Division of
Information Technology

Texas A&M University

Electronic Protected Health Information ROLE BASED ACCESS AND ACCESS ANNUAL REVIEW Control

Table of Contents

Purpose

The purpose is to ensure units have Electronic Protected Health Information (ePHI) procedures that only authorize access based on the job role of the requestor and the access is reviewed at minimum annually.

Scope

This policy applies to TAMU in its entirety, including all systems that process sensitive information.
HIPPA Safeguard: 45.CFR.164.308 (a)(4) Information Access Management

Roles and Responsibilities

TAMU units acting as Health Care Components will clearly identify and document:

- Information assets (devices, interfaces, applications, and datasets) that have ePHI.
- The information asset access protection mechanisms in place. This includes both logical and physical access.
- That unique user access and password management is in place on all logical information assets containing ePHI.

- That physical access controls are in place for the information asset physical location.
- That all ePHI access is be authorized by the Information Owner or their designee based upon requestor role.
- At least annually a review all access information to reaffirm the access is still required. A separation of roles should be considered between the person(s) undertaking the access review and those whose access is being reviewed.

Security Control

All TAMU information assets containing ePHI must have unique authentication granting access to ePHI based on the job role of the personnel. This includes physical access authorizations for where the information asset is physically stored (for example, either card-key or a physical key control system). For logical ePHI access, password management must be part of the authentication.

The authorization of all access must come from the unit information owner or designee and be based on concept of least privilege: allowing only authorized access and privilege for users which are necessary to accomplish assigned task in accordance with their role or business function.

All ePHI access must be reviewed and re-authorized annually and a record maintained.

All records of granting access, reaffirmation, or modification of access must be maintained for six (6) years following the termination of access and/or removal of the information asset ePHI.

Procedure(s)

Units with ePHI to authorize access must utilize:

- Unit procedures to ensure all access, whether physical or logical, is authorized, reaffirmed annually, documented, and maintained at least six (6) years after discontinuation of access..
- Role-based access control based upon what is only necessary to job duties (least privilege).
- Separation of duties through role-based access when feasible https://cio.tamu.edu/policy/it-policy/controls-catalog/controls.php?control=AC-5
- Auditable log tracking for both logical access and modification at the individual user level of any EPHI database, dataset, file, or functional access. https://cio.tamu.edu/policy/it-policy/hipaa/pdfs/InformationSystemActivityReviewControl.pdf

Contact and Questions

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