Health Care Operations (TPO) includes all of 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.

POLICY:

General Overview

TDH may collect, maintain, use, transmit, share and/or disclose information about clients, providers, and licensees, to the extent needed to administer TDH programs, services and activities. TDH will safeguard all PHI about clients, providers, and licensees, inform clients, providers, and licensees about TDH's privacy practices and respect clients', providers', and licensees' 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) Licensees or 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 licensees or 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 stricter requirement upon any TDH policy regarding the privacy or safeguarding of information, TDH shall act in accordance with the stricter standard.

TDH staff shall act in accordance with established TDH policy and procedures regarding the safeguarding of client information, whether health-related or not, in all TDH programs, services and activities. In the event that more than one policy applies but compliance with all such policies cannot reasonably be achieved, the TDH employee will seek guidance from supervisors according to established TDH policy and procedures. TDH staff 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 the TDH.

B. TDH will provide a copy of the current ***"TDH Notice of Privacy Practices"*** to any client who requests a copy. However, where TDH is a direct provider to the client, TDH is required to give a copy of the notice to the client on the first date that they receive services on or after March 26, 2013. 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 documentation as to the reason why one was not received must be made 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 he 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 and posted 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: The TDH must designate an individual to be the Department Privacy Officer, responsible for the development and implementation of department-wide policies and procedures relating to the safeguarding of PHI.

2. Subsidiary Privacy Officers will be appointed to represent bureaus/offices, 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, and maintenance of, and adherence to the department's policies concerning privacy. Establish and administer a process for receiving, documenting, tracking, investigations, and taking action on all complaints. Ensure that the Department is 1) in compliance with its privacy practices, and 2) consistently applies sanctions for failure to comply with privacy policies for all individuals in the Department's workforce 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 these to the Department Privacy Officer.

C. Workforce Training Requirements

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

1. On or before March 26, 2013, 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. After March 26, 2013, each new workforce member, or workforce member reporting to work for the first time since March 26, 2013, 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

NOTE: Revisions to the HIPAA Privacy Policies became effective on March 26, 2013. However, covered entities were granted 180 days beyond the effective date to become completely compliant with these policies in their program areas. Each bureau/office shall strive to achieve compliance in all areas as soon as feasible.

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

1. The 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. The TDH must change its policies and procedures as necessary and appropriate to conform to changes in law or regulation. The 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. Where necessary, TDH must make correlative changes in its privacy notice. The TDH may not implement a change in policy or procedure prior to the effective date of the revised privacy notice when required.

3. The TDH, and each bureau/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 #105**, *"Administrative, Technical, and Physical Safeguards."*

   b. Complaint process for documenting and referring complaints received by clients as outlined in **TDH HIPAA Policy #102**, *"Clients' Privacy Rights."*

   c. Application of sanctions and documentation of the application of appropriate sanctions against workforce members as outlined in **TDH HIPAA Policy #109**, *"Enforcement, Sanctions, and Penalties for Violation of Individual Privacy."*

   d. Each bureau/office must mitigate, to the extent practicable, any inappropriate use or disclosure of PHI by TDH or any of its business associates as outlined in **TDH HIPAA Policy #110**, *"Mitigation Efforts."*

   e. Neither the TDH nor any bureau/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 #102**, *"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 #102**, *"Clients' Privacy Rights."*

   b. The requirements TDH needs to follow regarding the uses and disclosures of client information is outlined in **TDH HIPAA Policy #103**, *"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 #104**, *"Minimum Necessary Information."*

d. TDH may use or disclose client's information for research purposes as outlined in **TDH HIPAA Policy #106,** *"Use and Disclosure for Research Purposes and Waivers."*

e. TDH staff 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 #107,** *"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 #108,** *"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: **102**

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

PURPOSE:

The intent of this policy is to establish the privacy rights that TDH clients have regarding the use and disclosure of their Protected Health Information (PHI) that is held by TDH, and to describe the process for filing a complaint should clients feel 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 the distribution of the notice is addressed in **TDH HIPPA Policy #101,** *"Administrative Requirements for the Implementation of HIPPA."*

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

1. Access to their own information, consistent with certain limitations;

a. Clients have the right to access, inspect, and obtain a copy of information on their own cases in TDH files or records, consistent with federal and Tennessee law. TDH will recognize the right of the personal representative of a deceased client to obtain a copy of PHI for the deceased. However, death certificates with cause of death will only be released in accordance with T.C.A. §68-3-205.

b. All requests for access will be made in writing in accordance with the appropriate bureau/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 see information about him or her, except as provided below:

i) If a person identified in the file is a minor child of the client, and the client is authorized under Tennessee law to have access to the minor's information or to act on behalf of the minor for making decisions about the minor's care, the client may also obtain information about the minor.

ii) If the person requesting information is recognized under Tennessee law as a legal guardian or legal custodian of the client and is authorized by Tennessee law to have access to the client's information or to 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 disclose to a family member, other relative or a close personal friend of the client, 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) In cases where the information is not maintained or accessible to TDH on-site, TDH must act on the client's request no later than 30 days after receiving the request.

ii) If TDH is unable to act within these 30-day limits, 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 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 any fees.

iv) TDH must arrange with the client for providing 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 protected information, and 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 inform the client of where to direct the request access.

2. **The TDH can deny access to the client to his PHI under the following limitations:**

a. TDH may deny clients access to his own health information if federal law prohibits the disclosure. Under federal law, clients have the right to access, inspect, and obtain a copy of their own health information in TDH files or records **except for:**

i) Information that, in good faith, TDH believes can cause harm to the client, or to any other person;

ii) 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;

iii) Information compiled for use in civil, criminal, or administrative proceedings;

iv) Information that is subject to the federal Clinical Laboratory Improvement Amendments of 1988, or exempt pursuant to 42 CFR 493.3(a)(2);

v) Documents protected by attorney work-product privilege; and

vi) Information where release is prohibited by state or federal laws.

b. Before TDH denies a client or their personal representative access to their information because there is a good faith belief that its disclosure could cause harm to the client or to another person, the TDH's decision to deny must be made by a licensed health care professional or other designated staff. TDH must make a review of this denial available to the client. If the client wishes to have this denial reviewed, the review must be done by a licensed 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 departmental 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 of PHI that TDH has made for any period of time, not to exceed six years, preceding the date of requesting the accounting. This right does not apply to disclosures made prior to March 26, 2013; however, a bureau/office may disclose prior to that date.

2. The 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 or for purposes described in **"TDH Notice of Privacy Practices."**

3. Clients may make request for an accounting of disclosure at any TDH office, either in the central office, or at a regional or local office. The office where the request is received is required to only make an accounting of the disclosures that were made by that office. When the accounting is made to the client, each office should include a statement that indicates that this is an accounting of disclosures for their particular office only, i.e. "This is an accounting of the disclosures made by the Wilson County Health Department only. If you are interested in whether or not other disclosures may have been by the TDH, please contact the Tennessee Department of Health Privacy Officer at....."

4. The Department Privacy Officer will be responsible for the accounting of disclosures received by his office. The Department Privacy Officer will do all the research to assure the accounting includes disclosure for the entire department and will issue the accounting to the client.

5. All requests for an accounting of disclosures will be made in writing by the client.

6. Disclosures that are not required to be tracked and accounted for by TDH are those that are:

   a. Made within TDH;

   b. Authorized by the client;

   c. Made prior to March 26, 2013;

   d. Made to carry out treatment, payment, and health care operations;

e. Made to the client;

f. Made as part of a limited data set in accordance with the **TDH HIPPA POLICY #107**, *"De-identification of Client Information and Use of Limited Data Sets;"*

g. For national security or intelligence purposes;

h. Required by law;

i. Made to a business associate and/or other state agencies covered by a Business Associate Agreement or Memorandum of Understanding; or

j. Covered under a disclosure protocol for that appropriate office.

7. Disclosures that are required to be tracked must be done in accordance with the appropriate bureau/office policy and procedure. The accounting must include, for each disclosure:

a. The date of the disclosure;

b. The name, and address, if known, of the person or entity who received the disclosed information;

c. A brief description of the information disclosed; and

d. A brief statement of the purpose of the disclosure that reasonably informs the client of the basis for the disclosure, or in lieu of such statement, a copy of the client's written request for a disclosure, if any.

8. TDH will temporarily suspend a client's right to receive an accounting of disclosures that TDH has made to a health oversight agency or to a law enforcement official; for a length of time specified by such agency or official, if:

a. The agency or official provides a written statement to TDH that such an accounting would be reasonably likely to impede their activities

b. However, if such agency or official makes an oral request, TDH will:

i) Document the oral request, including the identity of the agency or official making the request;

ii) Temporarily suspend the client's right to an accounting of disclosures pursuant to the request; and

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.

9. TDH must act on the client's request for an accounting no later than 60 days after receiving the request, subject to the following:

   1. 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 limit, and inform the client of the date by which TDH will provide the accounting.

   2. TDH will use only one such 30-day extension.

   3. In addition to the accounting of disclosures that is given to a client, a copy of any disclosure protocol should also be given to the client that indicates that if any of the situations described in the protocol were met, his PHI may have been disclosed to the specified agency.

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 their protected information, or if they have 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 Tennessee Department of Health's HIPAA 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. The TDH workforce may not require clients to waive their rights to file a complaint as a condition of providing of 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 or his designee will receive, review and determine the action to be taken on all complaints. The Department Officer will document and maintain all complaints, the findings from 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 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;

ii) Disclosure of health information to a relative or other person who is involved in the client's care;

b. TDH is not obligated to agree to a 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.

c. TDH is not required to agree to a restriction requested by the client.

i) 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.

ii) In an emergency situation, TDH may use or disclose such information to the extent needed to provide the emergency treatment to the client.

d. TDH will document the reasons for granting or denying the request for restriction in the client's hard copy or electronic record.

i) Prior to any use or disclosure of client information, TDH staff must confirm that such use of disclosure has not been granted a restriction by reviewing the client's case 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 case 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.

2. 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, fax 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 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.

3. Rights of clients to request amendments to their information.

a. Clients have the right to request that TDH amend their information in TDH files.

b. All requests for amendments must be made in writing and a justification must be given to support the request for the amendment in accordance with the appropriate bureau/office policy and procedure.

c. TDH is not obligated to agree to an amendment and may deny the requests or limit its agreement to amend. Prior to any decision, based on a client's request for TDH to amend a previously documented health or medical record, the bureau's medical director or a licensed health care professional designated by the bureau director shall review the request and any related documentation. The licensed health care professional may be a TDH staff person involved in the client's case.

d. Prior to any decision to amend any other information that is not a health or medical record, a TDH staff person 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 of the amendment; and

iv) Make reasonable efforts to inform, and to provide the amendment within a reasonable time to:

- Persons named by the client as having received protected information and who thus need the amendment; and

- Persons, including business associates of TDH, which TDH know have the protected information 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;

iv) The Information is not part of TDH records; or

v) 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 that 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 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 receipt; and
- TDH will use only one such 30-day extension.

E. **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 Disclosures of Client Information**

Policy Number: **103**

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

PURPOSE:

The intent of this policy is to specify when a client's protected health information (PHI) can be used or disclosed without the client's prior authorization. It will also specify how to use or disclose PHI when there is a client's authorization.

POLICY:

General – Client Authorization

TDH may disclose information for purposes of payment, treatment, and health care operations without client authorization unless otherwise required by bureau/office policy.

TDH shall not use or disclose any PHI about a client of TDH 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 as otherwise required by state or federal law.

A. A signed authorization is required in the following situations:

1. Prior to a client's enrollment in a TDH health service, if necessary for determining eligibility or enrollment;

2. For disclosure to an employer for use in employment-related determination; and

3. For research purposes unrelated to the client's treatment;

4. For any purpose in which state or federal law requires a signed authorization.

B. TDH may obtain, use, or disclose information only if the written authorization (excluding authorization for TPO if required by bureau/office policy) includes all the required elements of a valid authorization. The required elements are:

1. A description of the information to be used or disclosed that identifies the purpose of the information in a specific and meaningful fashion:

2. The name or other specific information about the person(s), classification of persons, or entity (i.e., TDH or specified TDH program) authorized to make the specific use or disclosure;

3. The name or other specific identification of the person(s), classification of persons, or entity to whom TDH may make the requested use or disclosure;

4. An expiration date, or an expiration event that relates to the client or to the purpose of the use or disclosure

5. Signature of the client, or of the client's personal representative, and the date of signature; and

6. If the client's personal representative signs the authorization form instead of the client, a description or explanation of the representative's authority to act for the client, including a copy of the legal court document (if any) appointing the personal representative, must also be provided.

C. Uses and disclosures must be consistent with what the client has authorized on the signed authorization form.

D. TDH may not require the client to sign an authorization as a condition of providing treatment services or to obtain payment for health care services.

E. Each authorization for use or disclosure of a client's information must be fully completed jointly by the staff member and the client, whenever possible, with the staff worker taking reasonable steps to ensure that the client understands why the information is to be used or released.

F. TDH must document and retain each signed authorization form for a minimum of six years.

G. When TDH receives a signed authorization from an outside entity, TDH must verify that it is a valid authorization (excluding authorization for TPO if required by bureau/office policy) and contains all the required information before TDH will release or disclose 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. Public health activity is defined as those duties necessary to prevent or control disease or injury; reporting vital events, such as births or deaths; and conducting public health surveillance, or interventions, etc.

1. Information about clients received or held by TDH as a governmental public health authority shall be safeguarded against loss, interception or misuse.

2. Allowable uses and disclosures for public health activities are as follows:

   a. A governmental public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability. This include 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 bureau/office and are included in the Department'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, that is 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 purposes 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, replacement, 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 the **TDH HIPAA Policy #106,** *"Use and Disclosure for Research Purposes & Waivers."*

c. Where state or federal law prohibits or restricts uses and disclosure of information obtained or maintained for public health purposes, such use and disclosure shall be denied or restricted.

4. Operation of the Public Health Laboratory

a. 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 requests of any state, county, or city institution or officer, and at the request of any licensed physician.

b. Laboratories are health care providers with an "indirect treatment relationship" as defined in federal regulations 45 CFR 164.501 and in accordance with CFR 45 164.506 (a)(2)(i).

c. TDH is authorized to use and disclose information for purposes of the operation of eth 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 protected information without written authorization of the client in the following circumstances:

1. TDH may use or disclose PHI without a client's 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 communication within TDH is permitted without client authorization, in compliance with **TDH HIPAA Policy #104**, *"Minimum Necessary Information."* However, disclosure of alcohol and drug 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. TDH clients may access their own PHI with certain limitations in compliance with **HIPAA Policy #102,** *"Clients' Privacy Rights."*

4. TDH may disclose information for purposes of payment, treatment, and health care operations without client authorization unless otherwise required by bureau/office policy.

5. 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 the Department 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;

      iii) Protect children from abuse and neglect, or

      iv) Conduct research when the bureau director gives prior written approval.

   b. TDH may not disclose the names, addresses, or other identifying information about the person who made the report.

6. If TDH has reasonable cause to believe that an adult is a victim of abuse or neglect, TDH may disclose PHI, as required by law, to a government 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 Staff, in the exercise of professional judgment and in consultation with an appropriate TDH supervisor, believes the disclosure in 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 protected information 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 staff make a disclosure permitted above, TDH must promptly inform the client that such a report has been or will be made, except if:

i) TDH staff, 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) TDH staff would be informing a personal representative and TDH staff 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 interests of the client, as determined by TDH staff, in the exercise of professional judgment and in consultation with the appropriate TDH supervisor.

7. 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.

8. TDH may disclose information 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. Unless prohibited or otherwise limited by federal or state law applicable to the program or activity requirements, TDH may disclose client information without authorization for judicial or administrative proceedings in which the TDH or State is a party, in response to an order of a court, a subpoena.

10. 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: TDH may report certain injuries or wounds; provide information to identify or locate a suspect, victim, or witness; alert law enforcement of a death if suspected it is as a result of criminal conduct; and provide information which in good faith constitutes evidence of criminal conduct on TDH premises.

11. TDH may disclose PHI without authorization for research purposes, as specified in **TDH HIPAA Policy #106**, *"Use and Disclosure for Research Purposes & Waivers."*

12. To avert a serious threat to health or safety, TDH may disclose client information without authorization if TDH believes in good faith that the information is necessary to prevent or lessen a serious and imminent threat to the health or 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.

13. TDH may disclose client information without authorization for other specialized government functions, including authorized federal officials conducting lawful intelligence, counterintelligence, and other national security activities that federal law authorizes.

14. TDH may disclose limited information 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.

15. In case of an emergency, TDH may disclose client information without authorization to the extent needed to provide emergency treatment.

16. The Family Educational Rights and Privacy Act (FERPA) and state law applicable to student records governs 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.

17. TDH may disclose information 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, trainees, learn under supervision to practice or improve their skills;

            - To the extent authorized under state law to defend TDH in a legal action or other proceeding brought by the client.

18. 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 purposes of this section.

19. When TDH is acting as a health oversight agency, TDH may use information for health oversight activities as permitted under this section.

20. TDH may use or disclose information without the written authorization of the client when TDH discloses information 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.

        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 staff should work with hearing officers to ensure that protective orders are used when appropriate in contested case hearings to prevent unauthorized uses and disclosures of information.

        ii) TDH staff will refer any questions or concerns regarding what is required by law, or by a court order, to the TDH Privacy Officer, who will then consult with the Office of General Counsel to resolve the question.

21. 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 information. TDH will identify confidentiality issues for discussion with the assigned legal counsel, in consultation with the TDH Privacy Officer, when deemed appropriate.

22. If TDH has obtained information in performing its duties as a health oversight agency, public health authority, nothing in this section supersedes TDH policies that otherwise permit or restrict uses or disclosures. For example, if TDH has obtained client patient information 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.

23. In any situation in which federal or state law prohibits or restricts the use or disclosure of information 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 HIPPA-authorized protective order may not be sufficient to authorize disclosure if it does not address other applicable confidentiality laws.

24. TDH may disclose information 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:
    1. Information on alcohol and drug treatment services can be disclosed only on the basis of a court order (42 CFR Part 2)
    2. 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.

25. TDH may disclose information 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.

26. TDH may disclose information to authorized federal officials for the protection of the President or of other persons authorized by applicable federal law.

Client's authorization that is <u>not required</u> if they are informed in advance and given the chance to object

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

For disclosure of health care information 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 protected information that directly relates to such person's involvement with the client's care or payment for such care.

B. TDH may use or disclose protected information 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 prior to, such a use or disclosure, TDH may disclose the protected information 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 in 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 of object.

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

Re-disclosure of a Client's Information:

A. Unless prohibited by state and federal laws, information held by TDH and authorized by the client for disclosure to a third party may be subject to re-disclosure by the third party. In such cases, the information is no longer protected by TDH or covered by its 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 can 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 information already released while the authorization was valid and in effect.

Verification of Client Requesting Information

PHI about a client may not be disclosed without verifying the identity of the person requesting the information in accordance with the appropriate Bureau or office policy and procedure, if the TDH staff 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, TDH shall deny any request for client information.

Prohibition of Use or Disclosure of Client's PHI

TDH shall not use or disclose any client's PHI for marketing purposes, except where communication describes a prescription drug or biologic and TDH cannot receive compensation for the communication. TDH shall not use or disclose any client's PHI for any fund-raising activities. TDH shall not disclose psychotherapy notes or any disclosure that involves the sale of Protected Health Information without prior authorization by patient.

Reference(s):

- 45 CFR 164.502(a)
- 45 CFR 164.508-164.512
- 42 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: **104**

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

PURPOSE:

This policy limits the amount of protected health information (PHI) that is used or disclosed by TDH workforce members to the minimum necessary and to ensure that TDH employees have access to the information they require to accomplish TDH mission, goals and objectives.

POLICY:

General:

A. TDH will use or disclose on 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 request by a health care provider for treatment;

2. Disclosures made to the client about his or her own protected information;

3. Uses or disclosures authorized by the client that are 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 that are 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

NOTE: Until guidance is published, by Secretary of HHS on what constitutes "minimum necessary" for use or disclosure of PHI, TDH must to the extent practicable, limit use, disclosure or request of PHI to the "limited data set" (Defined as PHI without names, addresses, telephone/fax, email, SSN, MRN and 9 other identifiers as outlined in TDH HIPAA Policy #107 *De-identification of Client Information and Use of Limited data Sets* under Requirements for De-Identification of Client Information Section B.), or if needed the minimum necessary to accomplish the intended purpose.

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 information to the minimum necessary needed to accomplish the intended purpose of the use, disclosure, or request.

B. If TDH policy permits making a particular disclosure to another entity, TDH employees may rely on a requested disclosure as being the minimum necessary for the stated purpose when:

1. Making disclosures to public officials that are permitted under 45 DFR 164.512, and as stated in **TDH HIPAA Policy #103**, *"Uses and Disclosures of Client or Participant Information,"* if the public official states that the information requests is the minimum necessary for the stated purpose(s). A "public official" is 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.

2. The information is requested by another entity that is a "covered entity" under the HIPAA privacy rules. A "covered entity" is a health plan, a health care provider who conducts electronic transactions, or a health care clearinghouse;

3. The information is requested by a professional who is a member of the workforce of TDH or is a business associate of TDH for the purpose of providing professional services to TDH, if the professional represent that the information 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 #106**, *"Use and Disclosure for Research Purposes & Waivers"* have been provided by a person requesting the information for research purposes.

Access & Uses of Information

A. TDH will make reasonable efforts to limit each workforce member's access to only the PHI that is needed to carry out his/her duties. These efforts will include internal staff to staff use and disclosure of PHI.

B. Each bureau/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, the employees will be informed. The determinations will be documented and shall include their accessibility to electronic, as well as, paper format for PHI.

Routine and Recurring Disclosure of a Client's Information

A. For routine and recurring disclosures (including disclosure in routine reports), TDH program areas will:

1. Determine who is requesting the information and the purpose for the request. If the request is **not** compatible with the purpose for which it was collected, refer to and apply the "non-routine use" procedures in the following section.

2. Confirm that the applicable TDH polices 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 kind and amount of information that is necessary to respond to the request; and

4. If the disclosure is one that must be included in the TDH accounting of disclosures, include required documentation required by the appropriate bureau or office.

B. For the purposes of this policy, "routine and recurring" means the disclosure of records outside TDH, without the authorization of the client, for a purpose that is compatible with the reason for which the information was collected. The following identifies several examples of uses and disclosures that TDH has determined to be compatible with the purposes for which information 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. For example, a mandatory child abuse report by a TDH employee would be a routine use.

3. When federal or state agencies – such as DHHS Office for Civil Rights, the DHHS 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 records necessary to carry out audit, or oversight of TDH programs or activities, TDH will make such records available as a routine and recurring use.

4. When the appropriate TDH official determines that records are subject to disclosure under Tennessee law, TDH may make the disclosure as routine and recurring use.

Non-routine Disclosure of a Client's Information

A. For the purpose of this policy, "non-routine disclosure" means the disclosure of records outside TDH (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 medial record is needed, and applicable laws and policies permit the disclosure of all the information in the medical record to the requestor.

C. Requests for non-routine disclosures must be reviewed on an individual basis to limit the information 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 information about a client from another entity, TDH employees must limit requests to those that are reasonable 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 needed.

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: **105**

Effective Date: **March 26, 2013**

PURPOSE:

The intent of this policy is to establish criteria for safeguarding protected health information (PHI) and to minimize the risk of unauthorized access, use or disclosure.

POLICY:

General:

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

Information to be safeguarded may be in any medium, including paper, electronic, verbal, and visual representations of PHI.

Safeguarding PHI Information – TDH Workplace Practices

A. Paper:

1. TDH staff must make reasonable efforts to ensure the safeguarding of PHI including the use of locked storage wherever available, and ensuring the safeguarding of PHI.

2. Each TDH workplace will ensure that the disposal of files and documents is performed on a timely basis, consistent with record retention requirements and are 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 employee 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 would include PHI on desk tops, computer screens, fax machines, photocopy machines, printers, management reports or other paper documents in accordance with the appropriate bureau of office policy and procedure.

Safeguarding PHI – TDH Administrative Safeguards

A. A determination of who should have access to the specific data will be established in each bureau and office and program area.

1. TDH managers and supervisors will determine the role of each of their staff members and request exceptions based on the needs of their office.

2. Managers are responsible for allowing access to enough information for their staff to do their jobs while holding to the minimum necessary standard.

B. TDH managers and supervisors will:

1. Safeguard confidential information:

2. Conduct a thorough assessment of each category of responsibilities and/or individual employee;

3. Foster a more secure atmosphere and enhance the belief that confidential information is important and that protecting privacy is key to achieving TDH goals.

4. Managers will update the safeguards in place each year, seeking to achieve reasonable administrative, technical and physical safeguards.

C. Utilize the security policies when they are developed to augment safeguard procedures.

D. TDH staff will be required to sign a "confidentiality statement" that constitutes a formal commitment to adhere to the department-wide privacy and security policies concerning the PHI.

Reference(s):

Contacts(s):

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

Tennessee Department of Health

HIPAA Policies

Privacy

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

Policy Number: **106**

Effective Date: **March 26, 2013**

PURPOSE:

The intent of this policy is to specify when TDH may use or disclose protected health information (PHI) about client's for research purposes.

POLICY:

General:

When TDH uses or discloses a client's PHI for research purposes, they must consider the following:

A. TDH may use or disclose a client's information for research purposes as specified in this policy. "Research" means "a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalized knowledge."

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 #107**, *"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 sets in **TDH HIPAA Policy #107**, *"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 may use an IRB established in accordance with 45 CFR Part 46 or a privacy board that has been established by TDH pursuant to this policy, 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 information for research purposes with the client's specific written authorization.

1. Such authorization must meet all the requirements described in **TDH HIPAA Policy #103,** *"Uses and Disclosures of Client Information."* and 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 provided that:

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 that:

      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. Documentation required of IRB or privacy board when granting approval of a waiver of an client's authorization for release of PHI must include:

a. A statement identifying the IRB or privacy board that approved the waiver of an 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 an 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; and

- The research could not practicable 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 an 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 164.512(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 use 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; the client PHI for which use or access is sought is necessary for the research purposes

   c. Researcher and his or her agents 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;

   d. Researcher and his or her agents agree not to publicly identify the information or contact the client whose data is being disclosed; and

   e. 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 about clients who are deceased. TDH should determine whether federal or state law otherwise permits such use or disclosure of information about decedents without client authorization or use of an IRB. There may be instances where it would be inappropriate to disclose information, even where the client subject of the information 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 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 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; and

c. Representation that the client's PHI for which use or disclosure is sought is necessary for the research purposes.

d. Researcher and his or her agents 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 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 is operating 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 rules. 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 the **TDH HIPAA Policy #107**, *"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.

Reference(s):

- 45 CFR Part 64
- 45 CFR 164.512

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: **107**

Effective Date: **March 26, 2013**

PURPOSE:

The intent of this policy is to prescribe standards under which client protected health information (PHI) can be used and disclosed without authorization or tracking of disclosures when all information that could identify a person 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 be 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 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.

D. TDH may disclose a limited data set for the purposes of research, public health or health care operation. However, unless TDH has obtained a limited data set that is subject to a data use agreement, TDH is not restricted to using a limited data set for its own activities or operations.

E. 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 and individual, only if ***either*** 1 or 2 below have occurred:

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; ***or***

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 age 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;

f. 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. The TDH Privacy Officer will designate the statistician or other person referred to above, who may be either:

1. A TDH employee;

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 set 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 that 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 that 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: **108**

Effective Date: **March 26, 2013**

PURPOSE:

The purpose of this policy is to specify when TDH may disclose a client's protected health information (PHI) to a business associate of TDH, and to specify provisions that must be included in TDH contracts with business associates.

POLICY:

General

A. TDH has many contractual and business relationships, and TDH has a policy related to its contracts and business relationships. However, not all contractors or business partners are "business associates" of TDH. This policy only applies to contractors or business partners that come within the definition of "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 Health and Human Services (HHS) for any breaches which occur on their behalf.

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 individually identifiable health information, 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 employee, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for TDH, where the provisions of the service involves the disclosure of individually identifiable health information from TDH, or from another business associate of TDH, 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. **EXCEPTION;** A researcher is not automatically a business associate despite the fact that they may be using the covered entity's Protected Health Information.

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; and

7. When the only information being disclosed is information that is de-identified in accordance with **TDH HIPAA Policy #107**, *"De-identification of Client or Participant Information and Use of Limited Data Sets."*

8. Persons or organizations (e.g., janitorial services) whose duties do not involve or 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 the information 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 client' rights regarding PHI;

   f. Make its internal practices, books, and records relating to the use and disclosure of PHI available to TDH and to the United States DHHS 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 information.

3. Authorize 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, rather than a contract, with the business associate if the memorandum of understanding contains terms covering all objectives of the contract requirements outlined in this policy;

2. The written contract, agreement, or memorandum 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 protected health information 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 health information 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 information is disclosed that:

i) It will be held or disclosed further only as require by law or for the purposes 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 information has been breached.

Responsibilities of TDH in Business Associate Relationships

A. TDH responsibilities in business associate relationships include, but are not limed 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 the United States DHHS.

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: **109**

Effective Date: **March 26, 2013**

PURPOSE:

The intent of this policy is to specify enforcement, sanction, penalty, and disciplinary actions that may result from violation of TDH policies regarding the privacy and protection of an individual's information and to offer guidelines on how to conform to 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 or provider's information.

   1. TDH employees, volunteers, interns and members of the TDH workforce who are uncertain if a disclosure is permitted are advised to consult with a supervisor in the TDH workplace. The Department Privacy Officer may be consulted on any disclosure question.

B. All employees are required to be aware of their responsibilities under TDH privacy policies and will be expected to sign a "Confidentiality Statement" (Form-3131) indicating that they have been informed of the business practices in TDH as it relates to privacy, and they understand their responsibilities to ensure the privacy of TDH clients and participants.

C. Supervisors are responsible for assuring that employees who have access to protected health information (PHI), whether it be electronic, hard copy, or verbally, are informed of their responsibilities.

D. TDH employees who violate TDH policies and procedures regarding the safeguarding of an individual's information are subject to appropriate disciplinary action by TDH up to and including immediate dismissal from employment, and/or

legal action by the individual, who may want to pursue a tort claim against the State of Tennessee or a lawsuit against the state and the employee.

E. TDH employees who knowingly and willfully violate state or federal law for improper use or disclosure of an individual's information are subject to criminal investigation and prosecution or civil monetary penalties and may be enforced by the federal Department of Health and Human Services.

F. If TDH, as a state agency, **fails to enforce privacy safeguards TDH may be subject to administrative penalties by the Department of Health and Human Services (DHHS), including federal funding penalties.**

Retaliation Prohibited

Neither TDH as an entity, nor any TDH employee 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, or for participating in any process established under TDH policy, including filing a complaint with TDH or DHHS.

2. Any individual or other person for:

   a. Filing a complaint with TDH or with DHHS as provided in TDH privacy policies;

   b. Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing relating to TDH policy and procedures; or

   c. Opposing any unlawful act or practice, provided that:

      i. The individual or other person (including a TDH employee) 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 protected information in violation of TDH policy.

Disclosures by Whistleblowers and Workforce Crime Victims

A. A TDH employee may disclose limited PHI about an individual to a law enforcement official 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, date 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 staff, 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 failure 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):

- 45CFR 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: **110**

Effective Date: **March 26, 2013**

PURPOSE:

The purpose of this policy is to specify the extent that mitigation must take place.

POLICY:

General:

TDH has the duty to mitigate "to the extent practicable," any harmful effects due to uses or disclosures of protected health information (PHI) in violation of the regulations 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. Bureaus/offices are required to take "reasonable steps" to reduce harmful effects of those actions about which they are aware.

Bureaus/offices are obligated to undertake reasonable close monitoring of the activities of members of their workforce. When unauthorized use or disclosures of PHI take place, precautions should be put in place to ensure that similar disclosures do not occur in the future. If the disclosure is made by TDH workforce, appropriate action should take place immediately.

The Department Privacy Officer shall be notified immediately when unauthorized uses or disclosures take place either internally or externally to determine if mitigation efforts should be undertaken.

Reference(s):

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: **111**

Effective Date: **March 26, 2013**

PURPOSE:

The intent of this policy is to establish criteria for issuing a notification in the case of a breach of unsecured protected health information (PHI).

POLICY:

General:

TDH must notify clients promptly if their unsecured PHI has been or is reasonably believed to have been breached. A breach is defined as "the acquisition, access, use, or disclosure" of PHI in a manner that violates the HIPAA Rules and also "compromises the security or privacy of the PHI."

"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."

A breach is the impermissible use or disclosure of Protected Health Information (i.e. a violation of the HIPAA Privacy Rule) and is presumed to be a breach UNLESS the Covered Entity or Business Associate, as applicable, demonstrates that there is a low probability that the Protected Health Information has been compromised.

The TDH shall perform a Risk Assessment to determine if Notification is required. Therefore, breach notification; which results from a reportable breach determination, is NOT required if TDH demonstrates through the Risk Assessment that there is a low probability that the Protected Health Information has been compromised.

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

1. The nature and extent of the Protected Health Information involved, including types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the Protected Health Information or to

whom the Protected Health Information was disclosed;
3. Whether the Protected Health Information was actually acquired or viewed; and
4. The extent to which the risk to the Protected Health Information has been mitigated.

Nothing prevents TDH from providing notification for each breach without performing the Risk Assessment. The Risk Assessment analysis is only required if TDH, based on the facts, wants to demonstrate that no notification is required.

TDH has the burden of proof, pursuant to 45 CFR 164.414, 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 under 45 CFR 164.404.

Breach Exceptions

Exceptions to the definition of a breach are:

1. Any unintentional access or use of PHI by a workforce member of TDH or person acting under TDH authority, is such access 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 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

The staff/workforce members must immediately in form the TDH Privacy Officer upon becoming aware or informed of a breach. The TDH Privacy Officer upon learning of such will no later than seven (7) days commence investigation of the reported breach.

Breach Response Team

A TDH Breach Response Team will be established by TDH for the purpose of receiving and reviewing the findings as a result of the Risk Assessment determination conducted by the Privacy Officer and Security Officer and advise what further action; if any.

The Breach Response Team shall be made up of a representative from the TDH Office of Human Resources, the TDH 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 breach 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 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 breach.

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 that occurred with respect to the breach, 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 disclosed during the breach;

3. A description of the steps the individual should take in order to protect himself or herself from potential harm caused by the breach;

4. A description of the what TDH is doing to investigate and mitigate the breach and to prevent future breaches; and

5. Instructions for the individual to contact the TDH.

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

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. The TDH must also notify the Secretary of HHS of any breach involving 500 or more people. Notification to the media and the Secretary must be made within 60 days of the discovery of the breach. The Privacy Officer will notify the Secretary. The notification to the media outlet will be handled through the TDH's Communications Office in conjunction with the Privacy

Officer. The Privacy Officer shall provide a copy of the log of all breaches to the Secretary within 60 days after the end of each calendar year.

Training Employees

TDH Privacy Officer must ensure that all current and new employees, including management are trained on this new policy within a reasonable period of time after the policy becomes effective.

Reference(s):

- 45 CFR 160 & 164, Subpart D

Contact(s):

- Privacy Program Office, (615) 741-1969
- Security Officer, (615) 741-0899
- TDH HIPAA Hotline, (877) 280-0054

Tennessee Department of Health

HIPAA Policies

Standard Transactions, Code Sets, and Identifiers

Policy Title: **Administrative Requirements for the Implementation of HIPAA Transactions, Code Sets, and Identifiers**

Policy Number: **201**

Effective Date: **March 26, 2013**

PURPOSE:

These policies govern the conduct of all HIPAA Electronic Data Interchange (EDI) Transactions with the Department of Health (TDH).

These policies also set forth TDH EDI Transaction requirements for purposes of the Health Insurance Portability and Accountability Act of 1996, 42 USC 1320d – 1320d-8, Public Law 104-191, sec. 262 and sec. 264, (HIPAA) and the implementing HIPAA Transaction Rule. The HIPAA Transaction Rule permits the use of a Trading Partner Agreement (TPA) to establish the parameters under which Covered Entities conduct Electronic Data Interchange (EDI) Transactions. Where a federal HIPAA Standard has been adopted for an EDI Transaction, this rule should be construed to implement and not to alter the requirements of the HIPAA Transaction Rules.

These policies do not mandate that individuals or agencies convert to EDI Transactions with TDH. Providers or Agencies who bill the TDH for services may continue to submit paper claims to the TDH.

Definitions:

For purposes of these policies, the following terms shall have the meanings set forth below. Capitalized items used in these Standard Transactions, Code Sets and Identifies Policies have the same meaning as those terms are defined in this section.

1. ***Access:*** The ability or the means necessary to read, write, modify or communicate Data or information or otherwise use and Information System resource.

2. ***Agent:*** Third parties or organizations that contract with a Trading Partner to perform designated services in order to facilitate a Transaction, or the conduct of other business functions, on behalf of the Trading Partner.

a. Examples of Agents include billing agents, including but not limited to the following: claims clearinghouses, vendors, claims value added networks, billing services, service bureaus, and accounts receivable management firms.

b. Agents may also include clinics, group practices and facilities, including the following: an employer of a Provider, if the Provider is required as a condition of employment to turn over his fees to the employer; the facility in which the service is provided, if the Provider has a contract under which the facility submits the claim; or a foundation, plan, or similar organization operating an organized health care delivery system, if the Provider has a contract under which the organization submits the claim.

c. Agents may also include EDI Submitters as that term is defined in these TDH EDI policies.

3. ***ANSI:*** American National Standards Institute.

4. ***Authentication:*** The verification of the identity of a person or process. In a communication system, authentication verifies that the messages really come from their stated source, like the signature on a (paper) letter.

5. ***Centers for Medicare and Medicaid Services (CMS):*** CMS is the federal agency charged with the administration of the Medicare and Medicaid programs within the U.S. Department of Health and Human Services and also charged with implementation of the HIPAA Transaction Rule.

6. ***Implementation Guide:*** TDH's business-specific instructions describing the Transaction-specific information necessary to submit a Data Transmission and have it be successfully processed.

7. ***Confidential Information:*** Information relating to Covered Individuals (as defined herein) which is exchanged by and between TDH, the Provider and/or Agents for various business purposes, but which is protected from disclosure to unauthorized persons or entities by applicable state and federal statutes, or the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 and its implementing regulations, which statutes and regulations shall hereinafter be collectively referred to as "Privacy Statutes and Regulations."

8. ***Contract:*** A specific written agreement between TDH and a Provider or Agency that provides, or manages the provision of, services, goods or supplies to Covered Individuals and in the provision of which TDH and the Provider or Agency may exchange Data (as defined herein).

9. ***Covered Individuals:*** Individual persons who are eligible for payment of certain services or supplies provided to them or their eligible dependents by or through a Provider or Agency (as defined herein) under the terms, conditions, limitations and

exclusions of a Contract applicable to a governmental program or a Letter of Agreement and for which TDH processes or administers Data Transmissions.

10. ***Data:*** A formalized representation of specific facts or concepts, suitable for communication, interpretation, or processing by people, or by automatic means.

11. ***Data Transmission:*** The transfer or exchange of Data between TDH and an EDI Submitter by means of an Information System (as defined herein) which is compatible for that purpose, and including without limitation, EDI, ERA, or EMC (all as defined herein) transmissions, pursuant to the terms and conditions set forth in a Trading Partner Agreement and these rules.

12. ***Department of Health (TDH):*** The Tennessee Department of Health or any of its divisions, programs or offices, including TDH Information Systems.

13. HIPAA ***Electronic Data Interchange (EDI):*** The exchange of business documents from application to application in a federally mandated format or (if no federal Standard has been promulgated) such other format as TDH shall designate.

14. ***EDI Submitter:*** A person or entity authorized to establish the Electronic Media connection with TDH to conduct an EDI Transaction. An EDI Submitter may be the Trading Partner, or may be an Agent of the Trading Partner.

15. ***Electronic Media:*** (1) Electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or (2) Transmission media used to exchange information already in electronic storage media. Transmission media includes, for example, the internet (wide-open), extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmission via electronic media, because the information being exchanged did not exist in electronic form before the transmission.

16. ***Electronic Media Claims (EMC):*** An Electronic Media means of submitting claims or encounters for or in relation to payment of services or supplies provided by a Provider or Agency (as defined herein) to a Covered Individual.

17. ***Electronic Remittance Advice (ERA):*** A document or electronic file containing information pertaining to the disposition of a specific claim for payment of services or supplies rendered to Covered Individuals (as defined herein) which are filed with TDH on behalf of the Covered Individual by Providers or Agencies (as defined herein). The documents include, without limitation, information such as the Provider name and address, individual name, date of service, amount billed,

amount paid, whether the claim was approved or denied, and if denied, the specific reason for the denial.

18. ***Encryption:*** A process for enciphering or encoding data to prevent illicit entry into a system.

19. ***Envelope:*** A control structure in a mutually agreed format for the electronic interchange of one or more encoded Data Transmissions either sent or received by the EDI Submitter or TDH.

20. ***HIPAA Transaction Rule:*** The Standards for Electronic Transactions at 45 CFR Part 160 and 162 (2003) adopted by the U.S. Department of Health and Human Services to implement the Health Insurance Portability and Accountability Act of 1996, 42 USC 1320d et. seq.

21. ***Information System:*** An interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications and trained personnel necessary for the successful Data Transmission.

22. ***Letter of Agreement:*** A specific written agreement between TDH and a Provider of Agency that provides, or manages the provision of, services, goods or supplies to Covered Individuals and in the provision of which TDH and the Provider or Agency may exchange Data (as defined herein).

23. ***Lost or Indecipherable Transmission:*** A Data Transmission which is never received by or cannot be processed to completion by the receiving Party in the format or composition received because it is garbled or incomplete, regardless of how or why the message was rendered garbled or incomplete.

24. ***Protected Health Information (PHI):*** Individually identifiable information relating to past, present or future physical or mental health or condition of an individual, provision of health care to an individual, or the past, present or future payment for health care provided to an individual.

25. ***Provider:*** An individual, facility, institution, corporate entity, or other organization which supplies or provides for the supply of services, goods or supplies to Covered Individuals pursuant to a Contract or Letter of Agreement with TDH.

26. ***Registered Transaction:*** Each type of Transaction (e.g., claims submission, eligibility inquiry, etc.) applicable to a Trading Partner must be registered with TDH before it can be tested or approved for transmission. Registration is initiated with an EDI Request Form.

27. ***Security Access Codes:*** Those alpha-numeric codes assigned to the EDI Submitter by TDH for the purpose of allowing access to TDH's Information System for the purpose of successfully executing Data Transmissions or otherwise carrying out the express terms of a Trading Partner Agreement and these policies.

28. ***Source Documentation:*** Documents or electronic files containing underlying Data which is or may be required as part of a Data Transmission with respect to a claim for payment of charges for medical services rendered or supplies provided to a Covered Individual, or with respect to any other Transaction. Examples of Data contained within a specific Source Document may include, without limitation, the following: Individual's name and identification number, claim number, diagnosis code for the services rendered, dates of service, service procedure description, applicable charges for the services rendered, the Provider's, or Agency's name and/or identification number and signature.

29. ***Standard:*** A rule, condition or requirement describing the following information for products, systems or practices: (a) classification of components; (b) specification of materials, performance, or operations; or (c) delineation of procedures.

30. ***Standard Transaction:*** A Transaction that complies with the applicable Standard adopted by the U.S. Department of Health and Human Services (DHHS) to implement the HIPAA Transaction Rules.

31. ***Transaction:*** The exchange of Data between TDH and its Trading Partner using Electronic Media to carry out financial or administrative activities.

32. ***Trading Partner:*** A Provider or Agency (as defined herein) that has entered into a Trading Partner Agreement with TDH in order to satisfy all or part of its obligations under a Contract or Letter of Agreement by means of EDI. ERA and/or EMC or any other mutually agreed means of electronic exchange or transfer of Data as provided for herein.

33. ***Trading Partner Agreement (TPA):*** A specific written agreement between TDH and a Provider or Agency that governs the terms and conditions for EDI Transactions in the performance of obligations under a Contract or Letter of Agreement. A Provider or Agency that has executed a TPA will be referred to herein as a Trading Partner in relation to those functions.

POLICY:

General:

1. No person or entity shall be registered to conduct an EDI Transaction with TDH except as authorized under these EDI TDH policies. Eligibility and continued participation as a Trading Partner or EDI Submitter in the conduct of Registered

Transactions is conditioned on 1) the execution and delivery of the documents required in these TDH EDI policies, 2) the continued accuracy and consistency of that information, and 3) compliance with the requirements of these TDH EDI policies. The information disclosed by Trading Partner or any EDI Submitter may be subject to verification. Data, including Confidential Information, governed by these TDH EDI Policies may be used for purposes related to treatment, payment and health care operations and for the administration of programs or services by TDH.

2. In addition to the requirements of subsection (1) of this Policy, in order to qualify as a Trading Partner:

   a. A person or entity must be a TDH Provider or Agency pursuant to a current valid Contract or Letter of Agreement; and

   b. The Provider or Agency must have submitted an executed TPA and all related documentation, including "EDI Submitter", Exhibit I of the TPA which identifies and authorizes the EDI Submitter.

3. In addition to the requirements of subsection (1) of this Policy, in order to qualify as an EDI Submitter:

   a. A Trading Partner must have identified the person or entity as an authorized EDI Submitter "EDI Submitter", Exhibit I of the TPA.

   b. If the Trading Partner identifies itself as the EDI Submitter, the "EDI Submitter", Exhibit I of the TPA must include the information required in the "Trading Partner Authorization of EDI Submitter" and the "EDI Submitter Information."

   c. If the Trading Partner uses an Agent as the EDI Submitter, the "EDI Submitter", Exhibit I of the TPA must include the information described in subsection (b) of this section and the signed EDI Submitter Certification.

4. The EDI Registration process described in these DPH EDI policies provides TDH with the essential profile information that may be used by TDH to confirm that the Trading Partner or EDI Submitter is not otherwise excluded or disqualified from submitting EDI Transactions to TDH.

5. Nothing in these policies or a TPA prevents TDH from requesting additional information from a Trading Partner or EDI Submitter to determine their qualifications or eligibility for registration as a Trading Partner or EDI Submitter.

6. TDH shall deny a request for registration as a Trading Partner Agreement or for authorization of an EDI Submitter or an EDI Registration if it finds any of the following:

a. The Trading Partner or EDI Submitter has substantially failed to comply with the applicable administrative rules or laws; or

b. The Trading Partner or EDI Submitter has been convicted (or entered a plea of nolo contendere) of a felony or misdemeanor related to a crime or violation of federal or state public assistance laws or Privacy Statutes or Regulations (as defined in these rules);

c. The Trading Partner or EDI Submitter is excluded from participation in the Medicare program, as determined by the Secretary of Health and Human Services; or

d. The Trading Partner or EDI Submitter fails to meet the qualifications as a Trading Partner or EDI Submitter.

7. Standard Transactions to be used between TDH and Trading Partners and/or EDI Submitters are as follows:

   a. 837 – P Professional
   b. 837 – I Institutional
   c. 837 – D Dental
   d. NCPDP Batch Standard Version 1.1
   e. 276 Claim Status Request
   f. 276 Claim Status Response
   g. 835 Claims Remittance Advice

8. Only HIPAA standard code sets will be used between TDH and the Trading Partners and/or EDI Submitters. The HIPAA standard code sets are:

   a. Health Care Financing Administration Common Procedural Coding System
   b. National Drug Code
   c. National Council for Prescription Drug Program
   d. International Classification of Diseases (ICD-9)
   e. American Dental Association Current Dental Technology (CDT-4)
   f. Diagnosis Related Group Number

Reference(s):

-

Contact(s):

- Privacy Program Office, (615) 741-1969
- Security Officer, (615) 741-0899
- TDH HIPAA Hotline, (877) 280-0054

Tennessee Department of Health

HIPAA Policies

Standard Transactions, Code Sets, and Identifiers

Policy Title: **Registration Process**

Policy Number: **202**

Effective Date: **March 26, 2013**

PURPOSE:

The purpose of these policies is to establish a registration process and requirements applicable to individuals or entities that desire to be treated as Trading Partners or EDI Submitters with the Department of Health (TDH).

POLICY:

General:

1. EDI Registration is an administrative process governed by these EDI Transaction policies. The EDI Registration process is initiated by the submission of a Trading Partner Registration Agreement (TPA) by a Provider or Agency, including all requirements and documentation required by TDH EDI policies.

2. Trading Partners must be TDH Providers with a current TDH contract under the Authorization to Contract provision of the State of Tennessee or have a Letter of Agreement with one of the programs within the Bureau of Health Services Administration. TDH will accept a TPA only from those individuals or entities who are Providers or Agencies that have a current contract or Letter of Agreement with TDH.

3. Trading Partner Agreement. In order to register as a Trading Partner with TDH, a Provider or Agency must submit a signed TPA to TDH. Signing the TPA constitutes agreement by the Provider or Agency to comply with all TDH EDI policies, and other TDH, state and federal laws and regulations applicable to the application for and conduct of EDI Transactions with TDH, and further constitutes Provider's or Agency's agreement to ensure compliance by its Agents with such laws, rules, policies and procedures.

4. In addition to the requirements in subsection 3. of this policy, a Trading Partner must submit an all three Exhibits (EDI Submitter – Exhibit I, TDH EDI Request Form, Exhibit II, Computer Access Agreement for TDH, Exhibit III) to the completely filled out and signed to the TDH. The EDI Submitter, Exhibit I, provides specific identification of and legal authorization from the Trading Partner for the EDI Submitter

to conduct EDI Transactions on behalf of the Trading Partner. The TDH EDI Request Form, Exhibit II, specifies the primary method of submission, the Encryption Tool the Trading Partner will use for EDI and the transactions to Trading Partner will use. The Computer Access Agreement, Exhibit III, outlines the guidelines for computer access with TDH.

5. Trading Partner Agents. A Trading Partner may use Agents in order to facilitate the electronic transmission of Data. If Trading Partner will be using an Agent as the EDI Submitter, the EDI Submitter, Exhibit I, required under subsection 4. of this policy shall identify and authorize the EDI Submitter and shall include the EDI Certification signed by the EDI Submitter before TDH may accept an electronic submission form, or send an electronic transmission to, such EDI Submitter. Submitting the EDI Submitter, Exhibit I, is not a guarantee that the ECI Submitter has been accepted by TDH to conduct EDI transactions.

6. Review and Acceptance Process. TDH shall review the documentation provided to determine compliance with sections 1. through 5. of this policy. Submission of such information is not a guarantee that a TPA or an authorization of an EDI Submitter has been accepted by TDH. The information provided may be subject to verification by TDH. When TDH determines that the information complies with these EDI policies, TDH will notify the Trading Partner.

Reference(s):

-

Contact(s):

- Privacy Program Office, (615) 741-1969
- Security Officer, (615) 741-0899
- TDH HIPAA Hotline, (877) 280-0054

Tennessee Department of Health

HIPAA Policies

Standard Transactions, Code Sets, and Identifiers

Policy Title: **Trading Partner as EDI Submitter**

Policy Number: **203**

Effective Date: **March 26, 2013**

PURPOSE:

The purpose of this policy is to specify the registration requirements for a Trading Partner who qualifies as the EDI Submitter.

POLICY:

General:

1. Trading Partner may be EDI Submitter. Any registered Trading Partner, that also qualifies as an EDI Submitter, may submit his or her own EDI transactions directly to TDH. The Trading Partner will be referred to as the EDI Submitter when functioning in that capacity, and shall be required to comply with all terms and conditions of these policies applicable to an EDI Submitter, except as expressly provided in subsection 3. of this policy.

2. Prior to acting as an EDI Submitter, the Trading Partner shall designate in the "EDI Submitter", Exhibit I, of the Trading Partner Agreement (TPA) that Trading Partner is the EDI Submitter who is authorized to send and/or receive Data Transmissions in the performance of EDI transactions. Trading Partner must complete the TPA and all three of the exhibits: "EDI Submitter", Exhibit I, "TDH EDI Request Form", Exhibit II, and "Computer Access Security Agreement", Exhibit III. The Trading Partner shall notify TDH of any material changes in the information no less than five (5) days prior to the effective date of such changes.

3. EDI Submitter Certification Conditions Not Required. Where Trading Partner is acting as its own EDI Submitter, Trading Partner is not required to submit the EDI Submitter Certification Conditions in the "EDI Submitter", Exhibit I of the TPA.

Reference(s):

•

Contact(s):

- Privacy Program Office, (615) 741-1969
- Security Officer, (615) 741-0899
- TDH HIPAA Hotline, (877) 280-0054

Tennessee Department of Health

HIPAA Policies

Standard Transactions, Code Sets, and Identifiers

Policy Title: **Trading Partner Agents as EDI Submitters**

Policy Number: **204**

Effective Date: **March 26, 2013**

PURPOSE:

The purpose of this policy is to specify the registration requirements for a Trading Partner who authorizes their Agent as their EDI Submitter.

POLICY:

General:

1. Responsibility for Agents. If the Trading Partner uses the services of an Agent, including but not limited to an EDI Submitter, in any capacity in order to receive, transmit, store or otherwise process Data or Data Transmissions or perform related activities; the Trading Partner shall be fully responsible to TDH for any acts, failures or omissions of the Agent in providing said services, as though the acts, failures or omissions, were the Trading Partner's own.

2. Notices Regarding EDI Submitter. Prior to the commencement of an EDI Submitter's services, the Trading Partner shall designate in the "EDI Submitter", Exhibit I, of the Trading Partner Agreement (TPA), its specific EDI Submitter(s) that are authorized to send and/or receive Data Transmission in the performance of EDI Transactions for the Trading Partner. Trading Partner must complete the TPA and all three of the Exhibits: "EDI Submitter", Exhibit I, "TDH EDI Request Form", Exhibit II, and "Computer Access Security Agreement", Exhibit III, required fields. The Trading Partner or authorized EDI Submitter shall notify TDH of any material changes in EDI Submitter authorization or information no less than five (5) days prior to the effective date of such changes.

3. Authority of EDI Submitter. A Trading Partner shall authorize the actions that an EDI Submitter may take on behalf of Trading Partner. The "EDI Submitter", Exhibit I, permits the Trading Partner to authorize which decisions may be made only by the Trading Partner and which decisions are authorized to be made by the EDI Submitter. The EDI Submitter information authorized in the "EDI Submitter", Exhibit I of the TPA will be recorded by TDH in an EDI Submitter Profile. TDH

may reject EDI Transactions from an EDI Submitter acting without authorization form the Trading Partner.

4. EDI Submitter Certification Conditions. Each authorized EDI Submitter acting as an Agent of a Trading Partner shall execute and shall comply with the EDI Submitter Certification Conditions that are incorporated into the "EDI Submitter", Exhibit I of the TPA. Failure to include the signed EDI Submitter Certification Conditions with the TPA shall result in a denial of EDI Submitter authorization by TDH. Failure of an EDI Submitter to comply with the EDI Submitter Certification Conditions may result in termination of EDI Submitter registration for EDI Transactions with TDH.

5. Responsibilities Regarding EDI Submitters. In addition to the requirements of section 1. of this policy, the Trading Partner is responsible for ensuring that the EDI Submitter will make no unauthorized changes in the Data content of any and all Data Transmissions or the contents of an Envelope, and further that such EDI Submitter will take all appropriate measures to maintain the timeliness, accuracy, truthfulness, confidentiality, security, and completeness of each Data Transmission. Furthermore, the Trading Partner further is responsible for ensuring that its EDI Submitter(s) are specifically advised of, and will comply in all respects with, the terms of these policies and any TPA.

Reference(s):

-

Contact(s):

- Privacy Program Office, (615) 741-1969
- Security Officer, (615) 741-0899
- TDH HIPAA Hotline, (877) 280-0054

Tennessee Department of Health

HIPAA Policies

Standard Transactions, Code Sets, and Identifiers

Policy Title: **Testing**

Policy Number: **205**

Effective Date: **March 26, 2013**

PURPOSE:

This policy outlines the requirement of testing before TDH shall authorize a Transaction for a Trading Partner or an authorized EDI Submitter.

POLICY:

General:

1. When a Trading Partner or authorized EDI Submitter registers an EDI Transaction with TDH, TDH will require testing before authorizing the Transaction. An EDI Submitter must be able to demonstrate its capacity to send and/or receive each Transaction type for which it has registered. TDH will reject any EDI Transaction if the EDI Submitter either refuses or fails to comply with TDH testing requirements.

2. After successfully demonstrating the ability to sustain compliant testing and obtaining required documentation of successful completion of testing requirements for a specific Transaction type to TDH satisfaction, TDH may initiate business-to-business testing for that Transaction type.

3. Testing will be conducted using secure Electronic Media communications methods.

4. The EDI Submitter may be required to re-test with TDH if TDH format changes or if the EDI Submitter format changes.

Reference(s):

-

Contact(s):

- Privacy Program Office, (615) 741-1969
- Security Officer, (615) 741-0899
- TDH HIPAA Hotline, (877) 280-0054

Tennessee Department of Health

HIPAA Policies

Standard Transactions, Code Sets, and Identifiers

Policy Title: **Conduct of Transactions**

Policy Number: **206**

Effective Date: **March 26, 2013**

PURPOSE:

This policy addresses the obligations of the TDH and the EDI Submitter for the conduct of the EDI Transactions between the two entities.

POLICY:

General:

1. EDI Submitter Obligations. In addition to the obligations of the Trading Partner and/or Agent(s) set forth elsewhere in these policies, the EDI Submitter is responsible for the conduct of the EDI Transactions registered on behalf of the Trading Partner, including the following:

   a. Accuracy of EDI Transmission. The EDI Submitter shall take responsible care to ensure that Data and Data Transmissions are timely, complete, accurate, and secure. The EDI Submitter shall take reasonable precautions to prevent unauthorized access to the Information System, the Data Transmission itself or the contents of an Envelope which is transmitted either to or from TDH pursuant to these rules. TDH will not correct or modify an incorrect Transaction prior to processing; such Transactions may be rejected and the EDI Submitter will be notified of the rejection.

   b. Re-transmission of Indecipherable Transmissions. Where there is evidence that a Data Transmission is Lost or Indecipherable Transmission, the sending party shall make best efforts to trace and re-transmit the original Data Transmission in a manner which allows it to be processed by the receiving party as soon as practicable.

   c. Cost of Equipment. EDI Submitter and TDH shall bear their own Information System costs. EDI Submitter shall, at its own expense, obtain and maintain its own Information System. Furthermore, EDI Submitter shall pay its own costs for any and all charges related to Data Transmission under these TDH EDI policies. These charges could include without limitation, charges for

Information System equipment, software and services, charges for maintaining an electronic mailbox, connect time, terminals, connections, telephones, modems, and any applicable minimum use charges, and for translating, formatting, or sending and receiving communications over the electronic network to the electronic mailbox, if any, of TDH. TDH is not responsible for providing technical assistance in the processing of an EDI Transaction.

d. Back-up Files. EDI Submitter shall maintain adequate Data archives and back-up files other means sufficient to re-create a Data Transmission in the event that such re-creation becomes necessary for any purpose at any time. Such Data archives or back-up files shall be subject to the terms of these TDH EDI policies to the same extent as the original Data Transmission.

e. Format of Transmissions. Except as otherwise provided herein, the EDI Submitter shall send and receive all Data Transmission in the federally mandated format, or (if no federal Standard has been promulgated) such other format as TDH shall designate.

f. Testing. EDI Submitter shall, prior to the initial Data Transmission and throughout the term of a TPA, test and cooperate with TDH in the testing of Information Systems as TDH considers reasonably necessary to ensure the accuracy, timeliness, completeness and confidentiality of each Data Transmission.

2. Security and Confidentiality. In addition to the other obligations in these policies, EDI Submitter shall also be specifically obligated to do all of the following:

a. To refrain from copying, reverse engineering, disclosing, publishing, distributing or altering and Data, Data Transmissions, or the contents of an Envelope, except as necessary to comply with the terms of these policies or the TPA, or use of the same for any purpose other than for which the EDI Submitter was specifically given Access and authorization by TDH.

b. To refrain from obtaining access by any means to any Data, Data Transmission, Envelope or TDH's Information System for any purpose other than that which the EDI Submitter has received express authorization to receive access. Furthermore, in the event that the EDI Submitter receives Data or Data Transmissions, which are clearly not intended for receipt of the EDI Submitter, the EDI Submitter shall immediately notify TDH and make arrangements to return the Data or Data Transmission or retransmit the Data or Data Transmission to TDH. After such re-transmission, the EDI Submitter shall immediately delete the Data contained in such Data Transmission from its Information System;

c. To install necessary security precautions to ensure the security of the Information System or records relating to the Information System of either

TDH or the EDI Submitter when the Information System is not in active use by the EDI Submitter

d. To protect and maintain at all times the confidentiality of Security Access Codes issued by TDH to the EDI Submitter; and

e. To provide special protection for security and other purposes, where appropriate, by means of authentication, encryption, the use of passwords or by other mutually agreed means. Unless otherwise provided in these TDH EDI policies, the recipient of a Data Transmission so protected shall use at least the same level of protection for any subsequent transmission of the original Data Transmission.

3. TDH Obligations. In addition to the other obligations of TDH, which are set forth herein, TDH shall also do the following:

   a. Availability of Data. TDH shall, subject to the terms of these TDH EDI Policies, make available to the EDI Submitter by Electronic Media those types of Data which the EDI Submitter is authorized to receive.

   b. Notices Regarding Formats. TDH shall inform the EDI Submitter of acceptable formats in which Data Transmissions may be made and shall provide such notices to the EDI Submitter within reasonable time periods consistent with HIPAA Transaction Standards, if applicable, or at least thirty (30) days prior electronic notice of other changes in such formats.

   c. Security Access Codes. TDH shall arrange to provide to the EDI Submitter with Security Access Codes which will allow the EDI Submitter access to TDH's Information System. It is expressly required by these policies that such Security Access Codes are strictly confidential and specifically subject, without limitation, to any and all of the restrictions. Furthermore, TDH reserves the right to change the designated Security Access Codes at any time and in such manner as TDH in its sole discretion deems necessary. Furthermore, the release of Security Access Codes shall be limited to authorized electronic data personnel of EDI Submitter and TDH with a need to know.

Reference(s):

-

Contact(s):

- Privacy Program Office, (615) 741-1969
- Security Officer, (615) 741-0899
- TDH HIPAA Hotline, (877) 280-0054

Tennessee Department of Health

HIPAA Policies

Standard Transactions, Code Sets, and Identifiers

Policy Title: **Confidentiality and Security**

Policy Number: **207**

Effective Date: **March 26, 2013**

PURPOSE:

This policy addresses the security requirements of Trading Partners and EDI Submitters to prevent any unauthorized access to Department of Health Information System.

POLICY:

General:

1. General Requirements. The Trading Partner and any EDI Submitter or other Agent(s) shall maintain adequate security procedures to prevent unauthorized access to Data, Data Transmissions, Security Access Codes or the TDH Information System, and shall immediately notify TDH of any and all unauthorized attempts by any person or entity to obtain access to or otherwise tamper with the Data, Data Transmissions, Security Access Code, or the TDH Information System.

    a. Individually Identifiable Health Information. The Trading Partner and EDI Submitter or other Agent(s) are responsible for ensuring the confidentiality of Individually Identifiable Health Information, consistent with the requirements of the Privacy Statutes and Regulations, and shall take reasonable action to prevent any unauthorized disclosure of Confidential Information by the Trading Partner and any EDI Submitter or other Agent(s). The Trading Partner and EDI Submitter or other Agent(s) shall in their performance of these TDH EDI Policies, comply with any and all applicable Privacy Statutes and Regulations relating to Confidential Information (as defined in these policies).

    b. Notice of Unauthorized Disclosures. The Trading Partner and EDI Submitter will promptly notify TDH of any and all unlawful or unauthorized disclosures of Confidential Information that comes to its attention or to the attention of its Agent(s), and will cooperate with TDH in the event that corrective action is required by TDH.

Reference(s):

•

Contact(s):

- Privacy Program Office, (615) 741-1969
- Security Officer, (615) 741-0899
- TDH HIPAA Hotline, (877) 280-0054

Tennessee Department of Health

HIPAA Policies

Standard Transactions, Code Sets, and Identifiers

Policy Title: **Record Retention and Audit**

Policy Number: **208**

Effective Date: **March 26, 2013**

PURPOSE:

This policy addresses the time period that Trading Partners and/or EDI submitters are required to maintain records and the rights of the Department of Health or its agents to audit the records.

POLICY:

General:

1. Records Retention. The Trading Partner and EDI Submitter shall maintain, for a period of no less than seven (7) years from the date of its receipt complete, accurate and unaltered copies of any and all Source Documents associated with all Data Transmission.

2. Right to Audit. The Trading Partner shall allow, and shall require any EDI Submitter or other Agent to allow, access to TDH, or its designees, and the U.S. Department of Health and Human Services, or its designees, to audit those relevant business records, Source Documents, Data, Data Transmissions, Trade Data Log or Information System of the Trading Partner and/or its Agents as necessary to ensure compliance with these TDH EDI Policies. Trading Partner shall allow, and shall require any EDI Submitter or other Agent to allow, access by TDH or its designees to ensure that adequate security precautions have been made and are implemented by the Trading Partner and its EDI Submitter or other Agent(s) in order to prevent unauthorized disclosure of any Data, Data Transmission or other information.

Reference(s):

-

Contact(s):

- Privacy Officer, (615) 741-1969
- Security Officer, (615) 741-0899
- TDH HIPAA Hotline, (877) 280-0054

Tennessee Department of Health

HIPAA Policies

Standard Transactions, Code Sets, and Identifiers

Policy Title: **Changes in Material Information**

Policy Number: **209**

Effective Date: **March 26, 2013**

PURPOSE:

This policy outlines the procedures a Trading Partner must follow if there are any changes in material information that the Department of Health has on record regarding the Trading Partner.

POLICY:

General:

1. Changes in Any Material Information. Trading Partner shall submit an updated TPA, to TDH within five (5) business days of any material changes in the information. A material changes includes but is not limited to changes in address or email address, identification of authorized individuals or the Trading Partner or EDI Submitter, the addition or deletion of authorized Transactions, or any other change that may affect he accuracy of or authority for an EDI Transaction. TDH is authorized to act on Data Transmissions submitted by the Trading Partner and its EDI Submitter(s) based on information on file until an updated form has been received and approved by TDH. Trading Partner's signature or the signature of an authorized EDI Submitter is required to ensure that an updated TPA, Authorization or EDI Registration form is valid and authorized.

2. Failure to submit a timely updated form may impact the ability of a Data Transaction to be processed without errors. Failure to submit a signed updated form may result in a rejection of a Data Transmission.

Reference(s):

-

Contact(s):

- Privacy Officer, (615) 741-1969
- Security Officer, (615) 741-0899
- TDH HIPAA Hotline, (877) 280-0054