



EAST TENNESSEE STATE UNIVERSITY

HIPAA Compliance

HIPAA Policy No. 001

Electronic Communication of Health Related Information via Email with Patients

Responsible Office HIPAA Compliance Office
Responsible Official HIPAA Compliance Officer

Effective Date 05.01.2016

Scope:

This policy applies to all ETSU Personnel working within or on behalf of the University covered components, as designated from time to time by the University for purposes of complying with the privacy and security provisions of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

This policy establishes standards for the electronic transmission of Protected Health Information ("PHI") via email and the safeguards that ETSU Personnel shall employ to protect the security and privacy of PHI when electronically communicating with patients.

Purpose:

To ensure PHI that is to be communicated electronically is transmitted in a manner that protects it against unauthorized access and maintains its integrity and availability. To accommodate both the need to protect PHI and the need for efficient communication of PHI electronically in support of patient care, PHI shall be transmitted electronically via email only when the limited circumstances described herein are met. When the circumstances allow transmission of PHI, reasonable and appropriate security measures shall be implemented.

Policy:

ETSU Personnel shall comply with the following whenever PHI is to be transmitted via email to patients:

- A. ETSU Personnel shall obtain consent from the patient prior to initiating email communications with the patient. (See "Exhibit A.")
- B. The use or disclosure of PHI must be permitted or required by law.
- C. PHI shall be limited to the minimum necessary amount required to accomplish the intended purpose. (See Minimum Necessary Policy.)
- D. ETSU Personnel shall utilize their official University assigned email account to transmit PHI.
- E. Highly sensitive PHI such as mental health information, substance abuse treatment, or HIV or STD status should be transmitted by email only in exceptional circumstances

- F. Emails containing PHI must include the University Privacy Statement. (See "Required Privacy Statement.")
- G. PHI may only be sent via unencrypted email after the recipient's address has been carefully verified and entered correctly.
- H. ETSU Personnel shall recommend use of patient portal where available instead of email as a more secure means of communicating PHI to the patient.

Procedure:

ETSU Personnel shall follow the procedures outlined below to communicate PHI via email with patients.

1. Obtain written patient consent to unencrypted email communications of PHI. This step should be followed regardless of whether the patient initiates email communications. (See "Exhibit A.")
2. File consent in the patient's medical record.
3. Ensure email communications with the patient are in line with consent given. If the patient consents to receive email only in re: to billing and appointment reminders, ETSU Personnel should only utilize email to send billing information and appointment reminders.

Required Privacy Statement:

CONFIDENTIALITY NOTICE: This electronic message, including any documents, files or previous electronic messages attached to it, may contain Protected Health Information or other confidential information protected under state and federal law, and is intended solely for the use of the individual or entity to whom it is addressed. If you are not the intended recipient please be advised that any unauthorized use, dissemination, printing, copying, or the taking of any action in reliance on the contents of this information is strictly prohibited. If you have received this electronic message in error, please immediately notify the sender with a copy to hipaa@etsu.edu, and destroy this message.

Definitions:

ETSU Personnel: all workforce members of the University's covered components including employees, students, volunteers, trainees and other persons who work in or on behalf of the covered component, whether or not they are paid.

Protected Health Information: all individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or medium, whether printed, spoken, or electronic.

- Common examples of protected health information include a patient's: diagnosis, prognosis, name, address, date of birth, social security number, payment information, insurance ID number, identities of a patient's relative, photographs, patient's email address, etc.

University Covered Component: a component or combination of components of the University that would meet the definition of a covered entity or a business associate if the component were a separate legal entity, designated in accordance with 45 CFR 164.105(a)(2)(iii)(D).

HIPAA Regulatory Information

Category: HIPAA Security Rule

Reference: Technical Safeguards 45 CFR 164.312

EMAIL COMMUNICATION OF HEALTH INFORMATION FACT SHEET

As a patient of East Tennessee State University, you may request that we communicate with you via unencrypted electronic mail (email). This Fact Sheet will inform you of the risks of communicating with your healthcare provider via email. Your health is important to us and we will make every effort to reasonably comply with your request to receive communications via email, however, we reserve the right to deny any request for email communications when it is determined that granting such a request would not be in your best interest.

PLEASE READ THIS INFORMATION CAREFULLY

ETSU healthcare providers and staff will make every effort to promptly respond to your requests for information via email, however, *if you are experiencing an emergency, you should never rely on email communications and should seek immediate medical attention.*

Risks of using email to send protected health information include, but are not limited, to:

- **Risk of Unauthorized Access by a 3rd Party:** Do you share a computer with your family? Is your email address or access to email provided through your employer? Do you access your email over an unsecured connection such as public Wi-Fi? Do you access your email on your mobile device? Emails may be accessed by someone you do not wish to know about your health information. Despite necessary precautions, email may be sent to the wrong address by either party. Email may be intercepted or altered in transmission by a computer hacker or computer virus.
- **Unique Difficulty in Verifying the Sender:** Email may be easier to forge than handwritten or signed papers. Your healthcare provider will only send emails to the email address you provide, but it may be difficult to confirm that you are in fact the person sending the request for information from your email address.

PATIENT CONSENT TO UNENCRYPTED EMAIL COMMUNICATIONS

By signing below, you acknowledge your recognition and understanding of the inherent risks of communicating your health information via unencrypted email and hereby consent to receive such communications despite those risks. By signing below, you also acknowledge that you have the choice to receive communications via other more secure means such as by telephone, in-person, or through the patient portal instead of via unencrypted email. By signing below, you agree to hold ETSU harmless for unauthorized use, disclosure, or access of your protected health information sent to the email address you provide. This consent does not expire.

Patient Printed Name _____

Date of Birth _____

Patient Signature _____

Date Signed _____

If signed by someone other than the Patient, state your relationship to the Patient and a description of your authority to act on the Patient's behalf:

Patient Email Address: _____

Please initial beside **one** of the following to indicate your email preferences:

_____ I consent to receive appointment reminders and billing information **only**.

_____ I consent to receive **full communication** of my protected health information via unencrypted email.

If at any time you change your email address or wish to discontinue email communications altogether, you must notify your healthcare provider immediately in writing.