







Live Webinar
on

HIPAA/HITECH – 2016

HIPAA Staff Training Boot Camp

Brian L Tuttle, CPHIT, CHA, CHP, CBRA, CISSP, CCNA, Net +

©MentorHealth2016 Wednesday, September 21, 2016 | 01:00 PM EDT



- The Health Insurance Portability Act of 1996 (HIPAA)
- Enacted by the United States Congress and signed by President Clinton in 1996.

www.mentorhealth.com 2



Also known as the Kennedy-Kassebaum Act named after two of its major sponsors:

- Senator Ted Kennedy (D) Massachusetts
- Senator Nancy Kassebaum (R) Kansas



HIPAA

HIPAA is an acronym for the Health Insurance Portability and Accountability Act of 1996



“Privacy” and “Security”
are not even in the name
“HIPAA” but they present
our biggest challenge



BOY WHO CRIED WOLF



Well the Wolf is Here



HIPAA Before Omnibus (September 23, 2013)





HIPAA After Omnibus (September 23, 2013)



September 23rd, 2013

D-Day

- The *HIPAA Omnibus Rule* went into affect
- Increases penalties
- Equals the burden between business associates and covered entities
- Enforces what was already on the books for covered entities
- ***Greatly enforces and increases federal auditing***
- ***More funding for 2016***
- ***More audits for 2016***
- ***Patient cash remedies***
- ***Every year since Omnibus fines have increased***
- ***Individual Remedy***



Background

- HIPAA has historically been a benign law
- No consequences for actions in most cases
- More of a nuisance than a real problem
- Fines were low and rare
- Audits were very rare
- Only Uncle Sam can sue (for now)



Can YOU and ME be arrested for
wrongful disclosure of protected
health information?

YES!!

WE ARE ALL RESPONSIBLE BOTH CIVIL AND CRIMINAL



Can Practice/Business/Organization be fined for HIPAA violations even if a breach **doesn't** occur?

YES!!



WHAT IS PROTECTED HEALTH INFORMATION?

- HIPAA defines PHI as:

Patient identifiable health information that is transmitted or maintained in any form or medium (electronic, oral, or paper) by a covered entity or its business associates, excluding certain educational and employment records.



PROTECTED HEALTH INFORMATION IDENTIFIERS

- Names
- Street address, city, county, precinct, zip code
- Dates directly related to an individual—birth date, admission date, discharge date, date of death
- Phone numbers
- Fax numbers
- Electronic mail addresses
- Social Security numbers
- Medical record numbers



PROTECTED HEALTH INFORMATION IDENTIFIERS

- Health plan beneficiary numbers
- Account numbers
- Certificate/License numbers
- Vehicle identifiers and serial numbers—license plate numbers
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Biometric identifiers—finger and voice prints
- Full-face photographic images and any comparable images



What Constitutes a Breach?

- Any impermissible use or disclosure of PHI is presumed to be a breach, with a subsequent requirement to provide a breach notification;

UNLESS:

- Covered Entity (CE) or Business Associate (BA) demonstrates there is low probability that the PHI has been compromised.
- NOTE: The burden is on the CE or BA to prove that notifications were provided or that a breach did not occur.



What Determines if PHI has been Compromised?

- The nature and extent of the PHI involved, including the types of identifiers
- The unauthorized person who used the PHI or to whom the disclosure was made
- Whether the PHI was actually acquired or viewed
- The extent to which the risk has been mitigated.



SUMMARY OF BREACH POLICY (cont)

- Discovery of breach
 - Treated as discovered on the first day known to practice
- Notify practice administrator, privacy officer immediately
- Conduct an investigation/risk assessment
- Begin notifying individuals who had or may have had their PHI accessed
- Notify HHS, media, and/or law enforcement



TOP THREE WAYS A BREACH OCCURS of EPHI

29% THEFT

Theft of unencrypted electronic devices or physical records is the most common method of breach in healthcare entities.



23% HACKING

Hacking is the most common method of breach for corporate entities.



**20% PUBLIC ACCESS/
DISTRIBUTION**

The largest fine paid by a healthcare entity to date was because patient records were accidentally made publicly accessible on the Internet.





OCR Enforcements

- Most frequent compliance issues that are investigated
 - Impermissible uses and disclosures of PHI
 - Lack of safeguards of PHI
 - Lack of patient access to their PHI
 - Lack of administrative safeguards of ePHI
 - Use or disclosure of more than the minimum necessary PHI



COMMON HIPAA VIOLATIONS

- Clinical documentation causing HIPAA violations
 - Selecting the wrong person to CC on an e-mail containing PHI
 - Selecting the wrong patient name
 - Selecting the wrong account number, medical record number, or subject ID
 - Entering the wrong supervising or attending physician
 - Sharing information about a patient with others when there is no reason for them to know
 - Failure to immediately report any potential breach or security incident to the compliance officer or your supervisor
 - Improper disposal of materials containing PHI





YOU ARE RESPONSIBLE

- Any activity on a computer under your username is your responsibility
- Prevent loss or theft of handheld phones and laptop computers
- Know where PHI and patient's information is being sent or received
- Close programs when not in use
- Follow policies
- Leave work out of social Website postings
- Be aware of cell phone texting of PHI
- Ask questions and report suspicious activity



FISHING OR PHISHING

- E-mail phishing is often identified as the origin of the breach
 - Phishing is a fake e-mail or Website that attempts to gather your personal information for identity theft or fraud
 - Phishing scams usually use a spoofed Website that looks very much like the real Website

What Does a Phishing E-mail Look Like?

Hello!
As part of our security measures, we regularly screen activity in the Facebook system. We recently contacted you after noticing an issue on your account.

Our system detected unusual Copyrights activity linked to your Facebook account , please follow the link below to fill the Copyright Law form:

http://www.facebook.com/application_form

Note: If you dont fill the application your account will be permanently blocked.

Regards,
Facebook Copyrights Department.

Spelling Links in email Threats Popular company

www.mentorhealth.com 25




DO NOT TEXT OR EMAIL EPHI WITHOUT ENCRYPTION UNLESS APPROPRIATE CARE IS TAKEN



I ♥

Texting

www.mentorhealth.com 26



<http://www.hhs.gov/hipaa/for-professionals/fag/570/does-hipaa-permit-health-care-providers-to-use-email-to-discuss-health-issues-with-patients/index.html>

Directly from www.HHS.gov

Does the HIPAA Privacy Rule permit health care providers to use e-mail to discuss health issues and treatment with their patients?



YES

Directly from www.HHS.gov

The Privacy Rule allows covered health care providers to communicate electronically, such as through e-mail, with their patients, provided they apply reasonable safeguards when doing so.



Continued

Directly from www.HHS.gov

Certain precautions may need to be taken when using e-mail to avoid unintentional disclosures, such as checking the e-mail address for accuracy before sending, or sending an e-mail alert to the patient for address confirmation prior to sending the message.



Continued

Directly from www.HHS.gov

While the Privacy Rule does not prohibit the use of unencrypted e-mail for treatment-related communications between health care providers and patients, other safeguards should be applied to reasonably protect privacy, such as limiting the amount or type of information disclosed through the unencrypted e-mail.



NOTE

An individual has the right under the Privacy Rule to request and have a covered health care provider communicate with him or her by alternative means or at alternative locations, if reasonable.



NOTE

Example: A health care provider should accommodate an individual's request to receive appointment reminders via e-mail, rather than on a postcard, if e-mail is a reasonable, alternative means for that provider to communicate with the patient. However, if the use of unencrypted e-mail is unacceptable to a patient who requests their PHI, other means of communicating (i.e. mail, telephone, patient portal) should be offered and accommodated.



I get this question often:

What if a patient initiates the conversation via email?

If this situation occurs, one can assume (unless the patient has explicitly stated otherwise) that e-mail/text communications are acceptable to the individual. If the CE or BA feels the patient may not be aware of the possible risks of using unencrypted e-mail/texting, or has concerns about potential liability, the CE or BA can alert the patient of those risks, and let the patient decide whether to continue e-mail communications. – recommended.



The above should also apply when communicating with other CE's or BA's




Let's review:

If you think the individual may not be aware of the possible risks of using unencrypted e-mail/texting, or has concerns about potential liability, you should **ABSOLUTELY** alert the patient of those risks, and let the patient decide whether to continue e-mail communications.

Remember – risks are higher now that patients can sue





BYOD



BRING YOUR OWN DEVICE

www.mentorhealth.com 35



DO NOT

- Allow PHI to be written to the mobile device
- Permit integration with insecure file sharing or hosting services
- Set it and forget it (always include BYOD in risk assessments)

www.mentorhealth.com 36



Best Practices

- Ensure security updates on the phone are done
- Use multi-factor authentication (i.e. passwords and biometrics)
- Encrypt the device using whole disk encryption (P.S. – a lost or stolen encrypted device is not a reportable breach under HIPAA)



#1 Compliance Worry with BYOD





Mitigating Steps for Theft

- PASSWORD PROTECT PRIOR
- Remote Tracking – GPS tracking ability, this is now standard on iPhones using “Find my iPhone” function
- Remote Disabling – secondary layer of protection but will not protect if SIM card was stolen....
- Remote Memory Wipe – must be installed prior via app or function (last resort)



TEXTING and HIPAA





TEXTING and HIPAA

- Almost 90% of mobile phone users send SMS text messages
- Texting has become entrenched in medical care too
- Many medical professionals are sending identifiable health information via non-secure texting



ENCRYPTION





ENCRYPTION

- Encrypt any portable device which access transmits or maintains EPHI
- Encrypt any thumb drive which may contain EPHI or sensitive data
- Encrypt any email transmissions outside of the Domain which may contain EPHI



OCR Case Real Example

Private Practice Revises Process to Provide Access to Records Regardless of Payment Source

At the direction of an insurance company that had requested an independent medical exam of an individual, a private medical practice denied the individual a copy of the medical records. OCR determined that the private practice denied the individual access to records to which she was entitled by the Privacy Rule. Among other corrective actions to resolve the specific issues in the case, OCR required that the private practice revise its policies and procedures regarding access requests to reflect the individual's right of access regardless of payment source.



OCR Case Example

- Private Practice Provides Access to All Records, Regardless of Source

A private practice denied an individual access to his records on the basis that a portion of the individual's record was created by a physician not associated with the practice. Among other steps to resolve the specific issue in this case, OCR required the private practice to revise its access policy and procedures to affirm that, consistent with the Privacy Rule standards, patients have access to their record regardless of whether another entity created information contained within it



OCR Case Example

Private Practice Ceases Conditioning of Compliance with the Privacy Rule

A physician practice requested that patients sign an agreement entitled "Consent and Mutual Agreement to Maintain Privacy." The agreement prohibited the patient from directly or indirectly publishing or airing commentary about the physician, his expertise, and/or treatment in exchange for the physician's compliance with the Privacy Rule. A patient's rights under the Privacy Rule are not contingent on the patient's agreement with a covered entity. A covered entity's obligation to comply with all requirements of the Privacy Rule cannot be conditioned on the patient's silence. OCR required the covered entity to cease using the patient agreement that conditioned the entity's compliance with the Privacy Rule. Additionally, OCR required the covered entity to revise its Notice of Privacy Practices.



OCR Case Example

Hospital Implements New Minimum Necessary Policies for Telephone Messages



A hospital employee did not observe minimum necessary requirements when she left a telephone message with the daughter of a patient that detailed both her medical condition and treatment plan. The employee left the message at the patient's home telephone number, despite the patient's instructions to contact her through her work number. To resolve the issues in this case, the hospital developed and implemented several new procedures. The new procedures were incorporated into the standard staff privacy training, both as part of a refresher series and mandatory yearly compliance training.




OCR Case Example

Dentist Revises Process to Safeguard Medical Alert PHI



An OCR investigation confirmed allegations that a dental practice flagged some of its medical records with a red sticker with the word "AIDS" on the outside cover, and that records were handled so that other patients and staff without need to know could read the sticker. When notified of the complaint filed with OCR, the dental practice immediately removed the red AIDS sticker from the complainant's file. To resolve this matter, OCR also required the practice to revise its policies and operating procedures and to move medical alert stickers to the inside cover of the records. Further, the covered entity's Privacy Officer and other representatives met with the patient and apologized, and followed the meeting with a written apology.

HIPAA Scenarios



www.mentorhealth.com 49

What should the physician do?

- A patient is demanding—she demands pain prescription medication the physician says, “NO!” The patient demands her medical records to go to another doctor’s office. The physician herself copies the records and gives them to the patient. Upon arriving home, the patient notices 3 different records of other patients—she calls the office and tells the physician to give her the pain medication prescription if she wants the records back.

www.mentorhealth.com 50



- A pharmacy calls and informs you that Mr. Smith is calling and pretending to be the doctor in order to obtain narcotics.
- Can you call other pharmacies and notify them about Mr. Smith's fraud?



Yes, there is a crime
being committed





- Does every patient, (new patients and old patients), need to sign a statement they have reviewed the new Notice of Privacy Policy?
- What if a patient has signed one last year ?



- YES—patients need to sign an acknowledgement that includes the following:
 - Opportunity to read the new notice
 - Opportunity to receive a copy
 - Opportunity to make changes to their PHI if they so desire
 - Opportunity to have questions answered



www.mentorhealth.com

55



IN THE NEWS..... **\$100,000**

The HHS Office for Civil Rights (OCR) opened an investigation of APDerm upon receiving a report that an unencrypted thumb drive containing the phi of approximately 2,200 individuals was stolen from a vehicle of one its staff members. The thumb drive was never recovered. The investigation revealed that APDerm had not conducted an accurate and thorough analysis of the potential risks and vulnerabilities to the confidentiality of ePHI as part of its security management process. Further, APDerm did not fully comply with requirements of the Breach Notification Rule to have in place written policies and procedures and train workforce members.

www.mentorhealth.com

56



- Employee or physician removed unencrypted ePHI from the office and failed to secure the drive
- ePHI was transferred to an unencrypted flash drive
- Risk assessment was never completed after discovering the loss of the flash drive
- No written policies and procedures and training in place for staff/physicians
- No risk management plan



IN THE NEWS..... **PRISON**

Dr. Huping Zhou, Sentenced to
Four Months in Prison and
Fined for HIPAA Violation



IN THE NEWS..... **PRISON**

- Zhou, who was a licensed cardiothoracic surgeon in China before immigrating to the US, was employed as a researcher with the UCLA School of Medicine
- Zhou received notice that UCLA intended to dismiss him for job performance reasons unrelated to the illegal access of medical records
 - That night, Zhou accessed and read his immediate supervisor's medical records as well as those of other coworkers



IN THE NEWS..... **PRISON**

- Over the next three weeks, Zhou abused his access to the organization's electronic health record system to view the medical records of celebrities and high-profile patients, including Drew Barrymore, Arnold Schwarzenegger, Tom Hanks, and Leonardo DiCaprio
- Zhou accessed the UCLA record system 323 times during the three-week period
- Zhou admitted he obtained and read patient health information on four specific occasions—with no legitimate reason, medical or otherwise—after he was terminated from his job



- **Knock Knock**

- *Who is there*

- **HIPAA**

- *HIPAA WHO*



I can't tell you



Is this a violation?

- A student nurse has just completed her Labor and Delivery rotation and posts a picture of a placenta on her Facebook.



- **No** a placenta is not PHI-however, the student will never work for that hospital because it may a policy that no patient information should be shared outside of the hospital



- A paralegal works for a law firm. She is asked by the attorney to review medical records for a car accident. She throws the medical records in the garbage—is this a HIPAA violation?



- **YES**
- Assuming the firm is a business associate



Things to Consider

- **Password sharing**
- Too many admin passwords
- Passwords not complex or changed often
- Bad backup policies
- No auto logoff or screen saver
- Where are financial discussions held?
- How are documents handled/stored prior to being shredded?



Low hanging fruit in an office walkthrough ..continued

- Server not in a secured area
- Paper based PHI not in a secure area
- Screens not physically adequate
- No TV or ambient noise
- Mannerisms of staff
- Social Networking
- **Voice level – minimum necessary**



Low hanging fruit in an office walkthrough ..continued

- Lack of system auditing
- Doors to sensitive areas not locked
- Encryption not being used
- Outsourced access(i.e. partners)
- Remote access
- Historical records
- **Minimum necessary standard – electronic systems**



Factors that Can Prompt or Increase Risk for an OCR HIPAA Audit

- 1. INTERNAL STAFF**
- 2. PATIENTS**
- 3. MEANINGFUL USE**
- 4. BUSINESS ASSOCIATES**
- 5. PREVIOUS or CURRENT BREACH**
- 6. NOT REPORTING A BREACH**
- 7. DISASTER**



Patient

- Patient may be upset with a bill
- Bad customer service
- Poor bedside manner
- Patient sees their chart laying around where anyone can see
- Patient over hears too much information via careless verbal discussions.



How to mitigate risk with patients?

- GOOD CUSTOMER SERVICE!!!!
 - Patients who love their doctor and staff less likely to cause an issue even if some areas are lax
- Train staff to only verbally speak the minimum amount of information necessary to perform job function. This is also called the “minimum necessary” standard.
- Setup practice “physically” in a strategic manner
- This will become a greater risk when patients are allowed to sue under HIPAA



How to mitigate risk with patients? ..continued

- Never leave a voice mail for any patient which discloses PHI
- Never disclose information to any family member unless they are on authorization form
- Auditors will call and test (pretending) – this is part of audit strategy



How to mitigate risk with patients? ..continued

- Keep voices low when discussing PHI.
- Limit discussions within the practice to the minimum necessary.
- Close windows at the front desk as much as possible and keep conversations to a minimum.



How to mitigate risk with patients? ..continued

- Close doors to exam or treatment rooms before discussing PHI.
- Discuss financial issues in a private area.
- Limit traffic in the clinical areas.
- Escort individuals who are not part of our workforce while they are in clinical areas.



How to mitigate risk with patients? ..continued

- Position terminals and written PHI so that unauthorized individuals may not readily access it.
- Place any papers in chart holders in such a manner as to protect any patient identifiers or health information from unauthorized individuals. This may mean placing the papers in the holders backwards, using only opaque holders, or using opaque paper in front of the health information.



How to mitigate risk with patients? ..continued

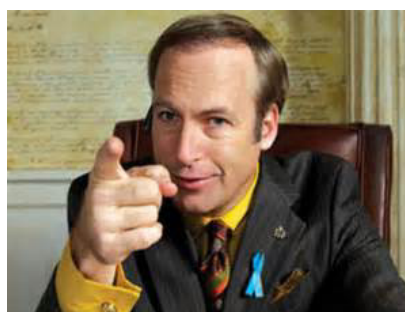
- Cover schedules or place them where unauthorized individuals cannot see them.

NOTE:

Patients may not outwardly say they are upset



OMNIBUS and Suing





CANNOT SUE UNDER HIPAA

There is no private cause of action allowed to an individual to sue for a violation of the federal HIPAA or any of its regulations. This means you do not have a right to sue based on a violation of HIPAA by itself. What most people don't get about HIPAA is that, as extensive as the statute is, and as serious as its potential penalties are, Congress, in its infinite wisdom, chose not to include a private right of action.



OMNIBUS and Suing

The Omnibus modifications to HIPAA made no impact on an individual's right of action. However, they do affect individuals in tangential ways.

Omnibus grants state attorneys general the ability to bring civil action and seek damages on behalf of their residents for HIPAA violations.



No Such Thing as 100% Security

Covered Entities and business associates are just expected to follow the Security and Privacy Rule standards; implement the proper policies, procedures, and technologies; and **reasonably show the organization is making an effort to protect against common threats and vulnerabilities.**



THE END

Q&A