Information Technology
HIPAA SECURITY RULE

Faculty and Staff Training

University of South Carolina
School of Medicine

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 Security

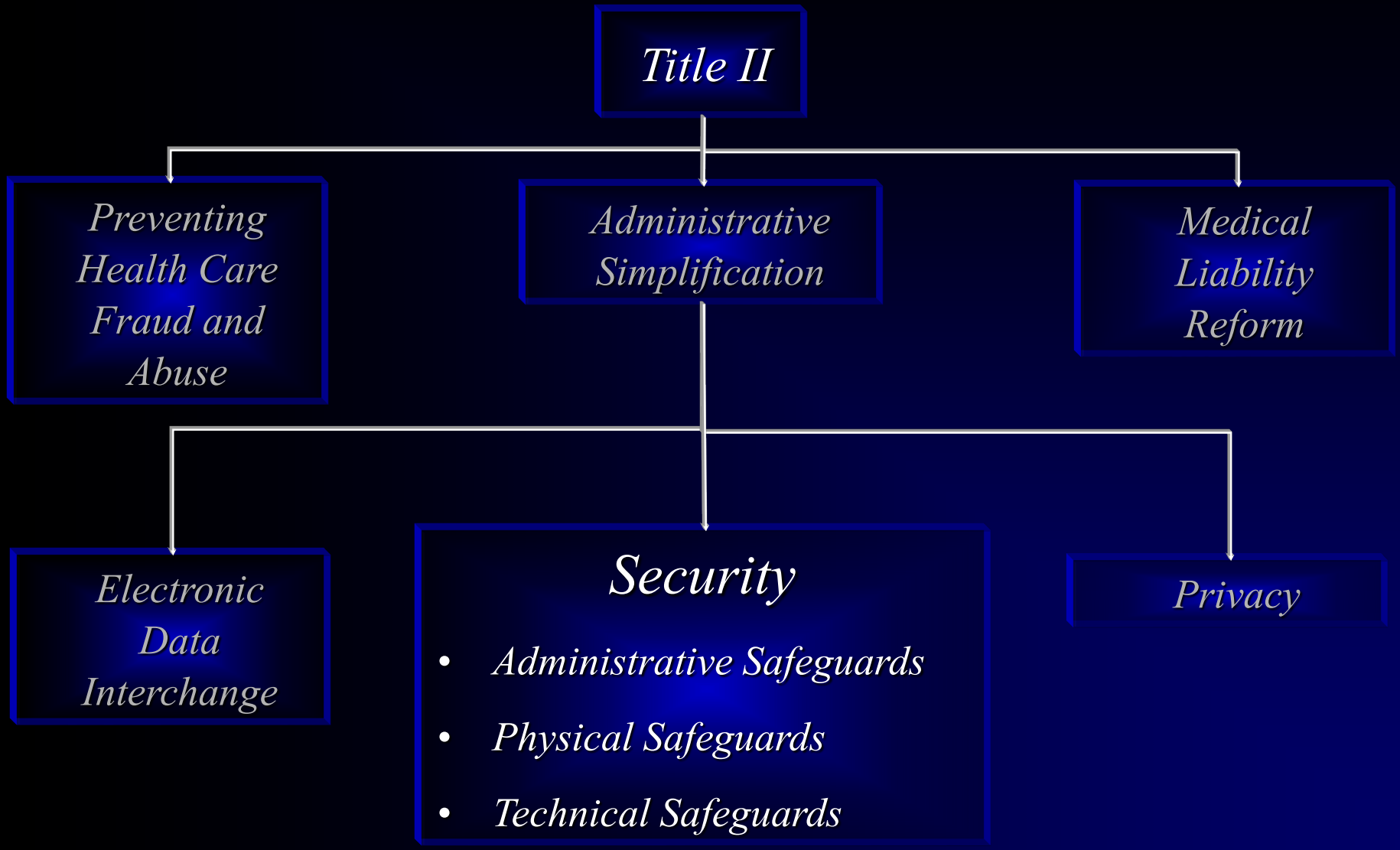
National Institute of Standards and Technology

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 address, city, county, zip code (more than 3 digits) or other geographic codes
- Dates directly related to patient
- Telephone Number
- Fax Number
- email addresses
- 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 year old and over population is relatively small)*

HIPAA Security Standards

Definitions continued…

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 or 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 measures 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 member, resident , student and volunteer must be familiar with these policies and procedures at the institution 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

- USCSOM 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 USCSOM 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 the computer is to type the “Windows” key + the “L” key.
- All laptop computers must employ whole-drive encryption.
- Desktop computers which are located in vulnerable locations must be whole-drive encrypted and physically secured as appropriate.

HIPAA Security Standards

Administrative - Access

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

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 passwords for USCSOM 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 must be utilized.
  - A minimum of 8 characters in length
  - Should contain a component from each of the 4 following categories
    - Upper case
    - Lower case
    - Numerals
    - Keyboard symbols

HIPAA Security Standards

Administrative – Passwords

Strong Password Examples:

- I like to play with computers 2!
  - Using the first letter of each word yields “Iltpwc2!”
- I wish these silly passwords would go away!
  - Using the first letter of each word and a $ symbol yields “I$wtsPwga!”
- Use a passphrase instead of a password.

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 USCSOM 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 USCSOM 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.

HIPAA Security Standards

Administrative – Malicious Software

Pirated software, "viruses," "worms," "Trojans," "spyware," and file sharing software e.g. Kazaa

- All software installed on USCSOM equipment must be approved by the department chairperson, administrative director or their designee – typically the department level security officer.
- Installation of software on USCSOM 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 anti-virus software must be installed and kept current on:
  - All USC computer systems.
  - Home equipment utilized to access the USCSOM network.
- Never disable anti-virus 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 web URLs
  - Do not open file attachments or URLs sent via instant messaging.

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.
- Security incidents must be fully documented to include time/date, personnel involved, cause, mitigation, and preventive measures.

Information Technology Security

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, and memory cards) 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

- Private Health Information 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®*.

Information Technology Security

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 USCSOM network is strictly prohibited. This includes:
  - 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 USCSOM Office of Information Technology.

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 with a degaussing device or approved software designed to overwrite each sector of the disk. This must be done prior to disposal or reuse.
- 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 the USCSOM for data recovery or for warranty repairs require a Business Associate Agreement with the specified vendor.
- The process must be coordinated through the Office of Information Technology.

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 USCSOM Office of Information Technology.
- All electronic transmission of ePHI must be appropriately encrypted.

HIPAA Security Standards

Technical – Network

- Private Health Information residing on any form of electronic media or computing device must be encrypted if stored or taken off-site 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 Technology

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: 545-5100
- Contact the Help Desk for any questions or assistance.