

## Chapter 274. Travis County Health & Human Services Privacy Policies and Procedures<sup>1</sup>

### Contents:

274.001	Definitions 1
274.002	General Principles 2
274.003	Purpose and Scope 2
274.004	Designation of Contact Office 2
274.005	Retention of Documentation 3
274.006	Disclosures and Uses of Protected Health Information 3
274.007	Protection of Protected Health Information 3
274.008	Routine Disclosures and Requests of Protected Health Information 4
274.009	Verifying Identity and Authority Prior to Disclosures 4
274.010	Disclosures to Other Business Associates 5
274.011	Judicial, Administrative and Governmental Disclosures 5
274.012	Disclosures to Patients/Clients In Furtherance of Services, Treatment, & Other Issues 6
274.013	Disclosures to Providers in Furtherance of Services 7
274.014	Procedure for Sending PHI Via Fax: 8
274.015	Procedure for Sending and Receiving Email Messages Containing PHI 10
274.016	Conversations Concerning PHI 11
274.017	Training 12
274.018	Sanctions and Mitigation 13
274.019	Reservation of Right to Change Policies, Procedures or Notice 13

### **274.001 Definitions**

(a) In this subchapter:

- (1) “Alternative Confidential Communications” means requests for communications by alternative means or to alternative locations.
- (2) “Electronic Mail Resources” refer to the County systems, networks, equipment, software, and processes that provide access to or use of these, including creating, accessing, downloading, receiving, transmitting, storing and retaining data and information, as well as the operation of software products and tools but excluding file transfer utilities.
- (3) “E-mail” means Electronic Mail.
- (4) “Electronic Mail Message” means a record created or received on Electronic Mail Resources, including brief notes, formal and substantive narrative documents, and any attachments that may be transmitted with the message.
- (5) “HHS” means Travis County Health and Human Services.
- (6) “Privacy Regulations” means the Health Insurance Portability and Accountability Act of 1996, Privacy Regulations,

---

<sup>1</sup> Chapter 71 was adopted 8/19/2003, Item 10.A. Chapter 71 was renumbered as 274 May 15, 2018, Item 7. Department names, county executive title updated May 29, 2018, Item 8.

promulgated by the Secretary of DHHS at 45 C.F.R. Subtitle A, Subchapter C.

- (7) “Protected Health Information” or “PHI” means any health information that:
  - (A) Is transmitted or maintained in any form, including demographic information collected from an individual,
  - (B) Is created or received by a health care provider, Health Plan, employer, or health care clearinghouse;
  - (C) Relates to the past present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
  - (D) Identifies the individual; or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.
- (8) “Secretary of DHHS” means the Secretary of the U. S. Department of Health and Human Services.

(b) In this subchapter, the definitions for the following words are the same as the definitions in the Privacy Regulations:

- (1) Business associate,
- (2) Covered entity.

#### **274.002 General Principles**

HHS is committed to protecting the privacy of each client’s protected health information in accordance with the Privacy Regulations and contractual agreements with Covered Entities consistent with the delivery of a quality services and effective management of service operations within budgetary restraints. This chapter implements privacy protections in consideration of the Privacy Regulations.

#### **274.003 Purpose and Scope**

The purpose and scope of this chapter is to delineate the privacy policies of HHS and the procedures for implementing the policies to achieve compliance with the obligations of HHS as a business associate of various Covered Entities.

#### **274.004 Designation of Contact Office**

- (a) The contact for privacy concerns is:
  - Privacy Office
  - 100 North IH 35

Austin, TX 78744

(512) 854-4100

- (b) The Privacy Office has responsibility for administering the policies and procedures under the direction of department management and acting as the point person for privacy issues with Covered Entities with which HHS has a business associate agreement.
- (c) The Privacy Office is responsible for responding to Covered Entity requests for patient access to information and other rights under the Privacy Regulations that the Covered Entity may have granted.

**274.005 Retention of Documentation**

Documentation required by the Privacy Regulations shall be maintained for six (6) years from the date a document is created or the date when it was last in effect, whichever is later.

**274.006 Disclosures and Uses of Protected Health Information**

- (a) HHS does not generally obtain a consent or authorization when the use or disclosure of PHI is for the purpose of carrying out treatment or payment or managing service operations or when permitted or required by any law.
- (b) HHS generally obtains a valid authorization from the client prior to using or disclosing PHI in circumstances not covered by 274.008. HHS does not have a HIPAA authorization for information containing PHI when it comes directly from the client, but other release forms may be signed.
- (c) When HHS receives an authorization for disclosures from a Covered Entity or client, HHS releases or discloses information accordingly.

**274.007 Protection of Protected Health Information**

- (a) Access to PHI by HHS employees shall be limited to the minimum necessary amount of PHI reasonably calculated to allow HHS employees to perform their duties.
- (b) Access to electronically maintained PHI shall be limited and controlled by network passwords and, where appropriate, by limitations on access to areas where PHI is present.
- (c) Appropriate physical safeguards shall be observed. Physical copies of records and reports containing PHI shall be maintained in secure filing cabinets, locked drawers or locked rooms and shall not be left open or available for inadvertent exposure.

- (1) Documents containing PHI shall not be left out on desks or in other areas where there is a significant danger of inadvertent disclosure.
- (2) At the end of the work day, documents containing PHI shall be filed in locked filing cabinets, locked desks or locked offices.
- (3) Staff involved in opening and sorting mail shall identify mail that contains PHI and shall route it to appropriate personnel. Mail or other documents containing PHI shall be processed timely and shall not be left out where there is significant danger of inadvertent disclosure.

**274.008 Routine Disclosures and Requests of Protected Health Information**

- (a) HHS generally discloses PHI only in furtherance of its role as a business associate of Covered Entities and in furtherance of the services it provides to its individual clients.
- (b) In general, HHS requests PHI on a routine basis only for purposes of providing services to its individual clients.
- (c) HHS shall not disclose or request an entire medical record unless the entire record is reasonably necessary to accomplish the purpose of the disclosure or request.

**274.009 Verifying Identity and Authority Prior to Disclosures**

- (a) Where HHS does not know the identity of the individual or entity requesting PHI (including public officials), it shall use its professional judgment to verify the identity and the authority of the individual or entity before disclosing the requested PHI unless one of the reasons identified in 164.510 of the Privacy Rule (e.g., in an emergency).
- (b) If the Privacy Regulations require documentation, statements, or representations (e.g., subpoena, authorization, and government letterhead) as a condition of making a disclosure, HHS may rely on these materials to make the disclosure of PHI without performing additional verification, unless otherwise required by the Privacy Regulations or other law.
- (c) With respect to disclosures to public officials, HHS may rely on the following to verify the public official's identity:
  - (1) If the request for PHI is made in person, agency identification, badge, or other proof of government status;
  - (2) If the request for PHI is made in writing, the request is on government letterhead; or

- (3) If the request is to an entity or individual acting on behalf of a government entity, documentation that the entity or individual is acting on behalf of the government entity.
- (d) With respect to disclosures to public officials, HHS may rely on the following to verify the public official's authority:
- (1) A written or oral statement of legal authority for the disclosure of PHI; or
  - (2) A warrant, subpoena, administrative or court order, or other legal process that provides legal authority for the disclosure.

#### **274.010 Disclosures to Other Business Associates**

HHS may disclose to other business associates of Covered Entities with which HHS has entered a business associate agreement.

#### **274.011 Judicial, Administrative and Governmental Disclosures**

- (a) Disclosures of PHI may be made in the following instances:
- (1) In response to a court order or administrative tribunal provided that only the PHI expressly authorized by the order will be disclosed.
  - (2) In response to a subpoena, discovery request, or other lawful process, that is not accompanied by an order of a court or administrative tribunal, if:
    - (A) HHS receives satisfactory assurance from the party seeking the information that reasonable efforts have been made by that party to ensure that the individual who is the subject of the PHI that has been requested has been given notice of the request. Satisfactory assurance means:
      - (i) The requesting party has mailed a written notice to the individual's last known address;
      - (ii) The requesting party provides HHS a written statement, with accompanying documentation, demonstrating that the notice was given and that it contained sufficient information about the litigation or proceeding in which the PHI is requested to permit the individual to raise an objection with the court or tribunal, and no objections were raised or all objections were resolved.
    - (B) HHS receives satisfactory assurance that the party requesting the PHI has made reasonable efforts to obtain a protective order. A qualified protective order means that the parties involved in the dispute are:

- (i) Prohibited from using or disclosing the PHI for any purpose other than the proceeding for which the information was requested; and
    - (ii) Required to return to HHS or to destroy the PHI at the end of the proceeding.
  - (3) Provided in response. to authorized public health requests;
  - (4) Provided for purposes of health oversight activities; and
  - (5) Provided for purposes of DHSS enforcement of Privacy Regulations.
- (b) Questions of appropriateness may be referred to the county executive of the agency or to the County Attorney's office for guidance.

**274.012 Disclosures to Patients/Clients In Furtherance of Services, Treatment, and Other Issues**

- (a) Generally, HHS personnel may use, disclose, and discuss an individual's PHI with the individual. There are exceptions for psychotherapy notes and certain institutional requests.
- (b) The procedure for identifying clients in person by personal knowledge is to identify them by government issued identification or other similar documentation.
- (c) A person may be identified over the telephone or over TTY. Before disclosing PHI by telephone or TTY with a client or personal representative, the identity of the individual must be ascertained as follows:
  - (1) A client may be identified over the phone if they have the following minimum required personal information:
    - (A) Client's Social Security Number,
    - (B) Client's address,
    - (C) Client's phone number,
  - (2) In the course of a client service call or other contact with a client, the client should have knowledge available to the client such as:
    - (A) Provider's name,
    - (B) Past services,
    - (C) Prior contacts.
- (d) If identity of a client is not certain or becomes suspect, no PHI should be disclosed.
- (e) If the caller is inquiring about another individual, verify the right of the caller to access the requested PHI.

- (f) Generally, parents have a right to access the PHI of minor children. If there are notes in the record addressing the issue of parental rights such as limiting a non-custodial parent's right of access, the notes should be followed when determining what access a parent should have to a minor child's PHI.
- (g) As permitted by state law, if a dependent child has established with HHS an approved mode of Alternate Confidential Communications, disclosure of PHI to the parent may not be permitted.
- (h) It is the obligation of the requesting individual to prove their right to the PHI. This may not be possible to do in all cases over the phone or TTY.
- (i) Identification over TTY offers challenges that may not exist in telephone identification. The degree of sensitivity of the information being disclosed is a factor to consider in both telephone and TTY conversations. For example, it may never be appropriate to disclose an AIDS diagnosis over the telephone or TTY. How the call originates may increase confidence depending on whether the HHS employee placed the call to the number a known client. Familiarity with the client's verbal patterns and idioms may enhance confidence. If in doubt, PHI should not be revealed or discussed. However, the HHS employee can always receive information. It is only disclosure that is not allowed. An employee can always receive a problem even if there is doubt about the identity of the caller, however, no PHI should be released in that case.

**274.013 Disclosures to Providers in Furtherance of Services**

- (a) PHI may be discussed or disclosed to a client's health care providers and other service providers in furtherance of treatment, health care operations, and payment.
- (b) The procedure for identifying provider or other service provider in telephone conversations is to verify the identity of the individual as a provider authorized to request information or discuss the PHI. If HHS personnel originate the phone conversation, it may be assumed the call recipient is appropriate. For example when calling the listed number of a medical office, it may be initially presumed the answering person is an authorized representative of the provider. When the contact is initiated by the provider, a provider may be identified over the telephone if the provider is known from prior contacts or has the following information:
  - (1) Client's billing information, or
  - (2) The client's social security number, or
  - (3) Demonstrated knowledge of the relevant client and history.

- (c) If the identity or authority of the provider personnel is in doubt, PHI should not be disclosed.

**274.014 Procedure for Sending PHI Via Fax:**

- (a) HHS has designated a certain fax machine for sending or receiving PHI.
- (b) Individuals have been trained and tasked to identify PHI related faxes and distribute them appropriately.
- (c) A Confidential Fax Coversheet to provide extra protection for PHI has been developed and it includes the following information:
  - (1) The headline of the coversheet states in large bold type: **"Confidential Health Information Enclosed."**
  - (2) Beneath this headline, is a statement: "Health Care Information is personal and sensitive information related to a person's health care. It is being faxed to you after appropriate authorization from the patient/client or under circumstances that do not require patient/client authorization. You, the recipient, are obligated to maintain the health care information in a safe, secure and confidential manner. Re-disclosure of the health care information transmitted without additional patient/client consent or as permitted by law is prohibited without additional patient/client consent unless otherwise authorized by law. Unauthorized re-disclosure or failure to maintain confidentiality could subject you to penalties described in federal and state law."
  - (3) Included at the bottom of the fax coversheet is a warning: "IMPORTANT WARNING: This message is intended for the use of the person or entity to which it is addressed and may contain information that is privileged and confidential, the disclosure of which is governed by applicable law. If the reader of this message is not the intended recipient, or the employee or agent responsible to deliver it to the intended recipient, you are hereby notified that any dissemination, distribution, or copying of this information is STRICTLY PROHIBITED. If you have received this message by error, please n o t e us immediately and destroy the related message."
  - (4) In addition to the warnings described in 274.014(3) and (4), the fax coversheet contains standard information including:
    - (A) Date and time of the fax,
    - (B) Sender's name, address, telephone number and fax number,

- (C) The authorized recipient's name, telephone number and fax number,
  - (D) Number of pages transmitted, and
  - (E) Information regarding verification of receipt of the fax
- (d) HHS staff shall make certain the fax transmittal has received the proper authorization as required by law (i.e., that an appropriate release or authorization is on file) or that there is implied consent because the transmittal is in furtherance of treatment, health care operations, or payment.
- (e) Faxing of sensitive health information, such as that dealing with mental health, chemical dependency, sexually transmitted diseases, HIV or other highly personal information, is prohibited without supervisor approval.
- (f) When expecting the arrival of a fax containing PHI, HHS staff coordinate with the sender whenever possible so the faxed document can be promptly retrieved upon arrival.
- (g) As with other PHI that arrives in the mail or by other means, HHS staff make sure faxes that contain PHI are placed in the designated secure/confidential location when they are delivered, and not left in an in-box in view of passers-by.
- (h) HHS staff confirm the accuracy of fax numbers. It is presumed the fax numbers provided by business associates are correct and secure. The numbers provided by recipients generally may be relied upon as valid. If there is reason to believe a number is not valid or security is suspect, the number or security of recipient machines should be checked by calling the intended recipients to double-check the numbers.
- (i) When faxes are regularly sent to the same recipients, these fax numbers are programmed into the machine's memory, using the speed-dial numbers. Programmed numbers are tested at regular intervals.
- (j) HHS staff make sure the fax machine prints a confirmation of each outgoing transmission and require machine operators to:
  - (1) Make sure the intended destination matches the number on the confirmation, and
  - (2) Staple the confirmation to the document that was faxed.
- (k) If a facsimile is misdirected, HHS staff make sure that improperly faxed documents are either immediately returned or destroyed by the recipient. HHS staff document that the fax was misrouted and take and document steps to prevent a reoccurrence of the error.

- (l) Proof of delivery of PHI that is faxed, will be retained as evidence of the time and date of the transmittal, the intended recipient, its contents, and the fax number at which it was confirmed to have been received.
- (m) In the business associate agreements, or two-way Covered Entity agreements, provisions are included requiring organizations that will receive your faxes to place their fax machines in secure areas.
- (n) As with all other paper documents that contain PHI, faxes that contain PHI are handled and stored in the regular secure manner and shredded when they have outlived their usefulness.

**274.015 Procedure for Sending and Receiving Email Messages Containing PHI**

- (a) E-mail Messages transmitted and received through to the County Electronic Mail Resources within the County network must be sent in compliance with the following procedures:
  - (1) Before sending PHI in an internal E-mail Message, the appropriateness of the communication is considered. The criteria used to determine appropriateness of the communication are the same as apply to any communication of PHI:
    - (A) Is the communication appropriate?
    - (B) Is all of the PHI necessary?
    - (C) Is the receiver in a position to receive in a confidential manner?
  - (2) Before sending PHI through County Electronic Mail Resources, the recipient's email address and recipient shall be verified.
  - (3) E-mail Messages containing PHI shall be deleted from the County Electronic Mail Resources after they are no longer required.
- (b) E-mail Messages transmitted to or received from networks, systems or Electronic Mail Resources external to the County, including but not limited to the Internet, must be sent in compliance with the following procedures:
  - (1) The criteria used in determining the appropriateness of whether to send PHI through E-mail Messages containing PHI from the County Electronic Mail resources to networks, systems or Electronic Mail Resources external to the County, such as the Internet are the same as determining whether to send E-mail Messages to other HHS employees or County employees internally through County Electronic Mail Resources. Consideration shall be given to the sensitivity of the information and the potential of inadvertent disclosure.

- (2) The E-mail address of the recipient shall be verified before sending the E-mail Message.
- (3) To reduce the risk of inadvertent disclosure of PHI, E-mail Messages containing PHI transmitted to networks, systems or electronic mail resources external to the County, including but not limited to the Internet, shall be encrypted in compliance with Travis County Encryption Standard and associated procedures, when adopted by Commissioners Court.
- (4) Where possible, County Electronic Mail Resources will be configured to enable the user of PHI to select delivery verification and to be notified that the recipient received the E-mail Message containing PHI.
- (5) The Email Message shall contain a notice that the email contains PHI which is confidential to provide extra protection for PHI and it should include the following information:
  - (A) Included at the top of the email is a warning:

“WARNING - This e-mail contains Personal Health Information that is protected by federal law and intended for the person to whom it has been addressed. If you received this message in error notify the sender immediately and delete this e-mail and destroy any paper copies. See below for disclosure penalties.”
  - (B) Beneath the text of the message and signature is the following statement: “Health Care Information is personal and sensitive information related to a person’s health care. It is being mailed to this address after appropriate authorization from the patient/client or under circumstances that do not require patient/client authorization. You, the recipient, are obligated to maintain the health care information in a safe, secure and confidential manner. Disclosure of the health care information transmitted is prohibited without additional patient/client consent unless otherwise permitted by law. Unauthorized redisclosure or failure to maintain confidentiality could subject you to penalties described in federal and state law.”

**274.016 Conversations Concerning PHI**

- (a) Employees should conduct conversations concerning PHI in a manner that limits the risk of inadvertent disclosure of PHI through casual overhearing or “overseeing”. Some conversations, because of sensitive nature of the PHI or concerns by the member of inadvertent disclosure, may only be possible in a private office or location.

- (b) Personnel initiating conversations or telephone calls concerning PHI should be aware of their surroundings. For example a call concerning PHI made by a case manager to discuss whether a diagnosis supports a certain medical procedure should not be made from the reception area with clients waiting in the area.
- (c) Personnel initiating a call concerning PHI should be aware of the surroundings of the call recipient. Inquiry may need to be made as to whether the recipient can converse without danger of PHI being inadvertently disclosed to individuals in the immediate area of the call recipient.
- (d) When clients initiate discussion of PHI with HHS staff, staff shall be aware of the potential for inadvertent disclosure of PHI when discussion takes place in reception or common areas of offices. HHS staff shall move appropriate conversations to offices or other quieter locations that reduce the potential for inadvertent disclosure.
- (e) Leaving voice mail or forwarding voice mail containing PHI should be done with the same considerations as engaging & conversations concerning PHI.
- (f) TTY conversation print outs shall be either shredded or placed in the file immediately.
- (g) Written phone messages and other notes shall be either filed or shredded after their use.

**274.017 Training**

- (a) All personnel who may have contact with PHI shall be trained in the requirements of protecting, using and disclosing PHI. Personnel includes all permanent full or part time staff, temporary staff, substitute workers, interns, volunteers, summer youth in work based learning, and other HHS staff that may handle PHI.
- (b) All personnel shall be trained in the requirements and procedures necessary to implement the privacy policies contained in Chapter 71 as relates to their respective jobs.
- (c) Training shall consist of content sufficient to provide:
  - (1) An overview of Health Insurance Portability and Accountability Act and the Privacy Regulations
  - (2) Detailed training on the portions of Chapter 71 that are relevant to the person's responsibilities.
- (d) The training materials are maintained by HHS on its web site or intranet for reference and review. In-service, refresher training is conducted upon determination by management that the policies,

procedures and laws have changed sufficiently to require further training or that compliance would be enhanced by additional training.

- (e) New employees and employees changing assignments are required to undergo relevant privacy training as a condition of their assuming their responsibilities.
- (f) A log shall be maintained that tracks the initial training given to all employees, as well as updates and in-service refresher training modules.
- (g) After completion of training, all personnel must sign a Confidentiality Statement that includes that they understand these policies and procedures and agree to act in compliance with them.

**274.018 Sanctions and Mitigation**

- (a) HHS may discipline any employee who has violated this chapter or the Privacy Regulations. Depending on the severity of the violation, employee discipline may include verbal warning, letter of reprimand, retraining, suspension or termination, whatever is appropriate. Management documents and maintains any sanctions that are imposed pursuant to section 274.005.
- (b) HHS will not discipline any employee who:
  - (1) Files a complaint with the Secretary of DHHS pursuant to the Privacy Regulations;
  - (2) Testifies or assists in an investigation, compliance review, or hearing regarding the compliance by HHS with the Privacy Regulations; or
  - (3) Opposes any act or practice that the employee believes, in good faith, is in violation of the law, if the employee has not disclosed the PHI in violation of the Privacy Regulations and if the opposition is reasonable.
- (c) HHS takes the appropriate and necessary steps to limit the harm of a use or disclosure by an employee in violation of this Chapter or the Privacy Regulations.

**274.019 Reservation of Right to Change Policies, Procedures or Notice**

The County reserves the right to change this chapter as circumstances dictate.