ADA Healthy Practice Webinar: HIPAA Security

Brandon T. Pauley, Esq.
Roderick Linton Belfance, LLP

Kim Cavitt, AuD
Audiology Resources, Inc.

HIPAA

- Health Insurance Accountability and Portability Act of 1996 (HIPAA)
  - http://www.hhs.gov/ocr/privacy/hipaa/administrative/
  - Civil and criminal penalties
  - Covers:
    - Standard Transaction and Code Sets
    - National Provider Identifier
    - National Employer Identifier
    - HIPAA 5010
    - Security
    - HITECH (Breach Notification)
    - Privacy
      - Marketing
      - Business Associates

HIPAA Overview

- Business Associates
  - “A business associate is a person or organization, other than a member of a covered entity's workforce, that performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involve the use or disclosure of individually identifiable health information. Business associate functions or activities on behalf of a covered entity include claims processing, data analysis, utilization review, and billing.
  - “Business associate services to a covered entity are limited to legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services”.
  - Providers are responsible for the actions of their business associates.
  - http://www.hhs.gov/ocr/

HIPAA Overview

- Privacy vs. Security
  - Privacy
    - How/when any and all protected health information can be used or disclosed
    - Paper and Electronic
  - Security
    - Specific to protecting electronic protected health information

HIPAA Overview: PHI

- Protected Health Information (PHI): Individually identifiable health information is that which can be linked to a particular person. Such information in electronic form is Electronic Protected Health Information (EPHI).
- Any health or personal information given to a covered entity, whether verbal, written or electronic needs to remain confidential.

HIPAA Overview: PHI

- Names
- Street number and name, city, and last two digits of the zip code
- Dates directly related to the individual (birth date)
- Phone number
- Fax number
- Email address
- Social security number
- Medical record number
- Health insurance member number
- Account numbers
- Certificate or license numbers
- Vehicle identifiers and serial numbers
- Device identifiers and serial numbers
- Hearing aid serial numbers
- URLs
- IP addresses
- Biometric indicators
  - Finger, retinal and voice prints
- Photos
- Any unique identifying number, characteristic or code

Security Rule Overview

- The Security Rule is an extension of the Privacy Rule
- Went into effect April 20, 2005
- Applies to electronic formats
- You also need policies and procedures related to operations and documentation
- http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/security101.pdf

Security Rule Overview

- General Purpose - Ensures that electronic protected health information (EPHI) is kept private
- Enforcement… Office of Civil Rights enforces the Privacy and Security Rules in several ways:
  - investigating complaints filed with it,
  - conducting compliance reviews to determine if covered entities are in compliance, and
  - performing education and outreach to foster compliance with the Rules' requirements.
- Penalties
  - Civil and/or Criminal

Security Rule Overview

- Four Requirements of Security:
  - Ensure confidentiality, integrity, and availability of EPHI.
    - Confidentiality - data or information is not made available or disclosed to unauthorized persons or processes.
    - Integrity - data or information have not been altered or destroyed in an unauthorized manner.
    - Availability - data or information is accessible and useable upon demand by an authorized person.
  - Protect against possible threats and hazards to EPHI.
  - Protect against unauthorized uses or disclosures.
  - Ensure compliance by the workforce.

Administrative Safeguards

- Information access management:
  - Access to EPHI based on what is needed to perform the job
    - Regulate who has access to protected health information
    - Minimum necessary access
  - Security awareness and training

Administrative Safeguards

- Security updates, incident reporting, log-in, and password management
- Security incidents will be reported if suspected or if there is an actual breach
- Sanctions Policy
  - Need to enforce, Educate workforce

http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/adminsafeguards.pdf

Security Rule: Risk Assessment

- "A risk analysis process includes, but is not limited to, the following activities:
  - Evaluate the likelihood and impact of potential risks to e-PHI
  - Implement appropriate security measures to address the risks identified in the risk analysis
  - Document the chosen security measures and, where required, the rationale for adopting those measures
  - Maintain continuous, reasonable, and appropriate security protections"
  - http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html
  - http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/riskassessment.pdf

Physical Safeguards

- Safeguard the facility and equipment, from unauthorized physical access, tampering, and theft
- Mobile Devices
  - Who has access to EPHI remotely
  - Are they accessible on personal devices?

Physical Safeguards

- Workstation use and security
  - Log on using unique ID/password
    - Log off prior to leaving the workstation
  - Inspect the last logon information
    - Report any discrepancies
  - Comply with all applicable password policies and procedures
  - Close files not in use

http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/physsafeguards.pdf

Technical Safeguards

- Access controls
  - User password protection
    - Unique passwords, periodic changes
    - NOAH should not be ABC-123
  - Automatic Logoff
- Auditing Systems
  - Safeguards to record and examine access

Technical Safeguards

- Transmission Security
  - Integrity of Systems
    - Ensure EPHI is not being altered or destroyed improperly
  - Encryption Decryption
    - Communications over networks
    - Should not send patient emails through typical email systems

- http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf

Security Rule:
Policies, Procedures and Documentation

- You need a Security Officer
- You must develop policies and procedures to comply with the security rule
  - If guidance is needed, consult an IT consultant who specializes in HIPAA
- Must have written policies and procedures
- Need to document staff training, actions, activities and risk assessments
- http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/pprequirements.pdf

Questions and Answers

Please forward any questions to

Kim Cavitt at
kim.cavitt@audiologyresources.com

For more information on available resources from ADA, please go to
http://www.audiologist.org/practice-resource-catalog