

Texas A&M University

Electronic Protected Health Information INADVERTENT DISCLOSURE OF ePHI VIA EMAIL Control

Table of Contents

Purpose	1
Scope	1
Roles and Responsibilities	1
Security Control	2
Procedure(s)	2
Contact and Questions	2

Purpose

The purpose of the control is to ensure the tracking and reporting of inadvertent disclosures of electronic Protected Health Information (ePHI) that occur although reasonable technical safeguards are in place. This control only applies when either a single email containing ePHI are sent in error to an incorrect recipient(s), discovered as an error, successfully recalled or acknowledged as deleted. Although limited in nature, this is not considered HIPAA incidental use.

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.

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

TAMU maintains reasonable and appropriate technical safeguards to ensure email containing ePHI can be encrypted and have return receipt. If emails are either sent externally without encryption or to an incorrect recipient they must be recalled, have validated removal, and tracked with an annual report to the TAMU HIPAA Privacy Officer.

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.

Procedure(s)

Upon discovery that an email with ePHI was sent to an incorrect recipient it is to be recalled. Since emails sent within the same email system this prevents further disclosure on same email thread by reply. For incorrect external recipients not on the same email system an email recall only flags the attempt to recall was made but will cannot truly recall the email.

The external incorrect recipient(s) should be contacted and told the email was in error and must acknowledge in a separate email that the email was deleted unread. If they have read the email and forwarded it on to others the TAMU HIPAA Privacy Officer must be contacted immediately.

Any messages that are sent without encryption must be reported in an “Annual Inadvertent Disclosures of ePHI Via Emails” form maintained by the unit. This form must contain:

- Date and time of email disclosure
- Date and time error was discovered
- Email sender
- Name of email address(es) of incorrect recipient(s)
- Brief description of ePHI in the email
- Date and time of recall message
- Date and time of external recipient(s) acknowledgement of deletion.

There must be an annual calendar year accounting of any inadvertent email errors. By January 15th of each year the unit must send a copy of the final prior year’s “Inadvertent Disclosures of ePHI Via Email” form to the TAMU HIPAA Privacy Officer.

Contact and Questions

Please send all inquiries to: ra@tamu.edu