11.1.12 E-Mailing Protected Health Information

Chapter 11 - Patient Privacy	Original Effective Date: May 2005
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 allows protected health information (PHI) to be transmitted by electronic mail (e-mail) for treatment, payment, or health care operations as permitted within the framework of this policy using the required safeguards. Licensed physicians with the Texas Medical Board must follow the rules outlined at http://www.tmb.state.tx.us/page/laws-main-page.

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. General Requirements

1. E-mail containing PHI should be treated with the same degree of privacy and confidentiality as all PHI maintained within UT Health San Antonio.
2. When using PHI in e-mail communications, staff should limit the information exchanged with authorized recipients to the minimum necessary. See HOP policy 11.2.5 Uses and Disclosures of Protected Health Information - Minimum Necessary Requirements.
3. In addition, de-identified information should be used whenever possible, according to HOP policy 11.2.9 De-Identification of Protected Health Information.

4. All external disclosures of PHI in e-mail communications must be in compliance with privacy policies addressing the use and disclosure of PHI. See HOP section 11.2 Uses and Disclosures of Protected Health Information and HOP policy 11.3.1 Accounting of Disclosures of Protected Health Information.
5. All disclosures of PHI in e-mail communications outside the realm of treatment, payment, and health care operations require additional patient authorization according to HOP policy 11.2.3 Uses and Disclosures of Protected Health Information Based on Patient Authorization.
6. E-mail containing PHI must have special encryption safeguards in place especially if the recipient is outside the UTHSCSA.edu (e-mail) network. The e-mail should be processed through the UT Health San Antonio secure e-mail gateway, which will encrypt the communication in a form that can be decrypted by the intended recipient. The instructions for securing e-mail are provided at https://infosec.uthscsa.edu/secure-email.
7. E-mail sent, received, or stored on computers owned, leased, administered, or otherwise under the custody and control of UT Health San Antonio is the property of UT Health San Antonio. For portable computing devices, see IHOP policy 5.8.12 Mobile Device and Personally Owned Computing Policy.

B. Patient Communication

1. The preferred route of communication with the patient is through a secure portal that enables the enrolled patients to have access to their health information and to communicate with their healthcare providers on-line.
2. Patients will be requested to provide their personal e-mail address to receive a link to the secure portal and a password to set-up an account.
3. E-mail addresses of patients, families, or legally authorized representatives should not be compiled and used for marketing purposes or supplied to any third party for advertising, solicitations, fundraising, or any other use.

C. Technical Safeguards

1. Never send PHI by e-mail unless you have verified that:
   a. The recipient is authorized to obtain the PHI;
   b. The recipient's email address is entered correctly; and,
   c. The e-mail has encryption safeguards in place (especially when the e-mail is being transmitted to an external recipient who does not have a UTHSCSA.edu email address).
2. Include a standard confidentiality statement on all outgoing e-mails. For example:

"The information in this e-mail may be confidential. This e-mail is intended to be reviewed only by the individual or organization named above. PHI in hardcopy format must be disposed of in accordance with the records retention schedules of UT Health San Antonio. If you are not the intended receipt or an authorized representative of the intended recipient, you are hereby notified that any review, dissemination, or copying of this e-mail and its attachments, if any, or the information contained herein is prohibited. If you have received this e-mail in error, please immediately notify the sender by return e-mail and delete this e-mail from your system. Thank you."

3. Information resources and the Office of Information Security administer technical safeguards to protect the security of e-mail, including publication of various policies in the IHOP. See the following policies in the HOP: 5.2.6 Electronic Mail Use and Retention, 5.8.13 Security Monitoring, and 5.8.9 Malware Prevention Policy.
4. E-mails containing protection health information must be retained in accordance with the records retention schedule of UT Health San Antonio. It is the user's responsibility, with guidance and training from the Records Management Officer, to manage e-mail messages according to the Records Retention Schedule.

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
05/2005	Policy Origination		
03/2013	Policy Revision		
01/2014	Policy Revision		
06/2022	Policy Revision		
01/2023	Policy Review, discretionary edits	ICPO	1/31/2023