AudiologyOnline Tech Support: 800.753.2160

HIPAA Redux 2013

Presented by:

Kim Cavitt, AuD

Moderated by:

Carolyn Smaka, Au.D., Editor-in-Chief, AudiologyOnline

AudiologyOnline Tech Support: 800.753.2160

Expert e-Seminar

TECHNICAL SUPPORT

Need technical support during event?

Please contact us for technical support at

800-753-2160

CEUs

CEU Total Access members can earn continuing education credit for participation in this course. Be sure to take the outcome measure following course completion to earn your CEUs, or contact us for more information or assistance: **800-753-2160**

HIPAA Redux 2013

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

Standard Transaction and Code Set

- This aspect of HIPAA requires that the following code sets be utilized for documenting and billing all medical items and services:
  - CPT (Current Procedural Terminology)
  - ICD9 (international Classification of Diseases-9th Revision)
    - Will become ICD-10 on October 1, 2014
  - HCPCS (Healthcare Common Procedure Coding System)
- Some state Medicaid programs still are allowed to utilize their own codes.
  - For example, Medi-Cal

National Provider Identifier (NPI)

- Requires that each individual provider utilize their own distinct, unique individual provider identification number for all payers
  - This number stays with the provider as they move from employer to employer
  - National Provider Identifier (NPI)
    - National Plan and Provider Enumeration System (NPPES)
      - https://nppes.cms.hhs.gov/NPPES/Welcome.do
  - This code is placed in box24J of the HCFA 1500 Claim form (or its electronic equivalent)

National Employer Identifier (EIN)

- Requires that each individual practice or facility utilize their own distinct, unique practice or facility identification number for all payers
  - This is required for every practice or facility except a sole proprietorship
  - The EIN is issued by the Internal Revenue Service (IRS)
  - Each practice also needs a facility or practice National Provider Identifier (NPI)
    - National Plan and Provider Enumeration System (NPPES)
    - https://npiregistry.cms.hhs.gov/NPPESRegistry/NPIRegistryHome.do

HIPAA 5010

- This was a systems update, that went into effect January 1, 2012 (enforcement began ion March 31, 2012) on that required systems updates to allow for transition to ICD-10
  - Affected software vendors, payers and clearinghouses much more than providers
  - Needed to allow increased fields for more digits (for ICD10)

Protected Health Information (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

Protected Health Information (PHI)

- 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

Protected Health Information (PHI)

- IP addresses
- Biometric indicators
  - Finger, retinal and voice prints
- Photos
- Any unique identifying number, characteristic or code

Security

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

Security Rule

- Covered entities must:
  - "Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit
  - Identify and protect against reasonably anticipated threats to the security or integrity of the information
  - Protect against reasonably anticipated, impermissible uses or disclosures
  - Ensure compliance by their workforce."
- http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html

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

Security Rule: Administrative Safeguards

- Security Measures
  - To reduce risks of breaching protected health information
- Need a Security Officer
- Information Access Management
  - Regulate who has access to protected health information
    - Minimum necessary access
- Training and Accountability
  - Authorize access to PHI
  - Train staff on policies and procedures
  - Sanction staff who do not comply
- http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/adminsafeguards.pdf

Security Rule: Physical Safeguards

- Facility access and control
  - Limiting and controlling physical access
- Workstation and device security
  - Proper use and access to workstations and electronic devices
  - Policies and procedures related to:
    - Transfer
    - Removal
    - Disposal
    - Re-use
  - http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/physsafeguards.pdf

Security Rule: Technical Safeguards

- Control of access
  - Passwords to protect access
- Audit
  - Safeguards to record and examine access
- Integrity control
  - Ensure that PHI is not improperly altered or destroyed
- Transmission security
  - Protections against "hacking"

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

Security Rule: Policies, Procedures and Documentation

- You must develop policies and procedures to comply with the security rule
- 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

HITECH-Breach Notification

- Effective date of February 17, 2010
- Breach
  - An "impermissible" or unauthorized use or disclosure of PHI
- Breach notification
  - Must occur within 60 days
  - Providers and business associates have burden of proof that notifications have been made
  - Business Associates must notify the covered entity
  - Notify the individual
  - Media
    - If breach is of more than 500 individuals
  - Notify Secretary of Health and Human Services
    - If breach is of more than 500 individuals

    http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html

Privacy Rule

- Protections of patient's health information and PHI
- Effects both paper and electronic records
- Effective April 14, 2003
- Protects" Individually identifiable health information" is information, including demographic data, that relates to:
  - The individual's past, present or future physical or mental health or condition,
  - The provision of health care to the individual,
  - The past, present, or future payment for the provision of health care to the individual,and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual.
  - Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number)".
  - http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html

Privacy Rule Specifics:

- Keep disclosures to "minimum necessary"
- Need a Privacy Officer
- Need training on privacy and that training must be documented
- Must have a complaint process
- Must have record safeguards
  - Storage
  - Disposal
  - Access

Privacy Rule: Authorization

- These three situations, with certain limits, do not require specific authorization:
  - Treatment
  - Payment
  - Healthcare operations
  - Other disclosures require authorization and a patient at any time can limit or require a reporting of their disclosures
  - http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/usesanddisclosuresfortpo.html

Privacy Rule: Marketing

- The Privacy Rule defines "marketing" as making "a communication about a product or service that encourages recipients of the communication to purchase or use the product or service."
- "An arrangement between a covered entity and any other entity whereby the covered entity discloses protected health information to the other entity, in exchange for direct or indirect remuneration, for the other entity or its affiliate to make a communication about its own product or service that encourages recipients of the communication to purchase or use that product or service."
- http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/marketing.html

Privacy: Business Associate

- "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/privacy/hipaa/understanding/summary/index.html

Omnibus Rule

- Effective September 23, 2013
- Business associates (any entity that creates, receives, maintains, or transmits PHI on behalf of a provider who supplied this information to them) and their contractors and subcontractors, are required to comply to the updated HIPAA Privacy and Security Rules, including breach notification;
- Patients have the right to request that a copy of their electronic medical record be supplied to them in an electronic format;

Omnibus Rule

- Patients who are paying privately for an item or service have the right to restrict any disclosure about this item or service to their health plan;
- "Marketing" has been redefined as any patient communication where the provider receives financial remuneration from a third-party whose products or services are being marketed. When "marketing" is being performed using PHI, a patient authorization must be in place prior to sending this marketing communication;
- The sale of PHI is prohibited;
- There must be a defined breach notification process where a situation is presumed to be a breach until the provider, business associate, contractor or subcontractor determines that there is a low probability that the patient's privacy has been compromised. A risk assessment must be performed anytime there is a breach of PHI;

Omnibus Rule

- Allows for broader use of PHI for fundraising opportunities;
- Allows for a streamlined authorization process for use of PHI for research purposes;
- Penalties have increased to up to $1.5 million maximum per calendar (many fines range between $100 and $50,000 per violation and degree of culpability) and up to 10 years in jail.

What Every Practice Needs:

- 2013 Revised Notice of Privacy Practices
- 2013 Revised Business Associate Agreement
- 2013 Revised Breach Notification Policy
- 2013 Revised Marketing Authorization
- Facility NPI
- Use and Disclosure form
- Acknowledgement of Receipt of Notice of Privacy Practices
- Security Policy and Process
- Breach Notification Policy and Process

What Every Practice Needs:

- Risk Assessment Process
- Independent Contractor Agreement that includes HIPAA Language
- Documentation of Staff Training
- Employee Confidentiality Form