INFORMATION TECHNOLOGY HIPAA SECURITY RULE

Faculty and Staff Training

UNIVERSITY OF
South Carolina

School of Medicine Columbia

HIPAA SECURITY RULE
AGENDA

- What is the HIPAA Security Rule
  - Authority
  - Definition
  - Scope
- Requirements
  - Administrative
  - Physical
  - Technical
  - Individual Responsibilities
  - Education
  - Security Consciousness
  - Reporting
  - Sanctions

INFORMATION TECHNOLOGY SECUIRTY

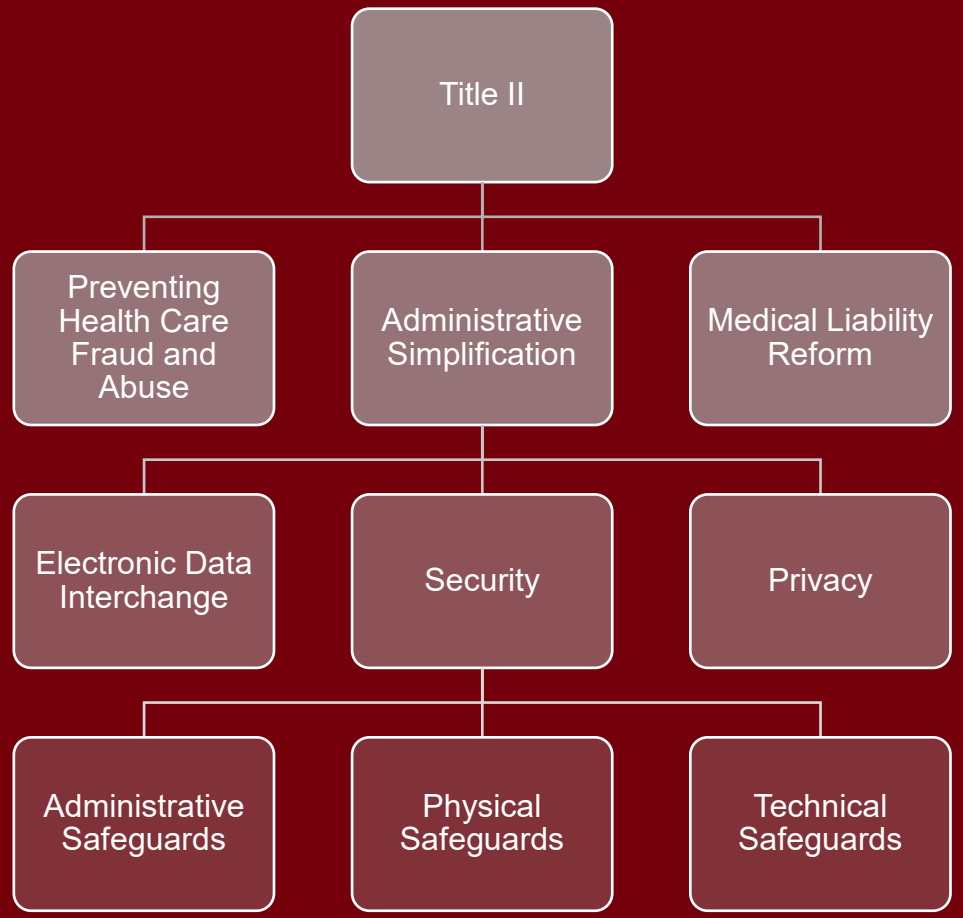
NATIONAL INSTITUE OF STANDARDS AND TECHNOLOGY

NIST SP 800-70: Security Configuration Checklists Program for IT Products.

"High Security: A High Security Environment is at high risk of attack or data exposure, and therefore security takes precedence over usability. This environment encompasses computers that are usually limited in their functionality to specific specialized purposes. They may contain highly confidential information (e.g. personnel records, medical records, financial information) or perform vital organizational functions (e.g. accounting, payroll processing, web servers, and firewalls)."

HIPAA

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996



HIPAA SECURITY STANDARDS

WHAT IS THE SECURITY RULE

- Legislation designed to protect the confidentiality, integrity and availability of electronic protected health information (ePHI)
- Deadline for compliance April 20th, 2005
- Comprised of three main categories of “standards” pertaining to the administrative, physical and technical aspects of ePHI
- Applies to the security and integrity of electronically created, stored, transmitted, received or manipulated personal health information

HIPAA SECURITY STANDARDS

WHAT IS THE SECURITY RULE

Bottom Line:

- We must assure that systems and applications operate effectively and provide appropriate confidentiality, integrity and availability of information.
- We must protect information commensurate with the level of risk and magnitude of harm resulting from loss, misuse, unauthorized access or modification.

HIPAA SECURITY STANDARDS

Definitions

Confidentiality: "the property that data or information is not made available or disclosed to unauthorized persons or processes."

Must protect against unauthorized:

- Access
- Uses
- Disclosures

HIPAA SECURITY STANDARDS
DEFINITIONS

Integrity: "the property that data or information has not been altered or destroyed in an unauthorized manner."

- Must protect against improper destruction or alteration of data
- Must provide appropriate backup in the event of a threat, hazard or natural disaster

HIPAA SECURITY STANDARDS
DEFINITIONS

Availability: "the property that data or information is accessible and usable upon demand by an authorized person."

- Must provide for ready availability to authorized personnel
- Must guard against threats and hazards that may deny access to data or render the data unavailable when needed
- Must provide appropriate backup in the event of a threat, hazard, or natural disaster
- Must provide appropriate disaster recovery and business continuity plans for departmental operations involving ePHI

HIPAA SECURITY STANDARDS

WHAT CONSTITUTES PHI – EIGHTEEN IDENTIFIERS

- Name
- Address – street, city, county, zip code (more than 3 digits) or other geographic codes
- Dates directly related to patient
- Telephone Number
- Fax Number
- Email Address
- Social Security Number
- Medical Record Number
- Health Plan Beneficiary Number
- Account Number
- Certificate/License Number
- Any vehicle or device serial number
- Web URL, Internet Protocol (IP) Address
- Finger or voice prints
- Photographic images
- *Any other unique identifying number, characteristic or code (whether generally available in the public realm or not)*
- *Age greater than 89 (due to the 90 years old and over population is relatively small)*

HIPAA SECURITY STANDARDS
DEFINITIONS

ePHI: data in an electronic format that contains any of the 18 identifiers

This may include but is not limited to the following:

- Data stored on the network, internet or intranet
- Data stored on a personal computer, tablet, smart phone, etc.
- Data stored on USB keys, memory cards, external hard drives, CDs, DVDs, digital cameras/camcorders, etc.
- Data stored on your HOME computer
- Data utilized for research

HIPAA SECURITY STANDARDS
ADMINISTRATIVE SAFEGUARDS

Administrative Safeguards – "Administrative actions, policies, and procedures to manage the selection, development, implementation, and maintenance of security measure to protect ePHI and to manage the conduct of the covered entity's workforce in relation to the protection of that information."

Bottom Line:

- USC School of Medicine has adopted policies and procedures to control access to ePHI
- Each employee, faculty, resident, student and volunteer must be familiar with these policies and procedures at the institutional and departmental levels

HIPAA SECURITY STANDARDS

ADMINISTRATIVE – ACCESS

- Access to ePHI is granted only to authorized individuals with a "need to know"
- SOM computer equipment should only be used for authorized purposes in the pursuit of accomplishing your specific duties
- Installation of software without prior approval is prohibited
- Disclosure of ePHI via electronic means is strictly forbidden without appropriate authorization
- Do not use computer equipment to engage in any activity that is in violation of the SOM/USC policies and procedures or is illegal under local, state, federal or international law

HIPAA SECURITY STANDARDS

ADMINISTRATIVE – ACCESS

- USC SOM will monitor logon attempts to the network
- Access to the SOM network will be monitored
- Inappropriate logon attempts should be reported to the respective departmental level security designee
- All USC SOM computer systems are subject to audit

HIPAA SECURITY STANDARDS

ADMINISTRATIVE – ACCESS

- All computers should be manually locked, logged off of or shut down when left unattended even for a short period of time
- A quick way to lock a computer is the keyboard shortcut: Windows key + L
- All computers must employ whole-drive encryption
- Desktop computers which are located in vulnerable locations must be physically secured as appropriate

HIPAA SECURITY STANDARDS

ADMINISTRATIVE – ACCESS

- You must access School of Medicine information utilizing YOUR username and password – *****NO PASSWORD SHARING*****
- You are personally responsible for access to any information utilizing your account credentials (user name and password)
- You are subject to disciplinary action if information is accessed inappropriately utilizing your credentials

HIPAA SECURITY STANDARDS

ADMINISTRATIVE – PASSWORDS

- Your user ID and password are critical to ePHI security
- Maintain your password in a secure and confidential manner
  - DO NOT keep an unsecured paper record of your passwords
  - DO NOT post your password in open view e.g. on your monitor
  - DO NOT share your password with anyone
  - DO NOT use the same password for USC SOM and your personal accounts
  - DO NOT include passwords in automated logon processes
  - DO NOT use "weak" passwords

HIPAA SECURITY STANDARDS

ADMINISTRATIVE – PASSWORDS

- Passwords must be changed every 90 days
- Passwords should be changed whenever there is a question of compromise
- Strong passwords:
  - Are a minimum of 8 characters in length
  - Contain at least one of each of the following:
    - Uppercase letter
    - Lowercase letter
    - Number
    - Special Character

HIPAA SECURITY STANDARDS
ADMINISTRATIVE – PASSWORDS

Password Examples:

- Use an entire passphrase instead of a password (recommended):
  - I like 2 play with computers!

- Shorten a passphrase into a password:
  - "I wish these silly passwords would go away" becomes "1wt$pwga" after using the first letter of each word and substituted characters

HIPAA SECURITY STANDARDS
ADMINISTRATIVE – ACCESS

Termination and/or transfer procedures:

- Administrative directors are responsible for informing the appropriate IT administrator of changes in an employee's employment status
- Upon termination of employment all USC SOM network and PC access is terminated
- All ePHI and computer equipment (laptops, tablets, etc.) should be retrieved
- The use of a prior employee's user IDs and passwords is strictly forbidden
- "Generic" user IDs are strictly forbidden

HIPAA SECURITY STANDARDS

ADMINISTRATIVE - REMOTE ACCESS

- All ePHI stored or accessed remotely must be maintained under the same security guidelines as for data accessed within the USC SOM network proper
- This applies to home equipment and Internet-based storage of data
- All ePHI should be kept in such a fashion as to be inaccessible to family members or other unauthorized individuals
- Stored data should be appropriately encrypted
- Cloud storage of ePHI is strictly forbidden without prior approval (with the exception of your SOM OneDrive storage).

HIPAA SECURITY STANDARDS

ADMINISTRATIVE – MALICIOUS SOFTWARE

Malicious Software – pirated software, viruses, worms, trojans, spyware, and file sharing software e.g. BitTorrent

- All software installed on USC SOM equipment must be approved by the department chairperson, administrative director or their designee – typically the department level security officer
- Installation of software on USC SOM computers must be in compliance with USC software policy and applicable licensing agreements
- Installation of personal software or software downloaded from the internet is prohibited unless specifically approved by OIT

HIPAA SECURITY STANDARDS
ADMINISTRATIVE – MALICIOUS SOFTWARE

- Approved antivirus software must be installed and kept up-to-date on:
  - All USC computer systems
  - Home equipment utilized to access the USC SOM network
- Never disable antivirus software
- Suspicious software should be brought to the attention of the IT technical support personnel immediately

HIPAA SECURITY STANDARDS
ADMINISTRATIVE – MALICIOUS SOFTWARE

- Emails with attachments should not be opened if:
  - The sender is unknown to you
  - You were not expecting the email/attachment
  - The attachment is suspicious in any way
- Do not open non-business-related email attachments or suspicious URLs
- Do not open file attachments or URLs sent via non-approved platforms

HIPAA SECURITY STANDARDS

ADMINISTRATIVE – BACKUP AND RECOVERY

- A system must be in place to ensure recovery from any damage to computer equipment or data within a reasonable time period based on the criticality of function
- Each department must determine and document data criticality, sensitivity and vulnerabilities
- Each department must devise and document a backup, disaster recovery and business continuity plan
- Backup data must be stored in an off-site location
- Backup data must be maintained with the same level of security as the original data

HIPAA SECURITY STANDARDS

ADMINISTRATIVE – INCIDENT REPORTING

- All known and suspected security violations must be reported
- Security incidents should be reported to the departmental Administrative Director or their designee
- SOM IT personnel should be contacted immediately to initiate the appropriate investigative processes and to mitigate against any data loss or corruption
- Security incidents must be fully documented to include time/date, personnel involved, cause, mitigation and preventive measures

HIPAA SECURITY STANDARDS
ADMINISTRATIVE – ASSESSMENTS

- Site surveys will be required
  - On an annual basis to reassess compliance, risks and vulnerabilities
  - When a new type of threat emerges
- Backup, disaster recovery and business continuity procedures must be reviewed and tested to determine their adequacy
- Any changes or additions to departmental electronic assets (hardware, software, server or endpoint devices) must be made in conjunction with SOM IT personnel and after performance of a proper risk assessment

HIPAA SECURITY STANDARDS
PHYSICAL SAFEGUARDS

Physical Safeguards– "the security measures to protect a covered entity's electronic health information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion."

Bottom Line:

- Electronic assets must be protected from physical damage and theft

HIPAA SECURITY STANDARDS

PHYSICAL – MEDIA AND DEVICES

- All electronic devices containing ePHI should be secured behind locked doors or otherwise physically secured
- All applicable SOM electronic media containing ePHI should be marked as confidential and properly encrypted

HIPAA SECURITY STANDARDS

PHYSICAL – MEDIA AND DEVICES

- Special security consideration should be given to portable devices (laptops, smartphones, digital cameras, digital camcorders, external hard drives, CDs, DVDs, USB flash drives, memory cards, etc.) to protect against damage and theft
- At no time should PHI be stored on any mobile device unless the data is properly encrypted

HIPAA SECURITY STANDARDS

PHYSICAL – MEDIA AND DEVICES

- PHI must never be stored on mobile computing devices or storage media unless the following minimum requirements are met:
  - Power-on or boot passwords are utilized
  - Auto logoff or password protected screen savers
  - Encryption of stored data by acceptable encryption software approved by the IT Security Officer or designee e.g. BitLocker®, AxCrypt®, FileVault®

HIPAA SECURITY STANDARDS

PHYSICAL FACILITIES AND HIPAA

§ 164.310 Physical safeguards

A covered entity must, in accordance with § 164.306:

Access control and validation procedures (Addressable): Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control and control of access to software programs for testing and revision

Maintenance records (Addressable): Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors and locks)

HIPAA SECURITY STANDARDS

PHYSICAL FACILITIES

- ID badges should be worn at all times and should be clearly visible
- At no time should you open secured doors for unidentified individuals without proper identification

HIPAA SECURITY STANDARDS

PHYSICAL – FILE SERVERS

- File servers and other mass storage devices must be installed in access-controlled areas to prevent damage, theft and access to unauthorized personnel
- These areas must provide appropriate levels of protection against fire, water and other environmental hazards such as extreme temperatures and power outages/surges

HIPAA SECURITY STANDARDS

PHYSICAL – WORKSTATIONS

- Workstations must be positioned so as to avoid viewing by unauthorized personnel
- Use privacy screens where applicable
- Use automatic password protected screen savers
- Lock, logoff or shut down workstations when not attended
- Workstation access should be controlled based on job requirements

HIPAA SECURITY STANDARDS
PHYSICAL – NETWORK

- Additions to or alterations of the USC SOM network is strictly prohibited, including but not limited to:
  - Physical connections via wired or fiber optic means
  - Wireless connections
  - Configuration changes
  - Addition of routers, switches, or hubs (includes wireless routers)
- All wireless network communications require proper security protocols and encryption technology managed by the USC SOM OIT

HIPAA SECURITY STANDARDS

PHYSICAL – INFORMATION DISPOSAL

- Disposal of electronic data must be done in such a fashion as to ensure continued protection of ePHI
- Magnetic media must be erased prior to disposal or reuse with a degaussing device or approved software designed to overwrite each sector of the disk
- CDs and DVDs must be broken, shredded or otherwise defaced prior to being discarded
- All media containing ePHI must be disposed of in compliance with the SOM Electronic Data Disposal Policy

HIPAA SECURITY STANDARDS

PHYSICAL – INFORMATION TRANSFER

- Hard drives containing PHI sent to vendors outside of the USC SOM for data recovery or for warranty repairs require a Business Associate Agreement with the specified vendor
- The process must be coordinated through the OIT

HIPAA SECURITY STANDARDS

PHYSICAL – INFORMATION DISPOSAL

- Special attention should be given to copiers and other multifunction devices which contain internal data storage
- Such devices with internal storage must be properly disposed of when taken out of service, leasing contracts are retired or equipment is updated or replaced
- All such devices containing ePHI must be disposed of in compliance with the SOM Electronic Data Disposal Policy

HIPAA SECURITY STANDARDS
TECHNICAL

Technical Safeguards – "the technology and the policy and procedures for its use that protect electronic protected health information and control access to it."

Bottom Line:

- Technological solutions are required to protect ePHI where applicable
- Examples include data encryption and secure data transfer over the network

HIPAA SECURITY STANDARDS

TECHNICAL – NETWORK

- All wireless network communications require proper security protocols and encryption technology
- Wireless networking must be configured and managed by the USC SOM OIT
- All electronic transmission of the ePHI must be appropriately encrypted

HIPAA SECURITY STANDARDS

TECHNICAL – NETWORK

- PHI residing on any form of electronic media or computing device must be encrypted if stored or taken offsite e.g. USB devices, CDs, DVDs, external Hard Drives, etc.

- Encryption must be achieved through software approved by the SOM IT Department Security Officer or designee, e.g. BitLocker®, AxCrypt®, FileVault®

INFORMATION TEHCNOLOGY UPDATE

SUMMARY

- You are the most important component of IT security
- Be mindful of security requirements and your responsibility to protect proprietary and patient information
- Report any suspicious activities or concerns to the Office of Information Help Desk: (803) 545-5100
- Contact the Help Desk for any questions or assistance