Security Rule for IT Staffs

J. T. Ash
University of Hawaii System
HIPAA Compliance Officer
jtash@hawaii.edu
hipaa@hawaii.edu

Disclaimer

- HIPAA is a “TEAM SPORT” and everyone has a role in protecting protected health information (PHI)
- This training only provides **“what”** needs to be done for Security Rule obligations, and not **“how”** you need to accomplish them. **“How”** is a risk-based collaboration between IT, Security, and Business.
- Information about HIPAA from the U.S. Department of Health and Human Services (HHS):
  - https://www.hhs.gov/hipaa/for-professionals/index.html
- Unofficial version from HHS combining all HIPAA regulatory standards in one document (115 pages):
  - https://www.hhs.gov/sites/default/files/hipaa-simplification-201303.pdf

HIPAA Privacy Rule

- The Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.
- https://www.hhs.gov/hipaa/for-professionals/privacy/index.html
- 45 CFR Part 160 and Subparts A and E of Part 164.

HIPAA Security Rule

- The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.
- https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html
- 45 CFR Part 160 and Subparts A and C of Part 164.
- Safeguards:
  - Administrative
  - Physical
  - Technical

Breach of Unsecured PHI

- **Notification to Individuals**: Individuals whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, used, or disclosed as a result of such breach must be notified without unreasonable delay and in no case later than 60 calendar days following the discovery of such breach.

- **Notification to Others**: A UH Covered Component shall also notify prominent local media outlets if the breach involves more than 500 residents of the State no later than 60 days after discovery of the breach.

- **Notification to DHHS Secretary**: A UH Covered Component shall notify the DHHS Secretary on an annual basis, in a manner specified on the DHHS Web site, and via a report due to the DHHS Secretary no later than 60 calendar days after the end of the calendar year in which breaches are discovered *if less than 500 individuals are involved*. *If more than 500 individuals are involved*, the UH Covered Component shall notify the DHHS Secretary in the manner provided by the DHHS Web site, which presently requires notice without unreasonable delay and in no case later than 60 days following a breach.

- **Notification by a Business Associate**. A Business Associate shall notify a UH Covered Component of a breach within 5 business days that the Business Associate discovered a breach occurred…

Mandatory Security Requirements

- Ensure the confidentiality, integrity, and availability of all its PHI;
- Protect against any reasonably anticipated threats or hazards to the security or integrity of the PHI, including ePHI;
- Protect against any reasonably anticipated uses or disclosures of PHI that are not permitted or required;
- Ensure compliance by its workforce.

Two types of Rule elements

1. Required standards
2. "Addressable" standards
   - CE must decide whether the standard is *reasonable and appropriate* to the local setting, and cost to implement
   - Can either
     - Implement the standard as published
     - Implement some alternative (and document why)
     - Not implement the standard at all (and document why)

Three Categories of Standards

- Administrative safeguards
  - Policies and procedures to prevent, detect, contain and correct information security violations
- Physical Safeguards
  - IT equipment and media protections
- Technical Safeguards
  - Controls (mostly software) for access, information integrity, audit trails

Administrative Safeguards

- Required
  1. Risk Analysis
  2. Risk Management
  3. Sanctions Policy
  4. Information System Activity Review
  5. Assigned Security Responsibility
  6. Isolating Health Care Clearinghouse Functions
  7. Security Incident Response & Reporting
  8. Data Backup Plan
  9. Disaster Recovery Plan
  10. Emergency Mode Operations
  11. Periodic Evaluations of Standards Compliance

Administrative Safeguards

- Addressable
  1. Workforce security authorizations
  2. Workforce clearance procedure
  3. Termination Procedures
  4. Information Access Authorization
  5. Access Establishment and Modification
  6. Security Reminders
  7. Protection from Malicious Software
  8. Log-in Monitoring
  9. Password Management
  10. Testing and Revision Procedures
  11. Applications and Data Criticality Analysis

Physical Safeguards

- Required
  1. Workstation Use
  2. Workstation Security
  3. Disposal of media
     - Deletion of PHI prior to disposal, or
     - Secure disposal so data is not recoverable
  4. Media Reuse
     - Deletion of PHI prior to re-use

Physical Safeguards

- Addressable
  1. Facility Contingency Operations
  2. Facility Security Plan
  3. Physical Access Control and Validation
  4. Facility Maintenance Records
  5. Device and Media Accountability
  6. Data Backup and Storage

Technical Safeguards

- Required
  1. Unique User Identification
     - No shared logins
  2. Emergency access procedures
  3. Audit controls
     - Logs of who created, edited or viewed PHI
  4. Person and/or Entity Authentication
     - No systems without access control

Technical Safeguards

- Addressable
  1. Automatic logoff
  2. Encryption
  3. Authentication of the integrity of stored and transmitted PHI

J. T. Ash
UH HIPAA Compliance Officer
jtash@hawaii.edu • (808) 956-7241