THE UNIVERSITY OF TENNESSEE
HEALTH SCIENCE CENTER

UT Health Science Center: H115 - Safeguards for Protected Health Information	
Version 2	**Publication Date: 07/17/2024**

Responsible Office: Institutional Compliance Office	**Last Review:** 07/17/2024 **Next Review:** 07/17/2027
Contact: Melanie Burlison, Privacy Officer	**Phone:** 901.448.8030 **Email:** institutional.compliance@uthsc.edu

Objective

To facilitate compliance with the Health Insurance Portability and Accountability Act (HIPAA) Standards for Privacy of Individually Identifiable Health Information (Privacy Standards), 45 CFR Parts 160 and 164, the Health Information Technology for Economic and Clinical Health Act (HITECH) component of the American Recovery and Reinvestment Act of 2009 (ARRA), and any and all other Federal regulations and interpretive guidelines promulgated thereunder. To establish guidelines for protecting and safeguarding protected health information (PHI).

Scope

UTHSC must take reasonable steps to safeguard and protect PHI. UTHSC must identify and utilize appropriate administrative, physical, and technical safeguards in order to protect PHI from inappropriate and/or unauthorized access, use, and/or disclosures. In particular, UTHSC must take additional steps to protect patient, patient personal representative, and guarantor social security numbers (SSNs) (e.g., masking or removing the SSNs from documents and/or systems) to help guard against identity theft and financial harm to patients and others. This procedure addresses oral and paper-based PHI. Safeguarding requirements for electronic PHI (ePHI) (e.g., encryption) are addressed in Information Security policies, standards, and procedures; however, general requirements are included for purposes of this procedure.

Definitions

- Administrative Safeguards - the administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic PHI and to manage the conduct of UTHSC workforce in relation to the protection of that information.
- Physical Safeguards - generally are physical measures, policies and procedures to protect and secure all forms of protected health information from unauthorized access, accidental or intentional use, disclosure, transmission, or alteration, and inadvertent or incidental disclosure.
- Technical Safeguards - the technology and the policy and procedures relating to electronic storage, maintenance, and transmittal of PHI, including authentication requirements, password controls, audit trails, email encryption, and Internet use.
- Workforce Members - shall include all UTHSC employees, faculty, staff, students, residents and volunteers.

Procedures

I. Faxing PHI

When faxing PHI, workforce members should take appropriate safeguards:

A. Locate fax machines in low-traffic areas and inaccessible to visitors.
B. Consider whether it is appropriate to fax the PHI (e.g., is there another secure method to send the information, is the recipient authorized to receive the information, is the PHI particularly "sensitive").
C. Confirm telephone requestors by returning the phone call prior to sending.
D. Verify the fax number before sending.
E. Use a fax coversheet.
F. Double check the fax number entered before sending.
G. Set the fax machine to print an auto-confirmation page, if available, and check the confirmation page to ensure:
    1. Delivery was successful, and
    2. Correct fax number was dialed.
H. Use pre-programmed fax numbers, if available:
    1. Test pre-programmed fax numbers prior to use.
    2. Have a process in place to verify the programmed numbers on a regular basis.
    3. Remind regular fax recipients to provide updated fax numbers when numbers change.

II. Paper Documents Containing PHI

Facilities must ensure that reasonable safeguards are in place to protect paper documents containing PHI:

A. To the extent feasible:
    1. PHI should be removed from high visibility areas, even if those areas are not open to the public, and
    2. PHI should be maintained in a confidential manner in order to prevent workforce members and others that do not have a need to know from accessing such PHI.
    3. Documents must not be left unattended in areas accessible to the public (e.g., charts may not be left unattended on a counter that is open to the public).
    4. Access to areas containing PHI must be limited to authorized personnel.
B. Documents containing PHI must be disposed of securely (e.g., place PHI in shred bins not regular trash cans or recycle bins that will not be shredded).
C. Mail and package delivery (e.g., US Postal Service, Fed Ex) pick-up sites should be in a separate location from employee desks or patient counters to help avoid the wrong information being picked up.
D. Clinics must have a process in place to verify documents are for the correct patient prior to providing the documents to the recipient (e.g., verify recipient and content prior to giving discharge papers to an individual).
E. Clinics may not send mailings to individuals if the clinic name on the postcard or envelope seems likely to reveal a patient's sensitive diagnosis.
F. Any removal of documents containing PHI from any clinic must be with the workforce member's manager's advance approval. Only the minimum necessary amount of information required to perform the job function may be approved. The workforce member is responsible for ensuring the documents are safeguarded at all times and promptly returned to the clinic. Safeguarding examples include, but are not limited to:

1. Logging the PHI that will leave the office or facility. PHI should not leave any office or facility unless another copy of the PHI removed remains at the office or facility.
2. Ensuring PHI is not left in an unsecured area (e.g., an unlocked vehicle or a locked vehicle in which the PHI is in plain view or is held in a visible container that may encourage theft such as a box of records, a briefcase, or a laptop computer case.)

III. Oral Communications Involving PHI

Workforce members may only discuss PHI with other authorized workforce members who have a legitimate "need to know" or with others as permitted by the HIPAA Privacy Rule. Clinics must ensure that reasonable safeguards are in place when workforce members verbally communicate PHI including:

A. When leaving messages on answering machines, workforce members must use professional judgment to ensure that such disclosures are in the best interest of the individual and that only the minimum necessary PHI is disclosed.
   1. If the information is necessary to ensure quality care, any and all information may be left, including PHI. The information may include:
      a. Pre-operative instructions (e.g., don't eat nor drink after midnight, take "x" medications).
      b. Urgent follow-up care is required. A voicemail message may be left for the patient stating:
         - The provider's name,
         - Who the caller is trying to reach,
         - It is urgent that the patient call to discuss his/her recent treatment,
         - The return telephone number of the provider, and
         - With whom the individual should ask to speak with when returning the call.
   2. To confirm appointments, workforce members must ensure that the clinic, or physician's name would not potentially reveal a sensitive diagnosis.

B. Clinics are permitted to use patient sign-in sheets or call out patient names in waiting rooms provided that the information disclosed is appropriately limited per minimum necessary standards and reasonable safeguards are in place (e.g., sign-in sheets do not require the patient to indicate the reason for being seen, removable labels are utilized).

C. Workforce members must take reasonable safeguards and precautions when discussing PHI. The HIPAA Privacy Rule exempts certain oral treatment communications in order to ensure a provider's primary concern is the treatment of the patient. In emergency situations, providers may engage in communications as required for quick, effective, and high-quality health care. When appropriate and practicable, suggested safeguard examples include, but are not limited to:
   - Using lowered voices.
   - Speaking apart from others.
   - Refraining from discussing PHI in elevators, or other public areas; and
   - Asking visitors to leave the room or obtaining patient consent prior to speaking in front of visitors.

IV. General Safeguards for Electronic Media

Workforce members must take appropriate safeguards to limit disclosure of PHI at workstations and other areas where computer monitors may be located:

A. Computer monitors must be positioned away from the direct view of the general public.
B. Password protected screensavers must be in place on computer monitors.
C. Passwords must not be displayed or viewable (e.g., attached to the monitor).

IT Security Department maintains Policies, Standards, guidance, and procedures which outline physical and technical safeguards to PHI which is stored on electronic media (ePHI), including detailed encryption requirements. For the purposes of this procedure, clinics must ensure that:

A. No media (e.g., cellular telephones, flash or "thumb" drives, laptop computers, workstations) are used to access or store PHI without appropriate encryption and authorization.
B. No personal media may be used to connect to UTHSC network, or to access or store PHI (or any type of UTHSC data). Note: This does not pertain to media purchased by medical residents from a communication's stipend from the University.