Chapter 11	Patient Privacy Policies	Effective:	May 2005
Section 11.1	General and Oversight Policies	Revised:	October 2016
Policy 11.1.12	**E-Mailing Protected Health Information**	Responsibility:	Chief Compliance Officer for Regulatory Affairs & Compliance

E-MAILING PROTECTED HEALTH INFORMATION

Policy

UT Health San Antonio allows the e-mailing of protected health information 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. E-mail containing protected health information should be treated with the same degree of privacy and confidentiality as all protected health information maintained within UT Health San Antonio.

Electronic mail destined for an address outside of the UTHSCSA.edu (e-mail) network that contains protected health information 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 at Secure Email.

Definitions

ELECTRONIC MAIL SYSTEM: Any computer software application that allows electronic mail to be communicated from one computing system to another.

ELECTRONIC MAIL (E-MAIL): Any message, image form, attachment, data, or other communication sent, received, or stored within an electronic mail system.

EXTERNAL E-MAIL: E-mail communications sent outside the UT Health San Antonio network, i.e., to an address other than 'username@uthscsa.edu'.

INTERNAL E-MAIL: E-mail communications exchanged within the UT Health San Antonio network, i.e., only to an address 'username@uthscsa.edu'.

PROTECTED HEALTH INFORMATION: Individually identifiable health information, including demographic data, that is maintained in any medium that relates to:

- The individual's past, present or future physical or mental health or condition,
- The genetic information of the individual,
- The provision of health care to the individual, and/or
- The past, present, or future payment for the provision of health care to the individual and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual.

Protected Health Information does not include individually identifiable health information of persons who have been deceased for more than 50 years.

PROVIDER: For purposes of this policy, the provider is the health care provider allowed by this policy to exchange protected health information via e-mail within the parameters of this policy.

Ownership

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. E-mail messages, sent or received, that concern the treatment of a patient are considered part of the patient's health record.

Also, for portable computing devices, see Section 5.8.12 of the *Handbook of Operating Procedures* (HOP), "Mobile Device and Personally Owned Computing Policy".

Patient Communication

Within the UT Medicine clinics the preferred route of communication with the patient is through a secure portal that enables the enrolled patients' access to their health information and to communicate with their healthcare providers on-line rather than through e-mail communication.

New patients to UT Medicine clinics will be requested to provide their personal e-mail address for receipt of a one-time e-mail generated by the UT Health San Antonio electronic health record providing the

patient with a link to the secure portal and a password to set-up an account.

Patient Authorization

Except as discussed above with the secure portal, all other e-mail communications with the patient or legally authorized representative must have their agreement to communicate via e-mail on non-emergent and non-urgent matters. The patient must specifically authorize e-mail communication to other family members, using the **Patient Authorization for Release of Health Records to External Parties** form.

The patient must complete the UT Health San Antonio **E-mail Authorization Agreement**. The provider may respond to patient e-mails only after the agreement is signed. A copy of the signed form is given to the patient if requested, and the original is forwarded to the medical record custodian for filing in the medical record.

Patient authorization is not required to exchange e-mail that contains protected health information internally (uthscsa.edu network) within the framework of this policy. UT Health San Antonio staff may not send or forward any protected health information outside or external to the UT Health San Antonio network unless specifically authorized to do so by the patient. Authorized external e-mail communication must be encrypted by the UT Health San Antonio secure e-mail gateway (instructions are provided at http://ims.uthscsa.edu/information_security/secure_email.aspx). The sole authorization exception is for providers exchanging protected health information for treatment purposes. Providers may do so without a specific patient authorization if sound encryption techniques are used and the provider's communication is an allowed use or disclosure according to Section 11.2.4 "For Treatment, Payment and Health Care Operations" of the HOP. Extreme caution should be used in any electronic exchange of protected health information.

Authority to E-Mail Protected Health Information

The authority to e-mail encrypted protected health information to patients and outside health care providers is limited to providers, such as faculty members, nurse practitioners, physician assistants, etc. The provider may appropriately delegate e-mailing protected health information to clinic or office staff. Other staff, such as billing staff, are

allowed to e-mail encrypted protected health information internally as authorized by the department administrators or chairs.

Residents are allowed to e-mail encrypted protected health information internally and externally to patients and external health care providers within the parameters of this policy. They are required to send a copy of the e-mail to the supervising faculty member.

Students are not allowed to e-mail protected health information to patients or outside health care providers under any circumstances. Students are only allowed to e-mail protected health information internally under the direction of the supervising faculty.

Provider Responsibilities

It is the responsibility of the UT Health San Antonio provider to ensure that the patient has signed the **E-mail Authorization Agreement** before corresponding by e-mail. If the agreement has not been signed allowing correspondence via e-mail, UT Health San Antonio personnel must have the patient sign the agreement before any further correspondence is initiated. The form may be faxed to the patient, and the signed copy may be returned to UT Health San Antonio via fax. All e-mail correspondence between a provider and patient must be in accordance with the agreement and this policy.

The provider should verify the accuracy of e-mail addresses when sending protected health information to guard against unauthorized disclosure of information.

As a guideline, providers should respond to patient e-mails within two to three business days. If an action is taken based upon an e-mail from a patient, the provider should respond to the patient's e-mail notifying him/her of the action taken. The provider is not compelled to respond to a patient's request to e-mail protected health information and may discontinue e-mail communication at any time.

All e-mails to patients regarding health care treatment should be forwarded to the medical record custodian for inclusion in the patient's health record.

Chapter 11	Patient Privacy Policies	Effective:	May 2005
Section 11.1	General and Oversight Policies	Revised:	October 2016
Policy 11.1.12	**E-Mailing Protected Health Information**	Responsibility:	Chief Compliance Officer for Regulatory Affairs & Compliance

Allowed E-Mail Communication

E-mailing of protected health information within the UT Health San Antonio system is allowed for treatment, payment, and health care operations. E-mailing protected health information externally is also allowed for these purposes if the patient has signed an agreement as described above. Specifically, we may send protected health information to the patient's other physicians, other hospitals, nursing homes, etc., involved in the patient's care.

In general, e-mail communication should be used to address administrative issues, relay follow-up information, and answer questions following a face-to-face evaluation and consultation. Initial evaluation and diagnosis and topics of a sensitive nature should not be communicated through e-mail. The health care provider should use discretion in corresponding with the patient through e-mail for treatment.

The following topics are examples of topics generally appropriate for e-mail communication:

- Prescriptions/refills.
- General medical advice after an initial face-to-face visit.
- Lab test results.
- Patient educational material.

Examples of inappropriate topics may include:

- Discussion of HIV status.
- Psychiatric disorder.

Urgent matters are generally not appropriate for e-mail communication.

Content of E-Mails

The content of e-mails should be in accordance with Section 5.2.6 of the HOP, "Electronic Mail Use and Retention" and Section 5.8.10 "Information Resources Acceptable Use and Security Policy". Although information exchanged in e-mails with patients may be somewhat informal in nature, the provider must ensure that language used in e-mail communications with patients is clear, concise, and professional.

The following are guidelines for e-mail communications:

- Include a clear and specific subject line;
- Edit any quoted text down to the minimum needed;
- Review the final draft before sending;
- Evaluate how the recipient might react to the message;
- Check spelling and grammar;
- Refrain from using ALL CAPS in e-mail as it may be perceived as direction, stern emphasis, or dictatorial;
- Use caution in the amount and type of information written in an e-mail;
- Assume the e-mail is not secure, and information in e-mail is always at risk; and,
- When in doubt about the content of the e-mail or the possible reaction of the recipient, call the patient rather than communicating by e-mail.

The footer used on e-mails exchanged with patients must include, “To My Patients: You must authorize me to communicate with you by e-mail in writing on a special form. If you have not signed an authorization form, please contact my office, and we will send you the form. Please note that e-mail is not necessarily confidential and should be used for routine matters only. Urgent or emergent issues should be handled by telephone. E-mails may not be read in a timely manner if I am out of the office.”

In addition, a standard confidentiality statement should be included on all outgoing e-mails, “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. If you are not the intended recipient 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."

Privacy Issues

All protected health information exchanged via e-mail is to be maintained in a private and confidential manner, according to Section 11.1.6 of the HOP, "Confidentiality of Patient Health Information". When using protected health information in e-mail communications, staff should limit the information exchanged to the minimum necessary to meet the requestor's needs. See Section 11.2.5 of the HOP, "Minimum Necessary Requirements for Uses and Disclosures of Protected Health Information" In addition, de-identified information should be used whenever possible, according to Section 11.2.9 of the HOP, "De-identification of Protected Health Information".

All external disclosures of protected health information must be in compliance with privacy policies addressing use and disclosure of protected health information found in Section 11.2 of the HOP, "Uses and Disclosures of Protected Health Information", including accounting for disclosures required under Section 11.3.1 of the HOP, "Accounting of Disclosures of Protected Health Information". Additional patient authorization is required for any disclosures made outside the realm of treatment, payment, and health care operations, according to Section 11.2.3 of the HOP, "Uses and Disclosures of Protected Health Information Based on Patient Authorization".

E-mail addresses of patients, families, or legally authorized representatives will not be compiled and used for marketing purposes or supplied to any third party for advertising, solicitations, fundraising, or any other use.

Technical Safeguards

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 HOP. See the following sections of the HOP: Section 5.2.6, "Electronic Mail Use and Retention", Section 5.8.13, "Security Monitoring", and Section 5.8.9 "Malware Prevention Policy"".

When sending a protected health information attachment externally, such as a letter or report, the attachment should be password protected either in a "Word" document or a zip file. The sender can also use encryption to protect the document from unauthorized access.

Retention

E-mails containing protected health information will be forwarded to the medical record custodian for inclusion in the health record, paper or electronic, and will be retained according to institutional retention guidelines.