MentorHealth

Live Webinar
on

Highest Risk Factors for HIPAA

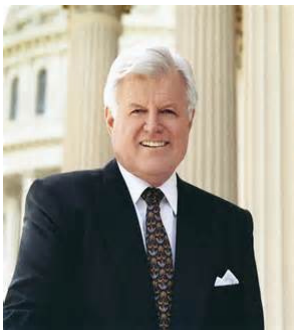
Brian L Tuttle, CPHIT, CHA, CHP, CBRA, CISSP, CCNA, Net +

Wednesday, March 9, 2016 | 01:00 PM EST

MentorHealth

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

MentorHealth



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

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

MentorHealth

HIPAA

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

MentorHealth

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

MentorHealth

HIPAA Titles

- **Title I** – Health Care Access, Portability, and Renewability
- **Title II** – Preventing Healthcare Fraud and Abuse, **ADMINISTRATIVE SIMPLIFICATION**, Medical Liability Reform.
- **Title III** – Tax Related Health Provisions
- **Title IV** – Application and Enforcement of Group Health Plan Requirements
- **Title V** – Revenue Offsets

MentorHealth

BOY WHO CRIED WOLF

MentorHealth

HIPAA Before Omnibus (September 23, 2013)

MentorHealth

HIPAA After Omnibus (September 23, 2013)

MentorHealth

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
- Proactive auditing and proactive fines
- Patient civil remedies
- ***Greatly enforces and increases federal auditing***

MentorHealth

Background

- 2009 HITECH Act & The Affordable Care Act (Obamacare) – Mandate that Health and Human Services (HHS) Office of Civil Rights (OCR) begin auditing covered entities and business associates
- HHS recently began awarding multiple firms contracts to carry out audits.
- HIPAA Omnibus Rule of 2013 primarily enforces laws already on the books and adds burden to business associates.

MentorHealth

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)

MentorHealth

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

YES!!

CONSTANTLY REINFORCE THIS TO STAFF

MentorHealth

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

YES!!

MentorHealth

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.

MentorHealth

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

MentorHealth

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

MentorHealth

WHAT IS A BREACH?

- **HIPAA defines a breach as:**

- An unauthorized acquisition, access, use, or disclosure of unsecured PHI
  which compromised the privacy, security, or integrity of the PHI
- PHI is considered unsecured if it is ***not*** encrypted or rendered unusable, unreadable, or indecipherable to unauthorized individuals

MentorHealth

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.

MentorHealth

What Determines if PHI has been Compromised?

A CE OR BA MUST CONSIDER THE FOLLOWING

- 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.

MentorHealth

SUMMARY OF BREACH POLICY

- HIPAA requires that covered entities notify individuals whose ***unsecured*** PHI has been impermissibly accessed, acquired, used, or disclosed, compromising the security or privacy of the PHI
- Notification requirements only apply to breaches of ***unsecured*** PHI
- Notification is not required if PHI is encrypted or destroyed in accordance with the HIPAA guidance

MentorHealth

SUMMARY OF BREACH POLICY (cont)

- Discovery of breach
  - Treated as discovered on the first day known to practice
- Notify practice administrator, privacy officer immediately
- Notify your Agent or a Patient Safety Risk Manager at The Doctors Company
- Conduct an investigation/risk assessment
- Begin notifying individuals who had or may have had their PHI accessed
- Notify HHS, media, and/or law enforcement

MentorHealth

TOP THREE WAYS A BREACH OCCURS

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.

MentorHealth

WHERE IS ELECTRONIC PROTECTED HEALTH INFORMATION LOCATED?

Which of the following are potential locations of ePHI?

A. Scan disks
B. Fax machines
C. Servers
D. Video surveillance system

1) A, B, C, but not D 2) A, B, D, but not C 3) All of the above

MentorHealth

BYOD

MentorHealth

BYOD

- Steadily growing
- Technology is ahead of compliance
- Considered by most IT managers as the highest risk for technological breaches of sensitive data

MentorHealth

Conundrum

- Highly effective
- Cheap to use
- Easy to use
- Very high risk
- Hard to manage

MentorHealth

Positives

- Provide flexibility
- Streamlines communications
- Increases productivity due to familiarity with device
- Can save the practice or business money (i.e. equipment, data plans, etc.)

MentorHealth

Positives

- Allows for easier tele-working
- Preferred by most staff members
- Employees can use apps which they prefer for productivity

MentorHealth

Negatives

- Who is responsible for support or repair?
- Audit devices for security may be considered intrusive and troublesome
- Device compatibility problems
- Problems with monitoring how and where PHI is stored

MentorHealth

Negatives

- Encryption?
- Are non-authorized individuals using the device? (i.e. kids playing games on phone)
- Theft?
- Weak passwords?

MentorHealth

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)

MentorHealth

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)

MentorHealth

Best Practices

- Train staff on appropriate apps and software as well as cyber threats
- Force complexity in the passwords and password change frequency of no more than 180 days
- Perform risk assessments annually to identify threats
- Role based access into systems

MentorHealth

#1 Compliance Worry with BYOD

MentorHealth

Mitigating Steps for Theft

- PASSWORD!!! Complex and Changed Every 180 days!!
- 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 first….
- Remote Memory Wipe – must be installed prior via app or function (last resort)

MentorHealth

TEXTING and HIPAA

MentorHealth

TEXTING and HIPAA

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

MentorHealth

TEXTING Positives in Healthcare

- Texting CAN provide great advantages in health care
  - Fast
  - Easy
  - Loud background noise problems are mitigated
  - Bad signal issues mitigated
  - Device neutral

MentorHealth

TEXTING Negatives in Healthcare

- Reside on device and not deleted
- Very easily accessed
- Not typically centrally monitored by IT
- Can be compromised in transmission relatively easy
- HIPAA Privacy Rule requires disclosure of PHO to patient (i.e. text message is used to make a judgement in patient care)

MentorHealth

Include Texting in Policies

- Address in risk assessment
  - Theft risks
  - Improper disposal risks
  - Interception of transmission risks
  - Lack of availability to persons other than the mobile device user

MentorHealth

Include Texting in Policies

- Administrative policy on workforce training (i.e. minimum necessary)
- Appropriate use of texting
- Password protections and encryption
- Mobile device inventory
- Retention period (require immediate deletion of PHI texts)
- Use of secure texting (i.e. TigerText)

MentorHealth

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

MentorHealth

What Does a Phishing E-mail Look Like?

MentorHealth

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

MentorHealth

OCR Enforcements

- The most common types of covered entities
  - Private practices
  - General hospitals
  - Outpatient facilities
  - Pharmacies
  - Health plans (group health plans and health insurance issuers)

MentorHealth

OCR Case 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.

MentorHealth

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

MentorHealth

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.

MentorHealth

OCR Case Example

Hospital Implements New Minimum Necessary Polices 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.

MentorHealth

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.

MentorHealth

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

MentorHealth

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

MentorHealth

Low hanging fruit in an office walkthrough

- **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?

MentorHealth

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
- No window at check in, patients too close to check in, more than one person at check in
- Do the providers dictate in areas where PHI could be overheard?

MentorHealth

Low hanging fruit in an office walkthrough ..continued

- Mannerisms of staff
- **Voice level – minimum necessary**
- Talking about PHI before entering an exam room
- Lack of adequate paperwork
- Outdated paperwork
- Lack of an alarm system if deemed reasonable

MentorHealth

Low hanging fruit in an office walkthrough ..continued

- Lack of EHR or PHI system auditing
- Backups not sound
- Doors to clinical area not locked
- Encryption not being used
- Outsourced access(i.e. transcription, billing)
- Remote access
- Historical records
- **Minimum necessary standard – electronic systems**

MentorHealth

Training Tips for General Medical Setting

- Every staff member in the office should be apprised of HIPAA standards and held accountable
- Do not discuss sensitive issues when the patient is standing in the reception window and within earshot of those in the waiting room
- Not only are health related issues confidential but insurance and billing discussions should be private as well
- When retrieving a patient from the waiting room for their appointment, use only first name
- When providing patients with drug samples, also provide a bag for them to discretely carry the medication through the waiting room

MentorHealth

Training Tips for General Medical Setting

- When placing charts for the physician, position in such a way that patient names are not visible
- Use a patient sign-in system that allows the reception staff to remove or obstruct the name after sign-in
- All physician offices should have a partition system so that those in the waiting area cannot hear business conducted by staff members
- When making appointment reminder phone calls to patients, exercise caution if you reach an answering machine and be certain not to leave overly detailed information in your message

MentorHealth

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***

MentorHealth

What can you do to mitigate risk with internal staff?

- Educate, educate, educate
- Understand personal responsibility aspects of HIPAA
- ALWAYS REPORT A BREACH IF HAPPENS
- Audit systems

MentorHealth

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.

MentorHealth

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
- 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

MentorHealth

Business Associates

- Disgruntled
- Does not protect your private health information adequately
- Ignorant of their responsibility
- A breach of your practices/businesses private health information, albeit the fines are levied against the business associate, can certainly spurn an audit. Or at the very least put egg on your face via the breach notification rule.

MentorHealth

How to mitigate risk from an audit caused by a business associate?

- What are their policies?
- Keep an eye on them
- Educate them – let them know THEY are entirely responsible under HIPAA for YOUR private health information
- Ask questions
- BE SURE A BUSINESS ASSOCIATES AGREEMENT IS IN PLACE

MentorHealth

Not reporting a breach

- Breach Notification Rule requires that a breach of a patient's health information be reported.
- If a breach is not reported you will be fined heavily
- It's true reporting a breach will increase chance of audit but NOT reporting a breach is big, big trouble
- They'll never catch me….
  - YES THEY WILL

MentorHealth

How to mitigate risks of a breach?

- CONDUCT A RISK ASSESSMENT
- Put proper policies in place
- Train staff
- Have good business associates
- Good IT practices
- Minimum Necessary standard
- Audit

MentorHealth

DISASTER

- Complete system outage and private health information cannot be accessed in a timely manner
- Patients under HIPAA have a right to their private health information
- Is private health information protected from unforeseen situations? Earthquake? Fire? Theft? Tornado?

MentorHealth

OMNIBUS and Suing

MentorHealth

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.

MentorHealth

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.

MentorHealth

Can a Patient Sue?

NOT UNDER FEDERAL LAW!!

HIPAA penalizes the violators on behalf of the patients and so the patients have no right to sue even when a gross HIPAA violation occurs.

Also if monetary fines are paid, they go straight to the Government and not to the patients.

HOWEVER PATIENTS CAN NOW SUE UNDER STATE LAW AND THE FEDERAL GOVERNMENT IS ENCOURAGING THIS!!

MentorHealth

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.**

MentorHealth

Questions

If there are any further questions which we were not able to get to today please feel free to contact me.

MentorHealth

Contact Us:

- *Customer Support at : 1.800.447.9407*
- *Questions/comments/suggestions: webinars@mentorhealth.com*
- *Partners & Resellers: partner@mentorhealth.com*