EAST TENNESSEE STATE UNIVERSITY

HIPAA Compliance

HIPAA Policy No. 001
Electronic Communication of Health Related Information via Email with ETSU Personnel

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 each other. This policy does not apply to email with patients. (See Electronic Communication of Health Related Information with Patients via Email.)

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:

A. PHI to be communicated by email shall be transmitted via ***encrypted email*** only.
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 encrypted email after the recipient's address has been carefully verified and entered correctly.

Procedure:
ETSU Personnel shall follow the procedures outlined below to encrypt all emails containing PHI.
Internal Encrypted Email (@etsu.edu to @etsu.edu addresses):

1. Users shall type the word ***encrypt*** anywhere in the subject line to encrypt the contents of the email and any attachments.
2. Users shall not include PHI in the subject line of the email—the subject line is not secure.
3. Users shall ensure the word ***encrypt*** remains in the subject line in subsequent emails (e.g., replies, forwards, etc) to maintain encryption of the email.

Encrypted emails sent internally will show up in the recipient's inbox and look completely normal. The recipient will not have to take any additional steps to decrypt/read the message.

External Encrypted Email (@etsu.edu to @msha.com, @gmail.com, etc.)

1. Users shall type the word encrypt anywhere in the subject line to encrypt the contents of the email and any attachments.
2. Users shall not include PHI in the subject line of the email—the subject line is not secure.

Encrypted emails sent to an external email address will show up in the recipient's inbox and require extra steps. The recipient will receive an email with a link. The recipient will have to follow the instructions to access the message inside a secure portal.

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:
Encryption: process of encoding a message so that it can be read only by the sender and the intended recipient.

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