11.1.15 Safeguards for Protected Health Information

Chapter 11 - Patient Privacy	Original Effective Date: February 2016
Section: 11.1 General and Oversight Policies	Date Last Reviewed: January 2023
Responsible Entity: Chief Compliance and Privacy Officer	Date Last Revised: January 2023

I. Purpose

UT Health San Antonio values its member's privacy rights and is committed to safeguarding protected health information. HIPAA Rules require that the University have reasonable administrative, technical and physical safeguards in place to protect patient protected health information (PHI) from any intentional or unintentional use or disclosure and to limit incidental uses or disclosures. UT Health San Antonio will make reasonable efforts to use or disclose only the minimum amount of PHI necessary for treatment, payment, or health care operations.

II. Scope

This policy applies to all faculty, staff, students, residents, healthcare providers, researchers, contractors, or any other individual (collectively, Workforce Member, including employees and non-employees) who has direct or indirect access to patient protected health information (PHI) created, held or maintained by any UT Health San Antonio controlled affiliate, including, but not limited to its clinics, hospitals, and research operations.

III. Policy

A. Administrative, Physical, and Technical Safeguards

1. Workforce members will only access or use the minimum necessary amount of PHI to carry out their job responsibilities related to treatment, payment or health care operations, or other authorized purposes.

2. Workforce members will disclose PHI only to other workforce members or authorized users who have "a need to know" in order to carry out their job responsibilities related to treatment, payment or health care operations, or other authorized purposes.

3. Workforce members must avoid unnecessary or inappropriate disclosures of PHI through oral communications.

4. Conversations, both phone and face-to-face, involving PHI shall take place in low tones, to the extent possible, and in closed offices or cubicles when possible.

5. When having a conversation in a public area with a patient, the patient's family members, or other conversations in which PHI is discussed, conduct the conversation in a lowered voice, to the extent possible, and avoid using patients' names or the names of patients' family members when persons who are not authorized to receive the information are present.

6. PHI may be released over the telephone in the same manner that it may be released in person, in accordance with the policies regarding disclosures of PHI, and will be documented as appropriate. When handling a call that involves PHI, efforts to verify the identity and authority of the caller will be made prior to discussing the PHI. (See IHOP policy 11.1.6 Confidentiality of Patient Health Information.)

7. PHI mailed must be in sealed envelopes and no PHI can be visible.

8. De-identified PHI must be properly redacted or de-identified in accordance with IHOP policy 11.2.9 De-identification of Protected Health Information.

9. The transmission of PHI via facsimile (fax) is permitted in accordance with the accounting of disclosures (See IHOP policy 11.3.1 Accounting of Disclosures of Protected Health Information), provided that an approved Facsimile Cover Sheet, containing confidentiality language is used. The sender ensures that an appropriate person is available to receive the fax as it arrives, and that the fax is being sent to a secure location. (See IHOP policy 11.1.8 Fax Transmittal of Protected Health Information.)

10. PHI may not be included in an electronically transmitted message over a public network (i.e., Internet, except as permitted by an in accordance with the Universities e-mail policy IHOP policy 11.1.12 E-mailing Protected Health Information). E-mail destined for an address outside of the UTHSCSA.edu (e-mail) network that contains PHI should be processed through UT Health San Antonio's secure e-mail gateway (see Secure Email instructions located at https://infosec.uthscsa.edu/secure-email) which will encrypt the communication in a form that can be decrypted by the intended recipient.

11. Computer screens and monitors will be located in areas or at angles that minimize viewing by persons who do not need the information or utilize privacy screens.

12. Whiteboards and scheduling boards that display PHI will be located in areas that minimize viewing by persons who do not need the information, or the information will be de-identified of PHI.

13. PHI should not be printed or copied indiscriminately or left unattended and open to compromise.

14. Workforce members must store paper PHI in secure areas that are not accessible to unauthorized individuals, preferably in a locked room or filing cabinet.

15. The original media should be used (e.g., hardcopy medical record, EPIC, My Chart) and only reproduced when absolutely necessary.

16. Printers and copiers used for printing of PHI should be in a secure location. If the equipment is in a non-secure location, the information being printed or copied is required to be strictly monitored. PHI printed to a shared printer should be promptly removed.

17. PHI in hardcopy format must be disposed of in accordance with the records retention schedules of UT Health San Antonio.

18. Disposal of patient information, when no longer needed or required by law, will be properly disposed of, or destroyed, so that it is unrecoverable. This may be accomplished by shredding or other methods that render the document non-readable. For example: documents can include but are not limited to sign-in logs, lab or diagnostic reports, patient schedules, billing and health records and duplicate cash receipts.

19. The designated custodian of the medical record had the sole authority to disclose PHI when a patient authorization is required.

20. Medical records, devices, or external media containing PHI that are transported should never be left unattended and be properly secured.

21. Workforce members must not share passwords or other log-in credentials to circumvent information security standards.

22. Workforce members must not bypass security measures to photograph and/or transmit PHI.

23. Workforce members must not post and/or transmit patient information, images, or PHI on social media web sites.

24. PHI stored in medical equipment (e.g., EKG, Ultrasound) must be kept secure and disposed in a way that preserves the confidentiality of the patient information.

25. For additional guidance relating to securing and storing PHI on mobile devices, see IHOP policy 11.1.14 Securing Protected Health Information and Mobile Devices.

26. For additional guidance on security of confidential information see IHOP Section 5.8 Information Security.

B. Mitigation

UT Health San Antonio, and or its business associates, to the extent practicable, maintains policies and procedure to mitigate harmful effects in the event of a violation of this policy or an improper use/disclose of PHI. The duty to mitigate includes, but is not limited to:

1. Taking operational and procedural corrective measures to remedy violations;

2. Taking employment actions, reprimand, or discipline Workforce members as necessary, up to and including termination;

3. Addressing problems with business associates once UT Health San Antonio is aware of a breach of privacy; and,

4. Addressing and investigating the UT Health San Antonio's facility workforce violations.

IV. Definitions

Terms used in this document, have the meaning set forth in the Patient Privacy Policies Glossary *unless a different meaning is required by context.*

V. Related References

For questions regarding this policy, contact the Privacy Program Director at 210-567-2014 or compliance@uthscsa.edu.

VI. Review and Approval History

A. The approving authority of this policy is the University Executive Committee.

B. The review frequency cycle is set for three years following the last review date, a time period that is not mandated by regulatory, accreditation, or other authority.

Effective Date	Action Taken	Approved By:	Date Approved
02/2016	Policy Origination		
01/2023	Policy Review	ICPO	01/31/2023
10/2023	Policy Revision	ICPO	10/02/2023