

HIPAA Security Rule Safeguards Recommended Standards

Developed by: USF HIPAA Security Team
May 12, 2005

INTRODUCTION

The Health Insurance Portability and Accountability Act (HIPAA) Security Rule, as a federal law, stipulates requirements and guidelines to safeguard the protection of Electronic Protected Health Information (ePHI). Within the HIPAA Security Rule are Required (R) and Addressable (A) Safeguards that must be part of the USF Covered Component policy structure. This document is meant to address this requirement.

PURPOSE

The purpose of this document is to establish standards which comply with the HIPAA Security Rule and will be used by the USF Covered Component and the Health Sciences Center (colleges of Nursing, Medicine and Public Health, and the USF Physician Group) to base computer and electronic information policies and procedures.

SCOPE

These standards apply to the Covered Component of the University of South Florida and to the Health Sciences Center (colleges of Nursing, Medicine and Public Health, and the USF Physician Group) as a whole, collectively the “USF Covered Component/HSC”. These standards apply to all individuals acting on behalf of the USF Covered Component/HSC, regardless of location, when performing academic, research, clinical or business functions.

Other Relevant Computer Policies

When interpreting these standards, existing computer and electronic information policies should be taken into consideration. Below are some examples:

USF Computer and Information Policies

The University of South Florida maintains computer and information usage policies that are relevant throughout the University of South Florida. These include, but are not limited to the following:

- **0-501 – Using and protecting information technology resources**
- **0-502 – Appropriate use of information technology resources**
- **0-508 – University information security structure**
- **0-511 - Securing Computer Accounts for Terminating Employees**

Health Sciences Center Computer Policies

The Health Sciences Center, composed of the three colleges of Medicine, Public Health and Nursing maintains the following existing computer policy & agreement:

- **HSC Computer Account Policy & Agreement**

STANDARDS

NOTE: These standards are organized under the structure of the Health Insurance Portability and Accountability Act Security, and are specifically written to provide guidance to the policies and procedures covering the USF Covered Component/HSC.

Administrative Safeguards

164.308(a)(1) – Security Management Process

- **Risk Analysis (R)** –The USF Covered Component/HSC shall conduct an initial risk analysis, and periodic analyses thereafter, to identify areas where Electronic Protected Health Information (ePHI) is stored throughout the USF Covered Component/HSC and determine any areas that are not compliant with HIPAA Security Rules. For each identified area of risk, the USF Covered Component/HSC shall determine whether the risk is acceptable, or whether to mitigate or transfer responsibility. The University HIPAA Security Officer convenes a “USF HIPAA Security Group” made up of representatives knowledgeable about the security practices of each area within the USF Covered Component/HSC, along with representatives from the University Research and Compliance Office, and other experts to review risk levels and recommend policy for University approval, as advised by General Counsel.
- **Risk Management (R)** – The USF HIPAA Security Officer works to establish training and monitoring procedures on compliance with HIPAA Security Rules, to be required for employees and other workforce members of the USF Covered Component/HSC and other appropriate university personnel. Certification/evidence of such training is to be kept as part of employees’ permanent record. Risk analysis shall be conducted periodically to review current HIPAA Security Rules with current USF Covered Component/HSC practices, identify new areas of risk, and to determine if current policy is adequate to meet HIPAA Security Rules for identified areas of risk.
- **Sanction Policy (R)** – Each policy or procedure covering an area of risk shall identify an appropriate sanction for initial or repeated violation, and shall identify the responsible authority for enforcement. The designated USF HIPAA Security Officer is responsible for identifying violations of the University’s HIPAA Security related policies and shall provide a report with recommendations for corrective actions and sanctions to appropriate authorities for implementation. Sanctions should be enforced uniformly across the USF Covered Component/HSC.

164.308(a)(2) – Assigned Security Responsibility (R)

The University shall maintain a designated USF HIPAA Security Officer to oversee the application of the HIPAA Security Rules. This person has responsibility and authority to apply HIPAA Security requirements throughout the University. The USF HIPAA Security Officer is to have thorough knowledge of the USF Covered Component/HSC computer systems and working environments.

The USF HIPAA Security Officer should maintain and chair a USF HIPAA Security Group, made up from representatives of the USF Covered Component/HSC. It is advisable that this group be a subgroup within the existing HSC Professional Integrity Council. The USF HIPAA Security Group's charge would be to continually monitor and revise standards, policies and procedures related to the HIPAA Security Rule.

164.308(a)(3) – Workforce Security

- **Authorization and/or Supervision (A)** – The USF HIPAA Security Group identifies “ePHI locations” and the associated “knowledgeable persons” responsible for developing, with approval by the HIPAA Security Officer, and managing procedures for supervision and/or authorization of workers in the “ePHI locations” to ensure security of ePHI is maintained.
- **Workforce Clearance Procedures (A)** – The USF HIPAA Security Group reviews position descriptions of all workers within the USF Covered Component/HSC and designates the level of access to ePHI that is appropriate for completing the assigned duties. This designation is to be indicated in the updated position descriptions. This review/updating process should involve the USF and USFPG Human Resources Departments along with the departmental heads throughout the USF Covered Component/HSC. The University shall develop an accompanying procedure requiring designation of ePHI access rights to be included in all position descriptions for USF Covered Component/HSC workforce members.
- **Termination Procedures (A)** – The USF HIPAA Security Group should periodically reviews current procedures for terminating access to ePHI when a individual member leaves the USF Covered Component/HSC. These procedures are updated, if needed, to ensure that the respective department management, along with HSC and USFPG IS and HR Departments coordinate appropriate termination of computer access including revoking passwords; disabling accounts; and retrieval of keys and USF/USFPG identification badges, and other building access devices. Consideration is given to the timing of these actions in connection with advance notice of termination and any associated risk of security breaches.

Every effort should be made to utilize existing University procedures and processes for identifying computer access terminations/modifications. It is felt that the reduction in processes to identify terminated/modified individual's status for computer access would strengthen the validity of such a process.

164.308(a)(4) – Information Access Management

- **Isolating Health Care Clearinghouse Function (R)** – Although University Medical Services Association (UMSA) does not meet the HIPAA definition of a Health Care Clearinghouse (and therefore this requirement is not applicable), the control and function of processing health insurance claims shall reside solely within UMSA.
- **Access Authorization (A)** – Access to all general computer systems and resources shall require, at minimum, the authorization of a designated department or higher authority, which shall approve security rights or modifications to those rights. For computer applications that maintain confidential information, the approval process should include both departmental (or higher) approval, along with approval from the designated business system owner(s). The authorization process is to be recorded for future reference. *Note: The business system owner(s) is defined as the person or persons that have assigned responsibility for the information within the computer application in question. Every computerized business application shall have a designated owner(s).*
- **Access Establishment and Modification (A)** – See *Access Authorization* above.

164.308(a)(5) – Security Awareness Training

- **Security Reminders (A)** –
 - All employees (Faculty, Staff, and Residents) and students, as well as all authorized HSC computer account holders, are required to satisfactorily complete computer security awareness training that includes HIPAA security issues. HIPAA security training should not be an isolated training event, but incorporated into an overall computer and information security training plan.
 - A process shall be developed for sending periodic reminders to the USF Covered Component/HSC community about HIPAA security issues.
 - Consideration is to be given to incorporating an ongoing education and verification process into the performance evaluation process.
- **Protection from Malicious Software (A)** – (See *Security Reminders* above)
- **Log-in Monitoring (A)** – (See *Security Reminders* above)
- **Password Management (A)** – (See *Security Reminders* above)

164.308(a)(6) – Security Incident Procedures

- **Response and Reporting (R)** – A formal process for identifying, recording and tracking of security incidents is to be developed and maintained. The HSC Information Services department shall be the owners of this process. Said process is to be used for tracking all electronic security events. Security “Events” are defined as reported, identified or potential electronic security exposures, threats or incidents. Events which relate to

disclosure or potential disclosure of ePHI shall be brought to the immediate attention of the USF HIPAA Security Officer.

164.308(a)(7) – Contingency Plan

- **Data Backup Plan (R)** – All electronic systems that maintain ePHI (with the exception of eMail, see below) shall be backed up on a nightly schedule. While the business clinical systems are of primary concern, it is however also important to backup all ePHI wherever it is maintained. All ePHI is to be stored on central USF Covered Component/HSC business servers for the purpose of benefiting from scheduled data backup processes. The USF Covered Component/HSC should maintain a business contracts with professional data backup storage providers to provide safe off-site storage with scheduled data pickups.

While eMail systems are backed up solely for the purpose of daily business recovery, for a variety of business and technical reasons there is no current process to archive eMail. Therefore, it is necessary to place the burden upon the individual users to maintain backup copies of eMail containing ePHI in accordance with USF Covered Component/HSC records retention policies. In order for individuals to backup their own eMail they should either perform this task themselves or place the necessary eMail onto servers that are backed up on a regular schedule.

- **Disaster Recovery Plan (R)** – All USF Covered Component/HSC business units that maintain computer systems that may contain ePHI, including but not limited to HSC Information Services and USFPG Information Technology, must maintain a formal Disaster Recovery Plan. Said plan should include recovery procedures for data and software, equipment replacement, necessary technical information for servers/routers/firewalls/switches/etc., critical contact list, relocation plans and other elements necessary to recover.
- **Emergency Mode Operation Plan (R)** – A major emphasis of HIPAA is to address the availability of ePHI to address situations when access to it is critical to providing health care to the patient. It is therefore required that the HSC Information Services and the USFPG Information Technology department maintain an Emergency Mode Operation Plan for critical clinical systems. Said plans shall address how access to ePHI data can continue in situations where normal operation has been disrupted. The plan shall address situations that can be reasonably foreseen.
- **Testing and Revision Procedure (A)** – In order to assure that the Disaster Recovery and Emergency Mode Operation Plans are adequate and up to date, they shall be periodically updated and revised. Both plans are to be reviewed and updated yearly, and recovery processes and procedures should be tested regularly.
- **Application and Data Criticality Analysis (A)** – The USF Covered Component/HSC shall identify electronic business systems that are critical to Health Care delivery and

processing. Special emphasis shall be placed on these systems in regards to contingency planning and recovery.

164.308(a)(8) – Evaluation (R)

The Health Sciences Center Information Services department performs on-going surveillance of the HSC Network and devices attached to that network. The goal of this effort is to identify vulnerabilities and possible breaches in security and/or policy violations. In addition, the USF Covered Component/HSC shall perform periodic analysis of security threats and risk. Information gathered will be used to continually revise and upgrade necessary requirements and procedures dealing with information security.

To achieve the above, the USF HIPAA Security Officer and the USF HIPAA Security Group shall provide:

- Oversight of policy and program development with the goal of high level of performance-compliance.
- Regular checks for changes in applicable federal law, standards, rules, etc.
- Periodic review of electronic systems' security, including on-site visits and/or audits of clinical, academic, administrative, and research processes
- Maintain records of required education and compliance requirements
- Periodic security incident review
- Periodic reports to of computer security & HIPAA Security Rule issues

164.308(b)(1) – Business Associate Contracts

- **Written Contracts or other Arrangements (R) –**
 - The current Business Associate Agreements managed by the HSC Professional Integrity Office shall be updated, as necessary, to address the HIPAA Security Rules.
 - The USF HIPAA Security Group shall identify any other arrangements that require contracts in compliance with the HIPAA Security Rule, and complete such.
 - The USF HIPAA Security Group shall develop a process and procedures for ongoing identification of arrangements that require contracts in compliance with the HIPAA Security Rule, and completing such.

Physical Safeguards

164.310(a)(1) – Facility Access Controls

- **Contingency Operations (A) –** In the event of a disaster, certain individuals must have access to facilities to minimize losses and restore business functions. These individuals may require physical access outside of normal working hours. It is the responsibility of the USF HIPAA Security Officer to assist in identifying those individuals who will need access to the facility in the event of a disaster, and to facilitate the delivery of appropriate

keys, codes, etc. to allow such access. This information is to be provided to appropriate building management and university authorities as part of a Business Continuity Plan.

- **Facility Security Plan (A)** – It is the responsibility of the USF HIPAA Security Officer to assist in identifying those individuals that will need after hours access to facilities and locked equipment rooms within the USF Covered Component/HSC, that contain or provide access to ePHI.
- **Access Controls and Validation Procedures (A)** – Unauthorized individuals are not permitted to have access to areas of a facility that allow access to ePHI. Prior to entry into a defined physical location or facility where ePHI is stored, maintained, or transmitted, all visitors are required to obtain appropriate authorization to be present within the physical location or facility. Authorization for minimum access to a facility may be provided through the use of identification badges, sign-in sheets, keys, escorts, or other methods approved by the USF HIPAA Security Officer. Any individual witnessing a visitor attempting to gain access to ePHI should immediately report such activity to the USF HIPAA Security Officer, or other designated personnel.
- **Maintenance Records (A)** – The USF HIPAA Security Officer is responsible for overseeing documentation of any maintenance that is performed on a USF Covered Component/HSC facility that may impact security of the facility. Some of the items that should be documented include repair or replacement of doors, windows, walls or locks within the facility. All facilities that store, maintain, or transmit ePHI must retain maintenance records. This information shall be documented as deemed appropriate by the USF HIPAA Security Officer.

164.310(b) – Workstation Use (R)

To the extent reasonable, workstation screens shall be turned away from visitors and other unauthorized persons or covered with a privacy screen. Employees shall log off of a workstation if leaving it unattended for any significant period of time. If used for creating, transmitting or storing USF Covered Component/HSC ePHI, portable workstations, such as laptops, notebooks, or PDA type devices, even if personally owned, shall be kept in a secure manner so that others do not have access to ePHI. For workstations in high traffic areas (such as in a hallway or patient/exam room) employees and students are responsible for securing the workstation before leaving the device unsupervised for any period of time. All computers physically connected to the HSC/USFPG networks are set up to provide login to the network domain to allow implementation of applicable security settings, and appropriate updating of the operating system, applications and virus protection software.

164.310(c) – Workstation Security (R)

See above

164.310(d)(1) – Device and Media Controls

- **Disposal (R)**
- **Media Re-use (R)**

- **Accountability (A)**
- **Data backup and storage (A)**

All disks, tapes, DVD/CD's, memory sticks/keys and other data storage media that may contain ePHI shall be erased prior to reuse and destroyed or erased prior to disposal. Prior to disposal, hard drives must be destroyed or erased with a program deemed to be acceptable by the USF HIPAA Security Officer. If equipment is transferred to another University/USFPG department, then all data shall be removed from the equipment prior to the transfer.

The USF HIPAA Security Officer or designee is responsible for keeping an audit list of all network attached devices. This list is kept in whatever format deemed appropriate.

Technical Safeguards

164.312(a)(1) – Access Control Mechanisms

- **Unique User Identification (R)** – All computer accounts within the USF Covered Component/HSC shall be uniquely assigned to a single individual, to ensure the ability to audit user access to information and resources. Individuals shall not allow the sharing of computer account/passwords, and shall not allow department-level or other multi-individual generic accounts. In cases where other auditable processes are in effect to track ePHI access, a computer account may be assigned, as approved by the USF HIPAA Security Officer, to a unique resource (i.e., individual workstation or internal computer application used to access multiple resources requiring distinct authentication).

Passwords are to consist of at least six characters, and should include alpha, numeric and special characters in order to prevent unauthorized password use or password guessing.

In the specialized cases of a “common area” computer, like a nurse’s station, where multiple users will need constant access to one workstation, steps should be taken to ensure that users are required to log into applications even if they are not required to log into a network or domain. Further, the users must be advised and trained that immediate logouts from applications are required to prevent unauthorized access and ensure audit trail integrity. These workstations should still employ screen savers to blank out potential information on the screen.

- **Emergency Access procedure (R)** - In the case of emergency, a computer account may be temporarily shared with another individual. The requirements for emergency access sharing are: there must be a true emergency, the sharing must be temporary, and the emergency incident must be reported to the managing authority of the computer account being shared. In no case should this emergency access sharing exceed 30 days.

The Emergency access procedure must be used in the case a terminated employee’s computer account must be maintained for business reasons. Unless the Emergency Access procedure is implemented, all terminated employee computer accounts will be deleted immediately upon notification of the termination to all relevant parties.

- **Automatic Logoff (A)** - While automatic logoff may not currently be technically possible, automatic screen blanking of a workstation after a period of inactivity is required.
- **Encryption and Digital Signatures (A)** - All USF Covered Component/HSC remote users use the appropriate (e.g. SecuRemote) VPN client to connect to the HSC network from any external location. The only exception to this policy is accessing applications that use an acceptable alternative encryption method, such as SSL/HTTPS. All communication between USF Covered Component/HSC network resources and remote sites is to be encrypted, and such encryption is selected and maintained by appropriate USF Covered Component/HSC information services representatives.

164.312(b) - Audit Controls (R)

Audit Controls for network, server and business systems should be implemented and used within the USF Covered Component/HSC. The USF Covered Component/HSC should implement hardware, software, and/or procedural mechanisms that record and examine activity in information system networks that contain or use ePHI. These include, but are not limited to, user and administrator account activity audits, workstations or other devices attached to the network, identifying and securing computers that access ePHI, installing secure network infrastructure devices: routers, switches, servers, and securing and managing hosts (multi-user systems or “servers”). Host systems should be managed based upon USF and HSC Standards and Guidelines for the specific platform.

164.312(c)(1) – Integrity Control Mechanism (A)

The USF Covered Component/HSC shall maintain mechanisms to protect data from improper alteration or destruction. These mechanisms include the following:

- **Server Hardware parameters:** redundant hard disks or Redundant Arrays of Inexpensive Drives (RAID). Redundant hot swappable components such as fans and power supplies, redundant Network Interface Cards (NICs). Error correcting memory is also recommended.
- **Environment parameters:** all multi-user or server systems shall be backed with UPS power, and designated air conditioning systems. Systems should be on dedicated electrical circuits
- **Software file integrity:** checksum based Host Intrusion Systems are recommended, and file logs shall be used where feasible. At minimum, the USF Covered Component/HSC shall require error and exception reporting as a functional minimum.
- **Digital signatures,** with time and date stamps, on files are recommended, but not required.

164.312(d) – Authentication Control Mechanism (R)

All computer accounts shall have properly constructed passwords, and passwords shall be kept confidential and known only to the assigned user. USF Covered Component/HSC computer

account users are required to change their passwords every 90 days, and shall keep any written passwords in a secure location.

164.312(e)(1) Transmission Security Mechanisms

- **Integrity Controls – (A)** - The USF Covered Component/HSC shall protect ePHI transmissions by using Public Key Infrastructure whenever feasible. The USF Covered Component/HSC shall use a certification process whenever healthcare or insurance records are transmitted across the Internet.
- **Encryption Controls – (A)** - All encryption shall be at an AES (Advanced Encryption Standard or 256 bits) level. In cases where this is not possible 3DES or Blowfish are acceptable. In all cases AES is the preferred method. Note that the USF Covered Component/HSC considers NAT (Network Address Translation) a subset of IPSEC and is therefore an additional security process, but not a substitute for AES. Because of the prevalence of NAT in some areas, the USF Covered Component/HSC has adopted ESP (Encapsulation Security Payload-transport mode) as the acceptable method for encapsulation.