SPEECHPATHOLOGY.COM

If you are viewing this course as a recorded course after the live webinar, you can use the scroll bar at the bottom of the player window to pause and navigate the course.

SPEECHPATHOLOGY.COM

This handout is for reference only. It may not include content identical to the powerpoint. Any links included in the handout are current at the time of the live webinar, but are subject to change and may not be current at a later date.

CONTINUED™
SPEECHPATHOLOGY.COM

HIPAA: Understanding Privacy Issues in Speech-Language Pathology

K. Todd Houston, PhD, CCC-SLP, LSLS, Cert. AVT

Moderated by:
Amy Hansen, MA, CCC-SLP, Managing Editor, SpeechPathology.com

SPEECHPATHOLOGY.COM

Need assistance or technical support?

- Call 800-242-5183
- Email customerservice@speechpathology.com
- Use the Q&A pod

SPEECHPATHOLOGY.COM

How to earn CEUs

- Must be logged in for full time requirement
- Log in to your account and go to Pending Courses
- Must pass 10-question multiple-choice exam with a score of **80%** or higher
  - Within **7 days** for live webinar; within **30 days** of registration for recorded/text/podcast formats
- Two opportunities to pass the exam

SPEECHPATHOLOGY.COM

Interested in Volunteering to be a Peer Reviewer?

- APPLY TODAY!
- 3+ years SLP Professional Experience Required
- Contact Amy Natho at anatho@speechpathology.com

HIPAA: Understanding Privacy Issues in Speech-Language Pathology

K. TODD HOUSTON, PHD, CCC-SLP, LSLS CERT. AVT
PROFESSOR OF SPEECH-LANGUAGE PATHOLOGY

SCHOOL OF SPEECH-LANGUAGE PATHOLOGY & AUDIOLOGY
THE UNIVERSITY OF AKRON

Objectives

- Describe the importance of HIPAA and its application to Speech-Language Pathology
- Define Protected Health Information (PHI)
- Describe how HIPAA interacts with other laws, such as the HI-TECH Act, in the practice of Speech-Language Pathology

HIPAA: The Basics

The Health Insurance Portability and Accountability Act (HIPAA), Public Law 104-191, enacted on August 21, 1996

Purposes of HIPAA:

- Privacy Rule: protects the privacy and addresses the use and disclosure of protected health information (PHI) by covered entities
- Security Rule: sets national standards for the security of electronic PHI
- Breach Notification Rule: requires covered entities and business associates to provide notification following a breach of unsecured PHI

Health Information Privacy, 2014

Privacy Rule

Covered Entities

A covered entity is:

1. Health care provider: Speech-Language Pathologist
   - Doctor
   - Dentist
   - Psychologist
   - Nursing Home
   - Pharmacy
2. Health plan
   - Health insurance company
   - HMOs
   - Company health plans
   - Government programs covering health care: Medicare, Medicaid, military/veterans healthcare
3. Healthcare clearing house
   - Entities that process nonstandard health information they receive from another entity into a standard format or vice versa
     - Billing services
     - Re-pricing companies
     - Community health management information systems

Health Information Privacy, 2014

Business Associates

A business associate is:

- A person or organization, not part of the covered entity's workforce, that performs certain services for said covered entity that involves use or disclosure of health information
- Business associates are directly liable for compliance with certain provisions of the HIPAA Rules
- Examples:
  - Legal services
  - Accounting services
  - Administrative services
  - Financial services
  - Data management

Health Information Privacy, 2014

Protected Health Information

Protected health information (PHI) includes:

- Name
- Address
- Birth date
- Social security number
- Demographic information relating to:
  - The patient's past, present, or future physical or mental health
  - The provision of healthcare to the patient
  - Past, present, or future payment for the provision of health care

Under HIPAA's Privacy Rule, all PHI used by a covered entity must be protected, no matter the form

- Electronic
- Paper
- Oral

Health Information Privacy, 2014

Disclosure of PHI

Required disclosure of PHI:

- To the patient or his/her personal representative
- To the Department of Health and Human Services when undertaking compliance investigations

Permitted disclosure of PHI (without patient's authorization):

- Treatment, payment, and health care operations
- Opportunity to agree or object (i.e. facility directory, persons operation on patient's behalf)
- Public interest and benefit activities (CDC, FDA, OSHA, law enforcement reasons)
- Limited data for research, public health, or health care operations

Health Information Privacy, 2014

Authorization for Disclosure of PHI

In order to disclose PHI for any purpose other than treatment, payment, or health care operations, the covered entity must obtain the patient's written authorization and the patient must be informed in writing the specific terms regarding who and in what context the PHI will be used.

In addition, efforts must be made to disclose only the limited PHI needed to provide health care services.

Health Information Privacy, 2014

Privacy Practice Notice

Each covered entity is required to provide every patient with notice of its privacy practices, which must include:

- Description as to why and how the health information may be used
- The covered entity's duties to protect PHI
- Describe the patient's rights to use and disclosure including how to report if they feel the privacy of their PHI has been breached

A covered health care provider with a direct treatment relationship to a patient must deliver the notice of its privacy practices to patients:

- No later than the first service encounter via personal delivery, electronic service delivery, or mailing
- By posting the notice in a clear and prominent location at each service delivery site
- In emergency situations, provide the notice as soon as practical after the emergency abates
- Upon request

In addition, the covered health care provider must make an effort to obtain written acknowledgement from patients of receipt of the practice's privacy policies

Health Information Privacy, 2014

Security Rule

Security Rule

- Also known as the Security Standards for the Protection of Electronic Protected Health Information
- Security standards for PHI held or transferred in electronic form (e-PHI)
- Applies to same covered entities and business associates as the Privacy Rule
- Applies to all PHI a covered entity creates, receives, maintains, or transmits in electronic form

Health Information Privacy, 2014

Security Rule Basics

- Confidentiality: e-PHI is not available or disclosed to unauthorized persons
  - Supports the Privacy Rule's prohibitions against improper use and disclosure of PHI
- Integrity: e-PHI is not altered or destroyed in an unauthorized manner
- Availability: e-PHI is accessible and usable on demand by authorized person

Health Information Privacy, 2014

Security of e-PHI

Because covered entities vary in size and environment, the Security Rule does not dictate measures required to ensure security of e-PHI

However, requires covered entities to consider:

- Size, complexity, and capabilities
- Technical, hardware, and software infrastructure
- Costs of security measures
- Likelihood and possible impact of potential risks to PHI

To accommodate constantly evolving technology, covered entities must review and modify security measures on continual basis

Health Information Privacy, 2014

Security Rule Standards

- The Security Rule does require the following standards to be addressed:
- **1. Administrative safeguards**
  - Security management process
  - Assigned security responsibility
  - Workforce security
  - Security awareness and training
  - Security incident procedures
  - Contingency plan
  - Evaluation
  - Business associate contracts and other arrangements

Security 101 for Covered Entities , 2007

2. Physical safeguards:

- Facility access controls
- Workstation use
- Workstation security
- Device and media controls

3. Technical safeguards:

- Access control
- Audit controls
- Integrity
- Person/entity authentication
- Transmission security

Security 101 for Covered Entities , 2007

4. **Organizational requirements:**
   - Business associate contracts and other arrangements
   - Requirements for group health plans
5. **Policies and procedures and documentation requirements**

Security 101 for Covered Entities , 2007

Breach Notification Rule

Breach Notification Rule

Breach: impermissible use or disclosure of PHI unless covered entity or business associates complete risk assessment and deem low probability PHI has been compromised

Covered entities and business associates are required to provide notification following a breach of unsecured PHI to:

- Affected individual within 60 days of breach
- Prominent media outlets if breach affects more than 500 residents of a state
- The Secretary of breaches of unsecured PHI
- The covered entity if breach occurs by business associate

Health Information Privacy, 2014

Penalties for Non-Compliance

Failure to comply with HIPAA can result in:

- Violations prior to 2/18/2009 => up to $100 per violation and $25,000 calendar year cap
- Violations after 2/18/2009 => up to $50,000 or more per violation and $1.5 million calendar year cap
- Criminal penalties of up to $50,000 and 1 year imprisonment if a person knowingly obtains or discloses PHI
- Criminal penalties increase to $100,000 and up to 5 years imprisonment if the conduct involves false pretenses
- Criminal penalties increase to $250,000 and up to 10 years imprisonment if the conduct involves intent to sell, transfer, or use PHI

Health Information Privacy, 2014

Non-Compliance Statistics

- According to Office of Civil Rights:
  - Average cost data breach: $5.5 million
  - Average cost per patient record breach: $240
  - Patient data breaches as of April 2013: 65,000 ($50 million)
  - Patient data breaches as of September 2013: 80,000

Keeping Data in Motion, 2013

Instances of Non-Compliance

- Hospice of North Idaho: $50,000 for losing laptop with 440 individuals' PHI
- Lab Corporation of America: stolen external hard drive with 2,773 individuals' PHI
- WellPoint: $1.7 million for leaving PHI of 612,200 individuals' accessible over the internet
- Children's Hospital of Orange County: unintentionally faxed individuals' records to auto shop
- Doctor in Tennessee: accidentally faxed individuals' PHI to a businessman for more than four years without knowledge of mistake

Keeping Data in Motion, 2013

HIPPA & Speech-Language Pathologists

HIPAA and SLPs

HIPAA pertains to all health-care professionals, including speech-language pathologists (SLPs)

- Hospital
- Skilled Nursing Facility
- University Clinic
- Private Practice (if not considered covered entity, still bound by ASHA Code of Ethics to always protect patient privacy)
- School (as well as Family Educational Rights and Privacy Act-FERPA)

SLPs Must Do the Following:

- Maintain the privacy of patients' health information
- Refrain from selling protected health information without the patient(s) individual written authorization
- Notify the patient if there has been a breach of unsecured protected health information
- Provide the patient with a paper copy of this notice of privacy practices upon request

DO'S FOR HIPAA

- Do secure all patient information, reports, billing records from the public view
  - Computer screens should be turned away from public view
- Log off the computer when unattended
  - Have screen savers set to go off within a certain time frame
  - Patient information must be discarded by shredding, NOT by placing in regular trash/recycle bins

DO'S CONTINUED

- Do respect patients and their right to privacy. Keep your voice low so others cannot overhear your conversation.
- Keep fax machines located away from the public & verify number prior to sending the information.
- If you think someone is misusing patient information then you have a duty to report it through appropriate channels.

DON'TS FOR HIPAA

- Do not leave printed or electronic patient information exposed where visitors or unauthorized individuals can see it.
- Only designated individuals are allowed back in the receptionist's area!
- Do not discuss patient information in public places or with unauthorized individuals
- Videotape, audiotape, and DVD recordings are considered part of a patient's PHI and are NOT to leave the facility for any reason.
  - Be care about using your smartphone for audio or video recordings.

WHAT ARE THE CRIMINAL PENALTIES UNDER HIPAA?

- There are severe civil and criminal penalties for a single violation that range from $100 per violation to $250,000 and/or 10 years in prison.
- The HIPAA Omnibus Rule of 2013 expanded the penalties up to $1.5 million for multiple violations in a covered year
- HIPAA is the only federal regulation that carries with it **personal** liability to individuals who violate the act.

Telepractice

Defined by the American Speech-Language-Hearing Association (ASHA) as a videoconferencing service delivery model used by SLPs

Allows for patient/clinician or clinician/clinician assessment, intervention, and consultation at a distance

Providers must ensure the same level of confidentiality in delivering services through telepractice as they do when providing services onsite

Security Issues in Telepractice

Speech therapy services delivered via telepractice can present several security issues

Areas to examine for potential security risks:

- Location of clinician when providing services
- Location of patient when receiving services
- Type of Voice over Internet Protocol (VoIP) or videoconferencing software being used
- Computer and technology protection (anti-virus software, passwords, internet connection)
- Documentation and reports
- Recording of sessions and sharing of recordings

Telepractice Security Precautions

To ensure patients' privacy when using telepractice, consider the following:

- Secure videoconferencing software
  - Free formats (Skype, iChat, and ooVoo) can be accessed by a third party
  - Audio and video transmissions must be secured using point-to-point encryption
- Firewall protection
- Anti-virus software
- Secure storage of records and PHI (not on cloud services)
- Password protection on all computers and software
- If services will be recorded, SLP and client must decide in writing how it will be stored and secured

Practice Guidelines for Video-Based Online Mental Health Services , 2013

HITECH Act

Health Information Technology for Economic and Clinical Health (HITECH) Act of the American Recovery and Reinvestment Act of 2009

Promotion of and guidelines for use of health information technology (HIT), including health information exchange (HIE) and electronic health records (EHRs)

Benefits of HIT:

- Improve care coordination
- Reduce healthcare disparities
- Engage patients and families
- Improve population and public health
- Ensure adequate privacy and security

Greater Enforcement of HIPAA

- The HITECH Act widens the scope of privacy and security protections available under HIPAA
- Extends complete Privacy and Security Provisions of HIPAA to business associates of covered entities
- New breach notification requirements
- Extends the current accounting for disclosure requirements to information that is used to carry out treatment, payment, and health care operations when an organization is using an EHR
  - Reduces timeframe for accounting from 6 to 3 years

SUMMARY

All health information that specifically identifies an individual is considered confidential!

Examples of PHI:

- Client's name
- Addresses
- Phone numbers
- Emails
- SSN's
- Date of birth
- Reports (progress reports, diagnostics, test forms)
- Other records (intake forms, case-histories)

SUMMARY

- Protecting the privacy of patient information is EVERYONE'S responsibility!
- Create best practices within your setting to ensure consistent compliance; don't "cut corners."
- Don't intentionally or unintentionally disclose patient information.
- If you suspect any privacy violations or concerns, notify the appropriate supervisors or compliance officer.

Resources

(2014). Health information privacy. U.S. Department of Health & Human Services. Retrieved from http://www.hhs.gov/ocr/privacy/index.html

HITECH act. HealthIT.gov. Retrieved from http://www.healthit.gov/policy-researchers-implementers/hitech-act-0

Houston, K.T., Behl, D., & Walter, K.Z. (2013). Using telepractice to improve outcomes for children who are deaf or hard of hearing & their families.

(2013). Keeping data in motion: The high cost of HIPAA non-compliance, part 2. OpenText. Retrieved from http://servicecenter.fiercemarkets.com/files/leadgen/opentext_wp_keeping_data_in_motion_part_2.pdf

Moreno, L., Peikes, D., & Krilla, A. (2010). Necessary but not sufficient: The HITECH Act and Health information technology's potential to build medical homes. Agency for Healthcare Research and Quality.

(2013). Practice guidelines for video-based online mental health services. American Telemedicine Association. Retrieved from http://www.americantelemed.org/docs/default-source/standards/practice-guidelines-for-video-based-online-mental-health-services.pdf?sfvrsn=6

(2007). Security 101 for covered entities. U.S Department of Health & Human Services. Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/security101.pdf

Thank You for Listening!

K. Todd Houston, PhD, CCC-SLP, LSLS Cert. AVT

Professor

School of Speech-Language Pathology & Audiology

The University of Akron

(330) 972-6141

houston@uakron.edu