



Live Webinar
on
**HIPAA –
Texting/Emailing/BYOD**

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

Wednesday, April 20th, 2016 – 1.00 pm EDT

© MentorHealth 2016



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

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

5

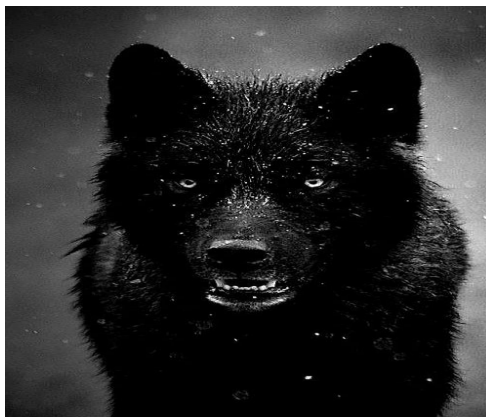


BOY WHO CRIED WOLF

6



Well the Wolf is Here



7



HIPAA Before Omnibus (September 23, 2013)



8



HIPAA After Omnibus (September 23, 2013)



Destructive like my dog....





D-DAY

9-23-2013



11



Background

- 2009 HITECH Act & The Affordable Care Act (Obamacare) & 2013 Omnibus Rule – 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.

12



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
- Every year since Omnibus fines have increased
- Individual Remedies

13



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)

14



Background

- Audits have begun in earnest
- Audits are targeting practices and business associates of all sizes, not just large entities
- Clearinghouses and insurance companies are also at risk
- The federal government is not accepting the same old excuses anymore

15



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

YES!!

CONSTANTLY REINFORCE THIS TO STAFF

16



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

YES!!

17



Business Associate (Definition)

- Business Associates (BA's) are individuals or entities who create, receive, maintain, or store private health information on behalf of a covered entity.
- Example: Answering Services, Medical Transcription, IT groups, Billing companies, shredding services are clearly under the auspices of "Business Associate"

18



OMNIBUS AND BUSINESS ASSOCIATES (cont)

- The OMNIBUS Rule requires business associates to comply directly with HIPAA regulations themselves.
- BA's must now
 - **develop policies and procedures for HIPAA**
 - **train staff**
 - **conduct risk analysis**
 - **be subject to federal inspections**
 - **Monitor covered entities where a BA exists**
 - **Have BAA's with sub-contractors**
 - **Be subject to the Breach notification Rule**

19



OMNIBUS AND BUSINESS ASSOCIATES (cont)

Although Uncle Sam poses risks to business associates in terms of audits:

The real risks tend to be with future and current clients of BA's

- **Losing clients**
- **Unable to get new clients**
- **Covered entities requesting more from BA's than just the business associate agreement**
- **Covered entities want to see policies, proof of risk assessment, etc.**

20



Now to the subject at hand....



I 
Texting



The HIPAA Security Rule tells us this...

§ 164.308 Administrative Safeguards

Standard: *Security Management Process*

Implement policies and procedures to prevent, detect, contain, and correct security violations.



<http://www.hhs.gov/hipaa/for-professionals/faq/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?

23



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.

24



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.

25






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.




26



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.

27



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.

28



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

29






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

30







SO HOW DOES THIS APPLY TO US?

LET'S FIGURE IT OUT USING THE SPECIFIC HIPAA GUIDELINES

REMEMBER -EVERYTHING IS BASED ON RISK

31

Straight from Uncle Sam
The HIPAA Security Rule tells us this...
 § 164.308 Administrative Safeguards.

Standard: ***Security Management Process***

Implementation Specification:

Risk Analysis (REQUIRED)

“Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.”

IN PLAIN ENGLISH – Find the risks!

32



Straight from Uncle Sam

The HIPAA Security Rule tells us this...

§ 164.308 Administrative Safeguards.

Standard: **Security Management Process**

Implementation Specification:

Risk Management (REQUIRED)

*Implement security measures sufficient to reduce risks and vulnerabilities to **reasonable and appropriate** levels*

IN PLAIN ENGLISH – Fix the problems!!

33



KEY WORDS ESSENTIAL TO
UNDERSTANDING HIPAA!!!

REASONABLE

and

APPROPRIATE

34



CONFUSED?

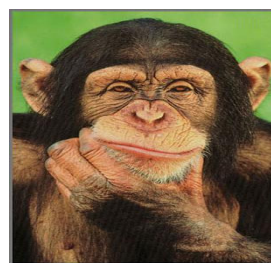


35



Let's Get Specific....

How does this apply to
email/texting? Hmm...



36



The HIPAA Security Rule tells us this...

§ 164.312 Technical safeguards.

Standard: **Access control**

Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights

37



Straight from Uncle Sam

The HIPAA Security Rule tells us this...

§ 164.312 Technical safeguards.

Standard: **Access control**

Implementation Specification:

Encryption and Decryption (Addressable)

“Implement a mechanism to encrypt and decrypt electronic protected health information”

In plain English: Is there a high risk that PHI can be compromised at rest?

38



Remember *Encryption and Decryption* is Addressable.

If we are not encrypting the data at rest what other things are being done to mitigate risks to *reasonable and appropriate* levels? Examples:

- strong usernames and passwords,
- enterprise level professionally configured firewalls,
- strict hiring procedures,
- strong physical security,
- role based access/minimum necessary,
- audit controls,
- Etc...



The HIPAA Security Rule tells us this...

§ 164.312 Technical safeguards.

Standard: *Transmission Security*

Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

Note: This is clearly the most applicable aspect to emailing and texting of protected health information and what HIPAA says



Straight from Uncle Sam The HIPAA Security Rule tells us this...

§ 164.312 Technical safeguards.

Standard: *Transmission Security*

Implementation Specification:

Integrity Controls (Addressable)

“Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.”

In plain English: What measures are planned to protect EPHI in transmission?

41



Remember *Integrity Controls* are Addressable.

To protect data in transmission what is being done to mitigate risks to *reasonable and appropriate* levels?

Let's take a deeper look:

- Are there adequate assurances PHI is not getting altered?
- What type of PHI is being transmitted?
- How often is PHI transmitted via non-encrypted means?
- Where is the PHI being transmitted to?

42



Straight from Uncle Sam The HIPAA Security Rule tells us this...

§ 164.312 Technical safeguards.

Standard: *Transmission Security*

Implementation Specification:

Encryption (Addressable)

Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

In plain English: Is encryption reasonable and appropriate for EPHI in transmission?

43



Remember: *Encryption* (via transmission) is Addressable.

What is being done to mitigate risks to *reasonable and appropriate* levels?

Let's take a deeper look:

- Is encryption needed to effectively protect the information?
- Is encryption cost-effective and feasible?
- What encryption mechanisms are available?
- Does the organization have appropriate staff to maintain a process for encryption PHI during transmission?
- Are staff members skilled in the use of encryption?

44



Is encryption needed to effectively protect the information?

It depends....

What are the identifiers? (i.e. basic tooth x-ray vs HIV records)

How often is transmitting PHI done? (i.e. if done often and a critical part of the organization - *reasonable and appropriate* would dictate that encryption is needed)

45





Is encryption cost effective and feasible?

It depends....








What is the size and scope of the organization? (i.e. if emails/texts are only transmitted on a rare occasion it is not necessarily a high risk which would warrant a large cost)

HOWEVER: Costs for 3rd party encryption software (both for text and email) is very reasonable these days

46

Secure Texting 3rd Parties Applications
Based on my review of the below, costs are clearly reasonable and appropriate



47

Secure 3rd Parties Applications for Email
Based on my review of the below, costs are clearly reasonable and appropriate



48



***What if a patient wants their health record sent to their
Yahoo email account and we don't have encryption?***



***Have them sign a *Request for Confidential
Communications* form***

REQUEST FOR ELECTRONIC COMMUNICATIONS

Name of Patient: _____

Date of Request: _____ Date of Birth: _____

I request that the following communications from the practice be delivered to me by the provided electronic means. I understand that this form of communication may not be secure, creating a risk of improper disclosure to unauthorized individuals. I am willing to accept that risk, and will not hold the practice responsible should such incident occur.

Communications
 _____ Appointment reminders _____ Prescription refill reminders
 _____ Other (list specifically): _____

Method
 _____ E-mail Address: _____
 _____ Text Phone Number: _____

Time period for this method _____

Acknowledgement and Agreements: I understand and agree that the requested communication method is not secure, making my PHI at risk for receipt by unauthorized individuals. I accept the risk and will not retaliate against the practice in any way should this occur.

SIGNED: _____ Date: _____



Print Name: _____ Phone No.: _____

Address: _____


Personal Representative: _____

Request Received By/Date: _____

51

BYOD



BYOD

BRING YOUR OWN DEVICE

52



BYOD

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

53



Conundrum

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

54



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.)

55



Positives

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

56



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

57



Negatives

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

58



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)

59



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)

60



Best Practices

- Train staff on appropriate apps and software as well as cyber threats
- Force complexity in the passwords
- Perform risk assessments annually to identify threats

61



#1 Compliance Worry with BYOD



62



Mitigating Steps for Theft

- PASSWORD PROTECT PRIOR
- Remote Tracking – GPS tracking ability, this is now standard on iPhones using “Find my iPhone” function or laptop tracking
- 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)

63



TEXTING and HIPAA



64



Can you use texting to communicate health information, even if it is to another provider or professional?

<https://www.healthit.gov/providers-professionals/faqs/can-you-use-texting-communicate-health-information-even-if-it-another-p>

It depends. Text messages are generally not secure because they lack encryption, and the sender does not know with certainty the message is received by the intended recipient. Also, the telecommunication vendor/wireless carrier may store the text messages.

However, your organization may approve texting after performing a risk analysis OR implementing a third-party messaging solution that incorporates measures to establish a secure communication platform that will allow texting on approved mobile devices

65



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

66



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

67



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 PHI to patient (i.e. text message is used to make a judgement in patient care)

68



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

69



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 applications

70



ENCRYPTION POLICY EXAMPLE



71



Laptops, Mobile Computer & Smart Devices

- All laptop computer devices must have approved encryption software installed prior to their use within network. In addition to encryption software the laptop must be password protected and have up to date anti-virus installed prior to their accessing or storing any confidential information.
 - The mobile computer devices & smart devices must have device encryption enabled or IT approved encryption software installed prior to accessing or storing any confidential information.
 - The preferred method of encryption for laptop computers, mobile computer devices and smart devices is whole disk encryption. Mobile computer devices and smart devices which are not capable of whole disk encryption must use file/folder level encryption to encrypt all confidential information stored on the device.
 - Laptop, mobile computer devices and smart devices MUST NOT be used for long-term storage of confidential information
- **NOTE: Microsoft Windows 8 or newer comes with free built in whole disk encryption called Bit Locker**

72



Transmission Security Policy

All protected health information transmitted through email to an email address **outside** of the domain must be encrypted or the patient must sign off on the Request for Confidential Communications form.

The transfer of such information outside of the domain must be authorized by senior management.

The authorization must be issued in advance of the first instance and will apply thereafter if necessary.

73



Removable Storage Devices

- All confidential and restricted information stored on removable storage devices must be encrypted. In addition to being encrypted, removable storage devices must be stored in a locked area when not in use.
- The preferred method of encryption for removable storage devices is whole disk/device encryption. Where whole disk encryption is not possible, then file/folder level encryption must be used to encrypt all confidential information stored on the removal storage device

74



USB Memory Sticks

- Confidential information may only be stored on approved encrypted USB memory sticks.
- Business approved USB memory sticks must only be used on an exceptional basis where it is essential to store or temporarily transfer confidential information. They **MUST NOT** be used for long term storage of confidential information.
- Confidential information stored on the approved USB memory stick **MUST NOT** be transferred to any internal (except a secure GET server) or external system in an unencrypted form.

75



OMNIBUS and Suing



76



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.

77



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.

78



State Laws

States are falling like dominos



- Individual court cases filed citing HIPAA violations are creating precedence

79



REMEMBER TO CONDUCT RISK ASSESSMENT

As quoted in from HIPAA's Security Rule (CFR) 164.308(a)(6), a covered entity is required to conduct a Risk Assessment:

- “identify and respond to suspected or known security incidents; mitigate, to the **extent practicable**, harmful effects of security incidents known to the covered entity; and document security incidents and their outcomes.”
- “*implement security measures sufficient to reduce risks and vulnerabilities to a **reasonable and appropriate** level to comply with 164.306 (a) [(the general requirements of the security rule)]*”

** The Risk Assessment is the building blocks for your policies and procedures. In fact, conducting a Risk Assessment is a “required” part of the HIPAA Security Rule!**

80



<http://www.healthit.gov/providers-professionals/security-risk-assessment-tool>

HealthIT.gov

Providers & Professionals Patients & Families Policy Researchers & Implementers

Benefits of EHRs How to Implement EHRs Privacy & Security EHR Incentives & Certification Success Stories & Case Studies Resource Center

Security Risk Assessment

Security Risk Assessment Tool (SRA Tool?)

What is the Security Risk Assessment Tool (SRA Tool)?

The Office of the National Coordinator for Health Information Technology (ONC) recognizes that conducting a risk assessment can be a challenging task. That's why ONC, in collaboration with the HHS Office for Civil Rights (OCR) and the HHS Office of the General Counsel (OGC), developed a downloadable SRA Tool (see - 66 MB) to help guide you through the process. This tool is not required by the HIPAA Security Rule, but it is designed to assist in compliance and demonstrate compliance.

SRA Tool (Windows version)

SRA Tool (iPad version)



<http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf>

NIST Special Publication 800-66-Revision 1

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule

Matthew Schell, Kevin Stone, John Hark, Pauline Brown, Arnold Johnson, Carl Dancy Smith, and Daniel I. Steinberg

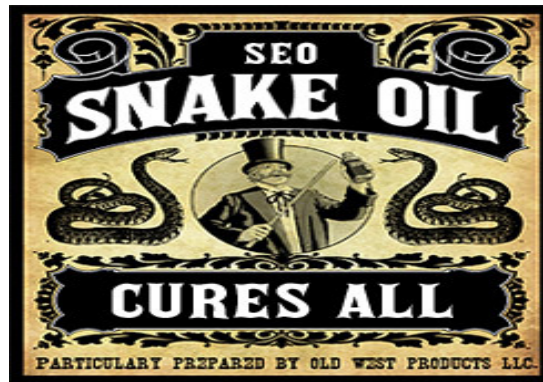
INFORMATION SECURITY

October 2008

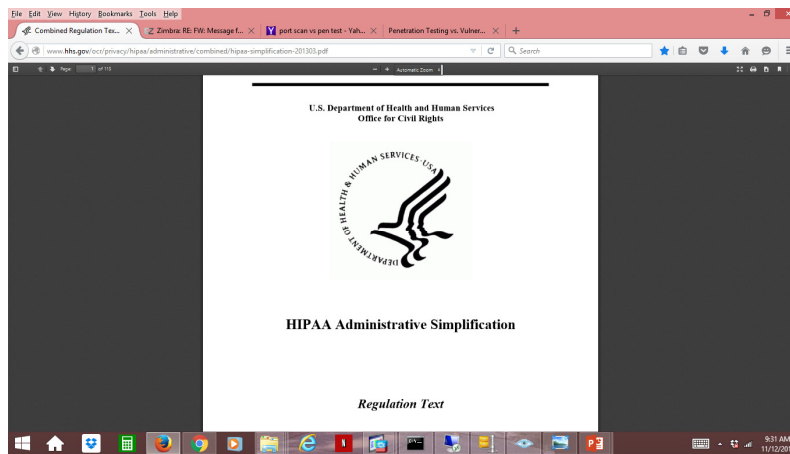
U.S. Department of Commerce
National Institute of Standards and Technology
Special Publication 800-66-Revision 1



ALWAYS FACT CHECK WITH [WWW.HHS.GOV](http://www.hhs.gov)
DON'T FALL FOR SNAKE OIL!!



<http://www.hhs.gov/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf>





FACTORS THAT CAN SPURN AN OCR AUDIT



85



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

1. *INTERNAL STAFF*
2. *PATIENTS/CLIENTS*
3. *MEANINGFUL USE (for covered entities)*
4. *BUSINESS ASSOCIATES/SUB-CONTRACTORS*
5. *PREVIOUS or CURRENT BREACH*
6. *NOT REPORTING A BREACH*
7. *DISASTER*
8. *BAD TECHNOLOGY*

86



Hypothetically -What is involved in an audit?

“Depending on size and scope - Site visits conducted as part of every audit would include interviews with leadership which may include, practice manager, HIPAA Privacy Officer, HIPAA Security Officer, CIO, legal counsel, medical records manager; **examination of physical features** and operations; **consistency of process to written policy**; and observation of compliance with regulatory requirements.” - www.hhs.gov

87



So far...

- The results of the OCR audits confirmed many suspicions...
 - **Small providers** had many more issues than the larger ones
 - **Healthcare providers and Business Associates** had more issues than clearinghouses or plans
 - **HIPAA Security Rule** is (by far) the biggest concern (**65%**) compared to HIPAA Privacy (26%) and Breach Notification Rule (9%)

88



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.

89



Best Course of Action

BE PROACTIVE!!



90



Questions

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



91



Contact Us:

- **Customer Support at :**
1.800.385.1607
- **Questions/comments/suggestions:**
webinars@mentorhealth.com
- **Partners & Resellers:**
partner@mentorhealth.com

92