Note: Legal and high-tech security issues are complex and highly fact-specific. (Some legal issues are also state-specific.) They require legal or technical expertise that cannot be provided in this forum. APA and APA Services Inc. attorneys do not, and cannot, provide legal advice to our membership or state associations. Any references to technical/security products or services in this presentation is not an endorsement in any way of those products or services. The information in this presentation does not constitute and should not be relied upon as legal or technical advice, and should not be used as a substitute for obtaining personal legal or technical advice and consultation prior to making decisions.
Chair & Presenters:

Chair and Presenter:
Alan Nessman, JD
Senior Special Counsel,
Office of Legal & Regulatory Affairs, APA

Presenters:
Deborah Baker, JD
Director, Legal & Regulatory Policy,
Office of Legal & Regulatory Affairs, APA

Brad Steinbrecher, JD
Director, Legal & Regulatory Affairs,
Office of Legal & Regulatory Affairs, APA

Nanci C. Klein, PhD
Director of Professional Affairs,
Utah Psychological Association
@drklein
Overview of today’s presentation:

Introduction
Potential changes to HIPAA
  Request for Information on potential changes to Privacy Rule
  Proposed rule on Electronic Health Information

HIPAA Refresher & Myths
  • HIPAA Basics
  • Privacy Rule
  • Security Rule & Tech issues
  • Breach Notification

Questions from the Audience
Introduction

HIPAA remains a major area of legal compliance hassle, worry and confusion for members.

Potential changes to HIPAA may add to the confusion.

APA Practice’s Office of Legal & Regulatory Affairs, working with our SPTA partners, is here to help and advocate.
The 3 HIPAA Rules psychologists need to know

**Privacy Rule:** Covers how you handle patient information and your *intentional* disclosures of that information. Also gives patients important rights re their Protected Health Information (PHI).

**Security Rule:** Applies to PHI that you store or transmit *electronically*. It requires that you have safeguards in place to prevent *unintended disclosure* or *loss* of ePHI.

**Breach Notification Rule:** Determines when the loss or theft of PHI is a “breach” that you need to notify affected patients and HHS about.
HHS Request for Information - background

• In December 2018, HHS’s Office for Civil Rights (OCR) issued a “Request for Information on Modifying HIPAA Rules to Improve Coordinated Care” (https://www.regulations.gov/document?D=HHS-OCR-2018-0028-0001)

• After seeking input from APA members knowledgeable in integrated/coordinated care, APA submitted comments in response to the RFI on February 12, 2019.

• RFI describes the changes OCR is considering and the rationale, and requests public input on specific questions.

• First step in the federal rulemaking process. RFI → Proposed Rule → Final Rule.
Title: “Request for Information on Modifying HIPAA Rules to Improve Coordinated Care”

Purpose: to identify HIPAA provisions that may be impeding the transformation to value-based health care or limiting care coordination

Request: “information on whether and how the rules could be revised to promote these goals, while preserving and protecting” patient privacy
HHS Request for Information - contents

RFI contained well over 100 questions, broken down into five main areas:

- Promoting Information Sharing for Treatment and Care Coordination
- Promoting Parental and Caregiver Involvement and Addressing the Opioid Crisis and Serious Mental Illness
- Accounting of Disclosures
- Notice of Privacy Practices
- Additional Ways to Remove Regulatory Obstacles and Reduce Regulatory Burdens to Facilitate Care Coordination and Promote Value-Based Health Care Transformation
Representative questions:

• “How feasible is it for covered entities to provide PHI when requested by the [patient] more rapidly than currently required under the rules?”

• “Should covered entities be required to disclose PHI when requested by another covered entity for treatment purposes?”

• “Should OCR modify the Privacy Rule to clarify the scope of covered entities’ ability to disclose PHI to social services agencies and community-based support programs where necessary to facilitate [coordination of care]?”
APA’s general response to HHS/OCR:

• Majority of clinical psychologists work in small practices, with very limited legal/administrative support

• Many of these potential changes (e.g., greater required disclosures and accounting, shorter timeframes) would be burdensome to small practices and difficult to implement

• If OCR moves forward with these changes → implement a small practice exception that carves out small and solo practices

• Many of the changes would permit/require greater disclosures for treatment/payment purposes. In most states, those changes would be preempted by state mental health privacy and confidentiality laws that are more protective than HIPAA.
Takeaways:

• HHS is thinking about changing the HIPAA Rules to facilitate the flow of PHI between and among patients, providers, and entities involved in care coordination.

• Many of the changes being contemplated would be burdensome to small practices. APA pushed back on that and will continue to do so.

• If HHS moves forward, timing is unknown (Proposed Rule in 2019/2020?)

• Stay tuned:
  • Monitor the APA Services website -- https://www.apaservices.org/practice
  • Sign up for the OCR Privacy Listserv -- https://www.hhs.gov/hipaa/for-professionals/list-serve/index.html
CMS Proposals on Interoperability & Patient Access

- Proposed rulemaking issued March 4, 2019
- Comments due by May 3, 2019
- Enable patient access to their health information electronically requiring payers to make patient data available through open APIs consistent with ONC standards
- Plans must share patient information (at patient’s request) with a new plan or other entity designated by the patient for up to 5 years after the patient has disenrolled with the plan
- Require provider network information available to patients through API technology
- Publish names of providers (equipped with EHRs) who engage in information blocking that is not otherwise allowed by HIPAA or other privacy laws
- 21st Century Cures Act requires creation of a provider digital contact information index
- Propose publicly reporting names & NPIs of those providers who do not add their information to NPPES by mid-2020
- Applicable to Medicare Advantage organizations, Medicaid state agencies, state CHIP agencies, Medicaid managed care plans, CHIP managed care & QHP issuers in FFEs
General HIPAA

This and Privacy Rule sections are covered by *Privacy Rule Primer* available at: https://www.apaservices.org/practice/business/hipaa/hippa-privacy-primer.pdf
General HIPAA

Most psychologists trigger HIPAA by:
• Electronically transmitting
• PHI
• In connection with a patient’s health insurance claims, e.g., claims to private or government insurers

Once you trigger HIPAA, it applies to your whole practice
BASIC COMPLIANCE STEPS

Privacy Rule
1. Understand Privacy Rule requirements and how they interact with your state law.
2. Give patients notice of your privacy practices and their privacy rights.
3. Have a business associate contract with outside entities who handle PHI for you (e.g., billing services and accountants).
4. Use other required forms to comply with the Rule, such as patient authorization forms.

Security Rule
1. Risk assessment
2. Risk management
3. Periodic reassessment
BASIC COMPLIANCE STEPS, cont’d

Breach Notification Rule:

Need to understand:

1. What is a “breach” of your PHI
2. If you have a breach, how and when you need to notify patients and the government

Steps required by multiple rules

1. Adopt and follow policies and procedures for all 3 HIPAA rules
2. Train employees so that they understand all your HIPAA policies and procedures
3. Designate a Privacy Officer and a Security Officer
4. Have a process for patient HIPAA complaints
5. Retain HIPAA documentation for 6 years
6. Update your HIPAA policies if necessary due to changes in the law or in your practice
General HIPAA: Myth or Fact?

1. The current Administration may be anti-regulation but it’s enforcing HIPAA aggressively.

2. My clinical practice my trigger HIPAA, but my forensic practice is separate and not health care so I don’t need to follow HIPAA for that part.

3. A list of patient contacts, without clinical records, can be PHI.

4. HIPAA sets a 6-year retention period for clinical records.

5. Using a traditional fax machine triggers HIPAA.
Privacy Rule: Myth or Fact? cont’d

1. I own the record so I don’t have to give patient a copy.
2. If the patient wants their records, I can just give them a summary instead because state law allows that.
3. Authorizations can’t last more than a year.
Privacy Rule: Myth or Fact? Cont’d

1. Because I can’t find an email service that will give me a Business Associate Agreement, it’s OK not to have a BAA.

2. Patients don’t have a right to raw test data because that would be an Ethics Code violation.

Resources:

1. “Nuts and Bolts of Business Associate Agreements,” S. Larson, JD, PsyD, Good Practice, Winter 2019 at p. 21. Sidebar has a list of cloud storage, text and email vendors who will sign a BAA.

SECURITY RULE MYTH: Skype is encrypted so it is ok to use with my patients.

- Encryption does not apply to Skype audio phone calls.
- While Skype uses encryption, it does not keep an audit trail, which is required by HIPAA.
- Skype has shared information with law enforcement suggesting that Skype has the encryption key allowing it to access calls.
- The regular, free version of Skype does not offer a BAA.
- Microsoft (which owns Skype) may share your personal and traffic data with other parties.
- Other commercial video-conferencing platforms provide better security & reliability for HIPAA compliance.
SECURITY RULE MYTH: Email is ok if my patient consents to it.

Providers should warn patients that email communications via the internet are not secure & discuss the risks of using email that includes patient health information (PHI).

HIPAA does not prohibit the use of email for sending ePHI.

But providers must take precautions to protect the integrity of ePHI and protect information shared over open networks. This includes considering whether to use encryption.

While HIPAA does not require encryption for email, encryption is a good defense if there is a security data breach.

Providers should be prepared to use email for certain communications, if requested by the patient. But must take steps to ensure they are not exposing information the patient does not want to be shared.

Consider using encrypted email service, sending files that are encrypted if using unsecure email or using an EHR with a secure patient communications portal.
SECURITY RULE MYTH: The Security Rule is too complicated and expensive so I shouldn’t bother.

- HIPAA requires that all covered entities comply with the Security Rule.
- All covered entities must comply with each of the Security Rule standards (administrative safeguards, physical safeguards & technical safeguards).
- BUT small providers are not expected to comply with Security Rule requirements in same way or on same scale as larger providers.
- BUT cost alone is not an acceptable reason to avoid complying.
How you implement each Security Rule standard is based on following:

- **Risk analysis** – What are the current circumstances leaving your practice open to unauthorized access & disclosure of patients’ electronic PHI?
- **Security analysis** – What security measures do you already have in place or could you reasonably put into place to protect patients’ ePHI?
- **Financial analysis** -- How much would complying with a particular standard cost?

Risk Analysis & Risk Management are 2 mandatory requirements

**Risk Analysis**

- Identify all electronic PHI created, received, stored & transmitted in your practice (where & how is that information stored?)
- Identify all potential risks & vulnerabilities (natural, human & environmental threats?) **in writing**
- Assess current security measures – technical & non-technical
- Rate “likelihood of occurrence” for identified threats/vulnerabilities (high, medium or low)
- Identify in writing steps to minimize risk to appropriate & reasonable level

**Risk Management** = ongoing obligation to assess & adhere to security plan

Reality is that with smaller practices, more control of ePHI with fewer staff & smaller scaled IT system so measures taken will be different compared to larger practices/systems
PROTECTING PHI IN 21ST CENTURY: ELECTRONIC HEALTH INFORMATION

- With expansion of digital age even psychologists with no interest in providing services remotely are being confronted by issues having to do with new internet & computer-based technologies

- Facebook, Google, cyber reviews & attacks, email, texting, Twitter, Skype, real time audio & visual technology, encryption & computer security are impacting almost all psychologists; questions regarding the internet and digital communication have arisen for psychologists
TECH ISSUES

- Email
- Texting
- Social media
- Cloud
TECH ISSUES

- Time of tremendous change in development & handling of PHI
- Fast-paced evolution of digital technology & emerging problems in software security require psychologists to keep up-to-date with changes related to privacy risks
- The rest of my presentation will focus on a key tech/security issues that members struggle with: encryption
**ENCRYPTION Cont’d**

▸ Used for thousands of years to protect trade, military, & other secrets; only recently publicly available & easier to use

▸ Widely accepted method for protection of digital info

▸ PHI encryption standard set by HIPAA’s Breach Notification Rule is 128 bit minimum

▸ For secure email encrypt 3 things: connection from your email provider; actual email messages; stored, cached, or archived email messages
Encryption cont’d

Resources for encryption software

• The 5 Best Secure Email Services for 2018
  https://www.lifewire.com/best-secure-email-services-4136763

• Best Email Encryption Services for Small Business in 2018
  https://blog.encyro.com/best-email-encryption-services/

• The 11 Most Secure Email Services for Better Privacy
  https://www.maketecheasier.com/secure-email-services/
Encryption is feasible option sending PHI via email

Less realistic option for text messaging

HIPAA texting policy derived from risk assessment: stipulate under what circumstances it is allowable to communicate PHI by text; include guidelines for the way in which PHI should be communicated by text; & what sanctions will be applied if the HIPAA texting policy is not followed
End-to-End Encryption Explained

1. When Alice starts the app, a private and public key are generated.

2. Alice's private key never leaves her phone. Her public key is stored on a server, available to all who send her a message.

3. When Bob writes to Alice, her public key is retrieved and used to encrypt his message in such a way that only Alice's private key can decrypt it.

4. An encrypted file is sent through the server to Alice.

5. The file is received by Alice and her private key is used to decrypt the message.

Prime Numbers & Encryption

11 × 17 = 187
The product of 2 large random prime numbers is the backbone of encryption.

Cracking the encryption means figuring out the 2 factors. Using brute-force, it takes decades with today’s computers. If the 2 numbers are known (a private key), a split second is all it takes.

17,425,170
The number of digits in the largest known prime number.

Cracking the public key is made up in part by calculating the number of integers that share no common factors that are less than the product of the 2 prime numbers (encryption is supposed to be confusing).
End-to-end encryption means encrypting communications in order to make information unavailable to third parties. So when two or more devices communicate via an app that features this level of encryption, the information will be transmitted using a secret code rather than insecure plain text.
Although encryption in transit is widely used, it has serious security problems. For example, the service provider could be hacked by an adversary, or compromised by an insider, causing sensitive information to be leaked. A fault in the service provider could cause data to be corrupted.

For these reasons, security experts are pushing towards widespread use of end-to-end encryption, which reduces the exposure to such attacks.
Most secure messaging apps:

- WhatsApp
- Viber
- LINE
- Telegram
- KakaoTalk
- Signal-Private Messenger
- Dust
- Threema
- Wickr-Secure Messenger

Breach & Breach Notification

• Brief overview only!

• For more in-depth explanation and guidance:
Breach – definition / examples

• A breach is a use or disclosure of PHI that violates the Privacy Rule and that compromises the security or privacy of the PHI.

• Common examples of potential breaches:
  ▪ a lost or stolen laptop or smart phone containing patient information
  ▪ someone hacking into your practice’s computer system
  ▪ an employee looking at PHI they’re not supposed to access
Breach Notification

• If you have a breach, you must give breach notification to affected patients and HHS.

• *However* – you don’t have to give notification if the breached PHI is encrypted to government standards.

• You also don’t have to notify patients/HHS if you can demonstrate that there is a “low probability” that the PHI has been compromised.
Breach Notification (cont.)

• If you have a potential breach, conduct a risk assessment to determine the probability that the PHI has been compromised. Risk assessment looks at four factors.

• Taken together, do the four factors indicate a low probability that the breached PHI has been compromised?

• If yes → you do not need to give breach notification.

• If no → you need to give notification to affected patients and to HHS (unless the PHI was encrypted to government standards).
Breach Notification (cont.)

• If you’re not sure whether there’s a low probability or not, we recommend that you go ahead and give notification.

• Regardless of what you decide, you should document your risk assessment (summarize your analysis of the four factors and why you reached your decision to give notification or not).
Breach Notification Myth: Breaches are only an issue with PHI stored in an electronic format

- PHI in hard copy, paper format can be breached just as much as electronic PHI can.
- Hypothetical:
  - Your office was broken into and your locked file cabinet with paper patient records was pried open.
  - You suspect the intruder was the spouse of a patient going through a contentious divorce because no valuables have been taken and only that patient’s file was opened – and because the spouse had made threats about taking drastic action.
- Breach! → need to notify the patient and HHS
THANK YOU

If you have questions, contact Legal Reg at praclegal@apa.org

Reminder: Legal and high-tech security issues are complex and highly fact-specific. (Some legal issues are also state-specific.) They require legal or technical expertise that cannot be provided in this forum. APA and APA Services Inc. attorneys do not, and cannot, provide legal advice to our membership or state associations. Any references to technical/security products or services in this presentation is not an endorsement in any way of those products or services. The information in this presentation does not constitute and should not be relied upon as legal or technical advice, and should not be used as a substitute for obtaining personal legal or technical advice and consultation prior to making decisions.