Section:	Information Security	Effective:	March 2007
Standard:	Media Control Accountability	Revised:	
Policy Ref:	5.8.22 Data Media Control	Responsibility:	Chief Information Security Officer

MEDIA CONTROL (ACCOUNTABILITY) SECURITY STANDARD

Security Standards: are mandatory security rules applicable to the defined scope with respect to the subject.

Overview

According to the Health Insurance Portability and Accountability Act (HIPAA), 45 CFR 164.310(d)(2)(iii), relative to the University, departments that use, store, maintain, or are otherwise responsible for electronic protected health information (ePHI) must implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of a department, and the movement of these items within the department, and to maintain records of that movement. Additionally, the Gramm-Leach-Bliley Act (GLB) includes provisions to protect consumer's financial information collected by institutions that offer products or services to individuals. Also the Family Educational Rights and Privacy Act (FERPA) (34 CFR Part 99) protects the privacy of student education records under Federal Law. Risks are associated with the movement of any electronic sensitive information, such as: loss, theft, breaches, or financial penalties. Thus, this standard is mandatory for ePHI and recommended for all other electronic sensitive information (as defined in HOP 5.8.21 Data Classification).

Scope

All personnel responsible for managing Departmental data processing equipment with ePHI or other sensitive information, especially data owners and data custodians.

Purpose

The purpose of this document is to establish a standard for achieving accountability in protecting or tracking the movement of electronic sensitive information in to and out of a department, as well as the movement of these items within the department, and to encourage the encryption of sensitive information whenever possible.

Instructions

Each department must identify, and assign individual responsibility, for the movement and storage of its sensitive data. This should be formally documented within the department. Data owners are ultimately responsible, but may delegate responsibility to the individuals managing or using the electronic sensitive information.

Hardware/media Identification

Departments already have mechanisms in place for accountability of equipment (inventory management). Similarly, all mobile media used to store sensitive information must be identified and inventoried. Care should be taken when marking media so as not to draw undue attention. Detailed tracking records are required if the movement of electronic sensitive information cannot be encrypted.

ENCRYPTED *(recommended)*

Information Security strongly recommends encrypting sensitive data in motion. If sensitive information on mobile devices and/or mobile media is encrypted, it can be considered as meeting the confidentiality requirements of HIPAA, other Federal guidelines, and this standard. Care must be taken that media/devices do not contain the sole sources of information (that is, the original sensitive information must reside on another source and be recoverable in a timely manner). When information on mobile devices/or mobile media is not encrypted, it must meet the additional detailed document control mechanisms described below.

UNENCRYPTED *(not recommended)*

Moving sensitive information that is not encrypted should be avoided and encryption options always explored.

Handling Documentation

After unencrypted sensitive information and its respective owners, users, hardware, and media is identified, the department must develop and document the processes for handling its storage and transport. This documentation must be kept up to date and include:

- who is accountable,
- when and where the unencrypted sensitive information comes or goes,
- hardware on which it resides,
- how it is transferred, and
- to whom it was transferred.

Formal Procedures

Departments must comply with HOP requirements when formally establishing the devices they will use to store and transfer unencrypted sensitive information. Higher risk is associated with allowing personally-owned computers to store UTHSCSA sensitive information in an unencrypted format; for this reason, tighter controls are recommended. Unencrypted sensitive information should never be placed on devices and media outside the direct control of the department and for which the users cannot be held individually accountable.

Tracking Movement

Examples of sensitive data movement activities that must be tracked include:

1. Copying sensitive information to and from external media;
2. Copying sensitive information from external media to some other primary storage;
3. Introducing new external media or primary storage into the department;
4. Duplicating external media;
5. Transferring hardware in to and out of the department;
6. Creating and storing data backups; and
7. Moving equipment as part of maintenance.

Summary
Following these steps and closely maintaining documentation will greatly reduce the possibility of the loss or unauthorized modification to departmental sensitive information.

Refer to the Information Security web site (http://infosec.uthscsa.edu) for suggested log formats and other related Information Security Standards and Guidelines.

Exceptions

Exceptions to this standard are not applicable since the direction for accountability comes from multiple Federal requirements, including, but not limited to, HIPAA, GLB, FERPA, etc.