Division of
Information Technology

Texas A&M University

Electronic Protected Health Information SECURITY INCIDENT REPORTING Control

Table of Contents

Purpose

This policy reflects TAMU's commitment to implement policies and procedures for detecting, reporting, and responding to security incidents involving electronic Protected Health Information (ePHI).

Scope

This policy applies to TAMU in its entirety, including all units as well as faculty and staff that utilize ePHI. In addition, some third parties, such as contractors or vendors, may be required to abide by parts of this policy if required by TAMU in a HIPAA Business Associate Agreement (BAA). For ePHI that is regulated by HIPAA (45.CFR.164. 308(a) (6) (i) Security Incident Procedures).

Roles and Responsibilities

Individual User Reporting Responsibilities

- When any individual observes or suspects the occurrence of an information security incident, they shall rapidly report the incident to:
    - appropriate personnel in the local unit
    - notify TAMU Help Desk Central: (979) 845-8300 or helpdesk@tamu.edu
      Or
    - emailing TAMU IT Security Operations at security@tamu.edu

- Interference with Reporting of Security Problems –Any attempt to interfere with, prevent, obstruct, or dissuade an employee in their efforts to report a suspected information security problem or violation is strictly prohibited. Any form of retaliation against an individual reporting or investigating information security problems or violations is also prohibited.

Priorities for handling information security incidents regarding ePHI are as follows:

- Protection of human life and safety.
- Protection of ePHI and any related TAMU RESTRICTED, CONFIDENTIAL, or CONTROLLED information.
- Compliance with applicable federal and state regulation concerning ePHI.
- Collection and analysis of information to determine if a computer crime or a violation of the TAMU Information Rules, SAPs, Security Controls, and Standards has occurred.
- Assurance that the confidentiality, integrity, and availability of ePHI is maintained.

Responding to Information Security Incidents – When a possible information security ePHI incident is reported to the TAMU Division of IT, the Division's Cybersecurity Incident Response Plan will be followed. This is in addition to any local unit IT incident response plan as required by TAMU Security Control IR-1, http://cio.it-test.tamu.edu/policy/it-policy/controls-catalog/controls.php?control=IR-1 .

Security Control

The HIPAA Security Rule defines a security incident as, "the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system."

Incidents are verified adverse events or situations that poses a threat to the integrity, confidentiality, or availability of information or systems. ePHI incidents may violate State and Federal Laws or Regulations. The direct result of information security incidents may include information disclosure, modification, destruction or denial of system services.

Indirect results of ePHI security incidents may include loss of ePHI, loss of computing capacity, violation of privacy, violation of HIPAA, civil lawsuits, loss of public confidence, or adverse consequences to other computing assets.

Without exception, all ePHI security incidents must be reported to the Division of IT.

Procedure(s)

The local unit incident response plan and the TAMU Division of Information Technology Cybersecurity Incident Response Plan must be followed.

Contact and Questions

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