Division of
Information Technology

Texas A&M University

Electronic Protected Health Information ENCRYPTION AND DECRYPTION Control

Table of Contents

Purpose

The purpose of the control is to implement a mechanism to encrypt and decrypt electronic Protected Health Information (ePHI). The Encryption and Decryption Security Control is intended to assist employees of TAMU in making a decision about the use of encryption technologies as a method of protecting data stored on systems that process 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 evaluate, purchase (or develop), and implement systems that store or process ePHI information. This control also applies to all systems, networks, and applications, as well as all facilities, which process, store or transmit ePHI information.

HIPPA Safeguard: 45.CFR.164.312 (a)(2)(iv) Encryption and Decryption.

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 will implement encryption controls to reduce the risk for unauthorized access to ePHI and other sensitive information when it is transmitted or stored on system, or an electronic portable media.

TAMU will identify members of the workforce, processes, and devices that require encryption capabilities and will implement those capabilities and test their proper functioning.

TAMU will protect encryption keys and only provide access to the encryption keys to members of the workforce whose job role requires knowledge of encryption keys.

Where appropriate, encryption should be used to protect the confidentiality, integrity, and availability of ePHI contained on TAMU computing systems. It is understood that the use of encryption implies that a reliable decryption method is employed

Procedure(s)

Information Asset Administrators shall ensure Encryption techniques are applied consistent with approved TAMU Information Security Policies and Procedures.

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.

- DATA ENCRYPTION – Data may be encrypted for transmission or storage using one of the following methods.
    - Proven encryption technologies that apply standard algorithms (i.e., AES, Blowfish, IDEA, RSA, RC5) may be used to protect data files. These algorithms represent the actual cipher used for an approved application (i.e. PGP, GPG, etc.). Proprietary algorithms are not considered an acceptable method for securing ePHI. Symmetric cryptosystem key lengths must be at least 256 bits, while asymmetric cryptosystem keys must be of a length that yields equivalent strength. Strong encryption hash should be used wherever possible.
    - When using zipped-file protection file, AES 256 level of encryption should be used. Password must be set to a minimum of 8 characters containing a

combination of upper case letter, lower case letter, number and or special character.
    - When communicating over the internet or over the network, TLS 1.2 or higher should be used where possible. Lowers level of encryption such as TLS 1.0 may be used when other risks have been identified and mitigated.
    - Secure FTP should be used instead of clear text based FTP communication.

- HARD DISK ENCRYPTION – The hard disk(s) of information assets may be encrypted using one of the following methods.
    - Full disk encryption technologies that apply standard algorithms (e.g. AES) to encrypt the entire hard disk, including the operating system, may be utilized. These solutions should employ pre-boot authentication and provide complete power off protection. Cryptosystem key lengths must be at least 256 bit encryption or above.
    - Virtual disk encryption technologies that apply standard algorithms (e.g. AES) to encrypt a portion of the hard disk may be utilized where full disk encryption would not be feasible. If virtual disk encryption is employed instead of full disk encryption, special attention should be paid to ensure that the operating system passwords for all users meet the guidelines outlined in TAMU Information Resource – Password Authentication http://rules-saps.tamu.edu/PDFs/29.01.03.M1.14.pdf . Cryptosystem key lengths must be at least 256 bit encryption or above is recommended.

- PORTABLE MEDIA ENCRYPTION – All portable media must be encrypted to protect ePHI.
    - Portable devices such as laptops, USB drives and CD's must be encrypted using AES 256 level encryption.

- WIRELESS ENCRYPTION – Encryption should be enabled for all Company wireless transmissions. The IEEE 802.11-2007 standard is the minimum acceptable level of acceptable conformance for wireless security architecture and encryption enabled on all such implementations. WPA2 is the most commonly utilized protocol that meets the standard.
- Where implementation of IEEE 802.11-2007 is not feasible, an application layer Virtual Private Network (IPSEC VPN or SSLVPN). A minimum 128-bit key strength should be implemented, and unique key encryption (per individual) should be implemented instead of shared key (one for everyone) encryption.
- Wireless user devices connecting to internal wireless networks must be authenticated via either a TAMU IT Identity Management NetID and password, a Health Science Center HSCID and password, a unique guest username and password, or active home institution's eduroam credentials.

Contact and Questions

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