Division of
Information Technology

Texas A&M University

Electronic Protected Health Information SECURE EMAIL TRANSMISSION Control

Table of Contents

Purpose

The purpose of the control is to ensure any external emails containing Electronic Protected Health Information (ePHI) are transmitted securely with encryption to the intended recipients. The Secure Email Transmission Security Control is intended to assist employees of TAMU in applying the required safeguard when emailing ePHI.

Scope

This control applies to all TAMU workforce members including, but not limited to full-time employees, part-time employees, trainees, students, providers, volunteers, contractors, temporary workers, and anyone else granted access to ePHI by TAMU. More specifically, this control applies to employees of TAMU that have the authority to process ePHI information. This control also applies to all email systems which process, store or transmit ePHI information.

HIPPA Safeguard: 45.CFR.164.312 (e)

Roles and Responsibilities

The Chief Information Security Officer (CISO), or delegate will be responsible for ensuring the implementation of this control. There are no exceptions granted to this HIPAA Security Control.

Security Control

All TAMU email systems that transmit ePHI externally must provide the email users a secure-email feature that encrypts the body and attachments of email at the level of encryption required by the “ePHI Encryption and Decryption Control” to reduce the risk for unauthorized access to ePHI and other sensitive information when it is transmitted.

ePHI users should always know who is authorized to receive the ePHI they work with. If an email user is uncertain the unit privacy point of contact should maintain an authorized list.

Forwarding email messages containing ePHI externally without encryption is not permitted.

Message received from outside TAMU that contain PHI must have any replies encrypted.

There should be an external recipient automatic email return read receipting to ensure the message reached the appropriate email account.

Any messages that are sent without encryption must be reported in the Unit’s “Inadvertent Disclosure of ePHI Via Email” form found in the related security control.

For any TAMU Hybrid Entity health care component that use an external email system or have threat or spam protection there must be Business Associate Agreement with the vendor providing the service

Procedure(s)

Both annual HIPAA and email user education must include instruction of how to encrypt message and a self-service knowledgebase article.

Encryption Methods – The following methods may be used to encrypt ePHI that is transmitted over untrusted networks.

- EMAIL ENCRYPTION – Emails transmitted from TAMU.EDU (or other TAMU managed domains) addresses containing ePHI to external email accounts must have their message body and attachments encrypted. Acceptable methods are:
    - Using TAMU Division of IT secure email solution.
    - S/MIME with recipient certificate enabled for encryption to organizations with documented key escrow practices.
    - Pretty Good Privacy/ GNU Privacy Guard encryption (PGP/GPG) to a recipient(s) with current enabled encryption key with documented key escrow practices.

External transmission of emails with ePHI transmission must have the email software configured to either automatically confirm the intended recipient received the email via a notification email, or a tracking digest. If neither is automatically available via the security method configuration then the sender must use “Return Receipt” on email with ePHI.

The procedure in the related ePHI security control, “Inadvertent Disclosure of ePHI via Email” to an external recipient(s) in error must be followed upon discovery.

Contact and Questions

Please send all inquiries to: *ra@tamu.edu*