EAST TENNESSEE STATE UNIVERSITY

HIPAA Compliance

HIPAA Policy No. 001
Electronic Communication of Health Related Information (Email)

Responsible Office HIPAA Compliance Office
Responsible Official HIPAA Compliance Officer **Effective Date** 07.01.2015

Scope:
This policy applies to ETSU Personnel working within or on behalf of the University's healthcare components, designated as such 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 will employ to protect the security and privacy of electronic PHI (e-PHI).

Policy Statement:
e-PHI shall be transmitted in a manner that protects it against unauthorized access and ensures its integrity and availability. To accommodate both the need to protect PHI and the need for efficient communication of PHI in support of patient care, PHI may be transmitted electronically via email only when the limited circumstances described herein are met. When the circumstances allow transmission of e-PHI, reasonable and appropriate security measures shall be implemented. Where feasible, ETSU Personnel should utilize secure messaging features available through our electronic medical record vendors instead of email.

Definitions:
Protected Health Information (PHI): all individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or media, 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.

Electronic Health Information (e-PHI): all protected health information that is created, received, used or maintained in electronic form.

ETSU Personnel: all individuals, whose duties in the clinical or academic setting necessarily involve access or exposure to PHI to carry out healthcare activities or related services. For the purposes of this policy ETSU Personnel also includes all individuals employed by Medical Education Assistance Corporation (MEAC) or working within the clinical setting at a MEAC operated facility.

Policy: Due to the sensitivity of patient health information and the inherent risks associated with communicating via email, email communications must meet the following requirements:

001.01 Email Communications

I. The use or disclosure of PHI must be permitted or required by law, or pursuant to a valid authorization executed by the patient.
II. PHI must be limited to the minimum information necessary for the permitted or required purpose.
III. ETSU Personnel may identify the patient using internal identifiers within the body of the email message, such as an internally assigned medical record number or account number. The use of all other patient identifiers within the body of the message is strictly prohibited. Where an internally assigned identifier contains patient specific information e.g. a patient's initials or year of birth, ETSU Personnel should contact the HIPAA office for further instruction. (See list below of prohibited patient identifiers).
IV. When other identifiable information must necessarily be included, it must be attached in a password encrypted file. The password should meet University standards for complexity and be communicated to the intended recipient via telephone. (See the instructions on how to encrypt a file below).
V. Highly sensitive PHI such as mental health information, substance abuse treatment, or HIV or STD status should be transmitted by email only in emergency circumstances.
VI. ETSU Personnel should always use their etsu.edu email account when communicating PHI. An etsu.edu email account that may send or receive PHI must never be set to auto-forward messages to a non-etsu.edu account.
VII. PHI may only be sent by email after the recipient's address has been carefully verified and entered correctly.
VIII. Email containing PHI must include the University privacy statement providing a contact to whom a recipient can report a misdirected message. (See required privacy statement below).

001.02 Email Communications with Patients (etsu.edu to Patient email accounts)

I. Prior to communicating with a patient via email, the risks associated with communicating health information via email must be clearly explained and written consent to receive communication via email must be obtained. This step should be followed regardless of whether the patient initiates email communications. (See required fact sheet and consent below).
II. PHI must be limited to the minimum information necessary for the permitted or required purpose.
III. Highly sensitive PHI such as mental health information, substance abuse treatment, or HIV or STD status should be transmitted by email only in emergency circumstances.
IV. ETSU Personnel should always use their etsu.edu email account when communicating PHI. An etsu.edu email account that may send or receive PHI must never be set to auto-forward messages to a non-etsu.edu account.
V. PHI may only be sent by email after the patient's email address has been carefully verified and entered correctly.

VI. Email containing PHI must include the University privacy statement providing a contact to whom a recipient can report a misdirected message. (See required privacy statement below).

Instructions to Encrypt a File:

In Microsoft Word 2010:

1. Click "File"
2. Click "Info"
3. Click "Protect Document"
4. Select "Encrypt with Password"
5. Type a complex password into the Password Box and Click "OK"

In Microsoft Excel 2010:

1. Click "File"
2. Click "Info"
3. Click "Protect Workbook"
4. Select "Encrypt with Password"
5. Type a complex password into the Password Box and Click "OK"

For PDF Files:

1. Right Click within the document
2. Click "Document Properties"
3. Select "Password Security" from the Security Method Dropdown
4. Click "Require password to open document"
5. Type a complex password into the Document Open Password Box and Click "OK"

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.

Patient Identifiers: Use of these identifiers in the body of an email message is prohibited.

-Name
-Address
-Date of Birth
-Social Security Number
-Driver's License or License Plate Number
-Any other identifying code or characteristic
-Email Address
-Medical Device Number
-Full Face Photograph
-Telephone Number
-Fax Number
-Identifiers of a patient's relative or employer

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.

Patient Signature_____ Date of Birth:_____

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.