# HIPAA: Direct Training for Health Care Workforce

**Presented by:**

**Marguerite Ahmann, Briar Andresen and Katie Ilten**

**June 10, 2020**

Fredrikson & BYRON, P.A.

# Overview

- Enforcement landscape
- HIPAA basics
  - Privacy Rule
  - Security Rule
  - Breach Notification Rule
- Common HIPAA issues
- Hypotheticals
- Q&A

# Acronyms

- CE = Covered entity
- BA = Business associate
- BAA = Business associate agreement
- PHI = Protected health information
- NPP = Notice of privacy practices
- OCR = Office of Civil Rights
- CMP = Civil money penalty

# What is HIPAA?

- Health Insurance Portability and Accountability Act
- Protects “protected health information” or PHI
- Gives individuals certain rights with regard to PHI
- Privacy, security and breach notification components
- Sets a floor for the protection of health information

# Enforcement

- The Office for Civil Rights enforces HIPAA
- There is no private right of action under HIPAA
- State attorneys general can bring a civil action on behalf of state residents for HIPAA violations
- Most OCR enforcement actions arise out of investigations of complaints. OCR may also conduct compliance reviews of CEs and Bas.

# Enforcement

- Who can get into trouble?
  - Covered entities
  - Business associates
  - Individuals (egregious, criminal circumstances)
- Potential penalties/enforcement action?
  - Resolution agreement
  - Civil money penalty (i.e., civil fine)
  - Criminal fine and/or imprisonment

# Civil Money Penalties

| Culpability | Minimum penalty per violation | Maximum penalty per violation | Annual Limit |
|---|---|---|---|
| No Knowledge | $100 | $50,000 | $25,000 |
| Reasonable Cause | $1000 | $50,000 | $100,000 |
| Willful Neglect- Corrected | $10,000 | $50,000 | $250,000 |
| Willful Neglect- Not Corrected | $50,000 | $50,000 | $1.5 million |

# State Law

- Some state laws are stricter than HIPAA – i.e., state law may prohibit a CE from making disclosures that HIPAA would otherwise permit
- Where the state law is more protective of health information, follow the state law
- Incorporate state law into policies
- Train staff on state law

# Privacy Rule Basics

- HIPAA permits these Uses and Disclosures:
  - Disclosure to the individual/personal representative
  - Treatment, payment and health care operations
  - Required by law
  - Business associates
  - As authorized by the patient
  - Other

# Other Permitted Disclosures – HIPAA**

- Disclosure to family/friends
- Public health activities
  - To public health authority
  - To report child abuse/neglect
  - To FDA
- Law enforcement purposes
- Abuse, neglect and domestic violence
- Research
- Workers' compensation
- Judicial and administrative proceedings

**Remember that state law may be more protective.

# Disclosure to Family/Friends

- When individual is present (and has capacity) and:
  - Agrees or has previously agreed; or
  - Has had the opportunity to object and does not; or
  - It can be reasonably inferred from the circumstances that the person does not object.
- When individual is unable to consent in an emergency:
  - When professional determines it is in patient's best interests; and
  - Only as directly relevant to the person's involvement in care.
- May use professional judgment to make reasonable inferences about who is permitted to pick up prescriptions, supplies or other similar forms of disclosures of PHI

# Incidental Disclosures

- Allowed if a byproduct of another permissible or required use or disclosure
- CE must have “reasonable safeguards” to protect against impermissible uses and disclosures
- CE must also use “minimum necessary” policies and procedures

# Incidental Disclosures

- Examples:
  - Health care staff may orally coordinate services at nursing stations
  - Nurses or other health care professionals may discuss a patient's condition over the phone with the patient, a provider or a family member
  - A physician may discuss a patient's condition or treatment regimen in the patient's semi-private room
- All about reasonableness

# Minimum Necessary

- Use and disclose only the minimum amount of PHI necessary to accomplish the purpose of the request, use or disclosure
  - Internal uses: use/disclosure should be consistent with job responsibilities

# Minimum Necessary

- The minimum necessary standard does not apply to the following:
  - Disclosures to or requests by a health care provider for treatment purpose
  - Uses and disclosures by or to a patient of his or her own PHI
  - Disclosures made under a valid authorization
  - Disclosures to public officials when disclosure is required by law and the official represents that the information requested is the minimum required for the purpose

# Business Associates

- CE must have a Business Associate Agreement with every Business Associate
- A Business Associate is a person or entity that creates, receives, maintains or transmits PHI on behalf of the CE (e.g., document storage companies, IT vendors, shredding companies, lawyers, outside coders)

# De-identification

- Once information has been de-identified, it is no longer considered PHI
- “De-identified Information” = NOT PHI
  - Doesn’t identify an individual AND
  - No reasonable basis to identify individual
- Two ways to accomplish de-identification
  - Qualified statistical expert OR
  - Safe harbor

# De-identification – Safe Harbor

- Name
- Geographic subdivisions – including zip code
- Elements of dates (except year)
- Telephone number
- Fax number
- E-mail
- SSN
- Medical record number
- Any other unique identifying characteristic or code
- Health plan beneficiary number
- Account number
- Certificate or license number
- License plate number
- Device identifiers
- URLs
- IP address
- Biometric identifiers including fingerprints and voice prints
- Full face photographic images

# Patient Rights

- Right to access
- Right to request restrictions
- Right to amend
- Right to an accounting of disclosures
- Right to confidential communications

# Patient Rights: Access

- A CE has 30 days to provide access
  - One-time 30-day extension
  - If person requests an electronic copy of PHI maintained in a designated record set, must provide access in electronic form/format requested by person, if readily producible, or (if not) in readable electronic format as agreed by CE and individual
    - If the EHR has links to images or other data, the images/data must also be included in the electronic copy provided to the individual

# Patient Rights: Access

- Can send an unencrypted email if CE advises individual of risk and individual still chooses that method
- Not required to permit the patient to use their own portable external media, but a CE can't make a patient buy a thumb drive
- You must have a reasonable electronic format:
    - Consider encrypted emails
    - CD-ROMs with PDFs

# Patient Rights: Access

- If requested by an individual, a CE must transmit the copy of PHI directly to another person designated by the individual
- Request must be in writing, signed by the individual, and clearly identify the designated person and where to send the copy of the PHI
- Different from an authorization

# Patient Rights: Access

- Charging patients – “reasonable, cost-based fee”
- Permits charging only for the labor costs of copying PHI, supplies, postage and labor to prepare summary/explanation (if agreed to in advance)
- Not ok to charge a retrieval fee
- Not supposed to be a revenue stream
- Consider state laws – but keep in mind what is “reasonable”

# Patient Rights: Access

- Three options:
  - Actual costs
  - Average costs
    - Can develop a schedule of costs for labor based on average labor costs to fulfill standard types of access requests
    - Can add any applicable supply/postage costs
    - Can be calculated/charged as a per-page fee only when in paper form
  - Flat fee for electronic copies maintained electronically
    - $6.50
    - Includes labor, supplies and postage

# Patient Rights: Access

- Unencrypted email:
  - Permitted only if the CE advises individual of the risk of no encryption and the individual agrees in writing to receive the unencrypted email
- Reasonable electronic formats:
  - Not required to permit the patient to use their own portable external media
  - A CE cannot make a patient buy a thumb drive
  - Consider patient portals, encrypted emails, or encrypted flash drive with PDF

# Patient Rights: Restrictions

- Right to request restrictions to health plan when paying in full
  - Exception when disclosure is required by law
  - If patients don’t pay, CE can bill insurance
  - Can ask patients to pay up front
  - Can require prepayment where precertification would otherwise be required

# Other Patient Rights

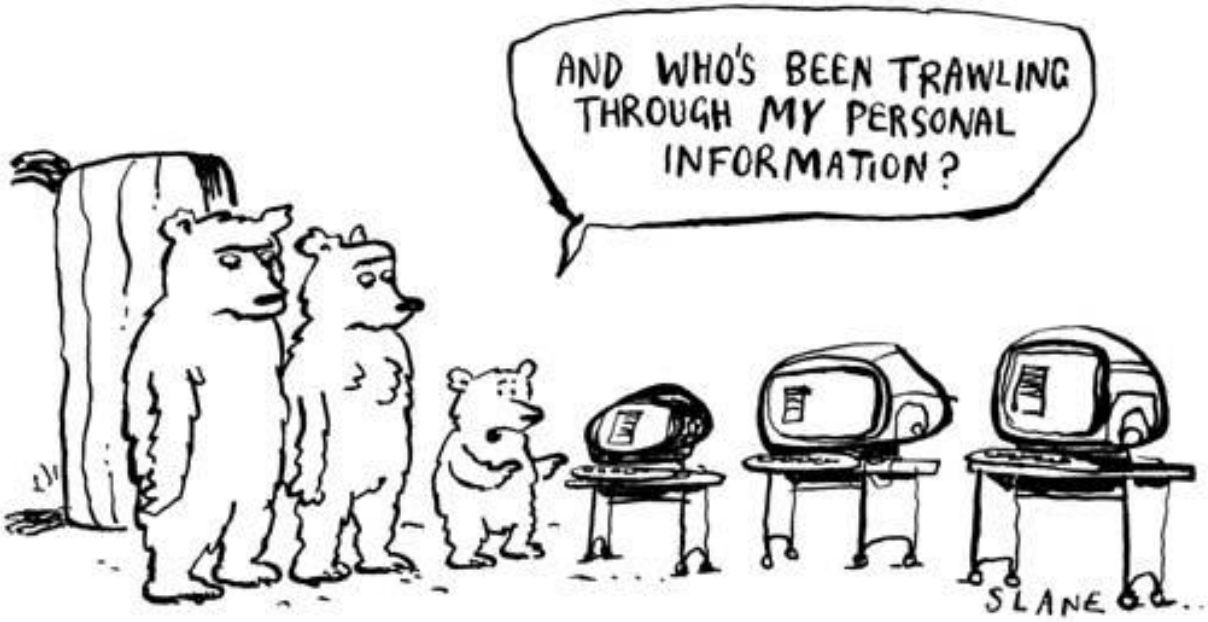
- Right to Request Confidential Communications
  - Must agree to reasonable requests, can't ask why
- Right to Amendment
- Right to Accounting of Disclosures
  - Must account for certain disclosures Don't need to account for:
    - Treatment, payment or health care operations disclosures
    - To individual
    - Incidental/authorized
    - Facility directory
    - National security
    - More than six years prior

# Marketing, Fundraising or Sale of PHI

- Use of PHI to make a subsidized marketing communication requires an authorization
- Sale of PHI requires an authorization
- Use of limited PHI for fundraising purposes is okay
- Take away: tread carefully!!

# HIPAA Authorization

- Receipt of notice of privacy practices is NOT a substitute for a HIPAA authorization
- Requires certain language –
  - Purpose of use/disclosure
  - Right to revoke
  - When CE may condition treatment, etc.



# Security Rule

- Requires covered entities to protect the "confidentiality, integrity, and availability" of **electronic** PHI
- Administrative, physical and technical safeguards
- A ton of guidance from OCR
  - Still difficult to comply completely
  - Need to be vigilant

# Security Rule

- Must perform a security risk assessment and implement protections based on the risk assessment
- Protect against reasonably anticipated threats
- Risk assessment is ongoing process to determine risks to ePHI, wherever it is

# Examples of Threats

- Theft
- Loss
- Malware/hacking/ransomware
- Snooping employee
- Emailing PHI to wrong recipient
- Inadvertent disclosures (exam room PCs)
- Natural disaster

# Security Rule

- CE determines who is responsible for developing and implementing Security Rule policies
- Identify which employees need access to ePHI, and what level of access is required
- Provide security awareness and training

# Security Rule

- Encryption is not required for every CE, but "reasonable" security measures are required
  - OCR may decide that encryption is reasonable for your organization
  - Safest option: if you *can* encrypt, you should . . .

# Security Rule

- Encrypt, encrypt, encrypt:
  - Laptops
  - Phones
  - Flash drives
  - iPads
  - Desktops
- Use passwords as well
- Do periodic Security Rule audits
- If something is NOT encrypted, use extreme caution!

# Malware

- Anchorage Community Mental Health Services paid $150,000 and adopted a corrective action plan after a breach of unsecured ePHI caused by a malware incident affected 2,743 individuals. The investigation revealed ACMHS had adopted sample Security Rule policies and procedures in 2005, but these were not followed. Moreover, the security incident was the direct result of ACMHS failing to identify and address basic risks, such as not regularly updating their IT resources with available patches and running outdated, unsupported software.

# Mobile Devices and HIPAA

- Password protect
- Auto lock/logoff
- Regularly install security patches and updates
- Install or enable encryption, anti-virus/ anti-malware software and remote wipe
- Privacy screen
- Don’t use that camera

# Mobile Devices and HIPAA

- Use only secure Wi-Fi connections
- Use secure VPN
- Prohibit downloading of third-party apps?
- Delete all PHI before discarding or reusing

# Breaches

- What is a breach?
  - An impermissible use or disclosure of “unsecured PHI” is presumed to be a breach unless CE (or BA) can demonstrate that there is a low probability that the PHI has been compromised
- What is “unsecured PHI”?
  - PHI that has not been rendered unusable and unreadable, or encrypted

# Not a Breach!

- Unintentional acquisition or access or use of PHI by an employee if made in good faith and in scope of authority AND doesn't result in further use/disclosure in violation of the rule
- Disclosure made to unauthorized individual who couldn't reasonably retain the information

# Breaches

- Factors to assess the probability that PHI has been compromised:
  - Nature and extent of PHI involved, including identifiers and likelihood of reidentification
  - Unauthorized person who used the PHI or to whom the disclosure was made
  - Whether PHI was actually acquired or viewed
  - Extent to which the risk to the PHI has been mitigated
  - Other factors may be considered “where necessary”

# What if there is a breach?

- CE must report:
  - To the individual
  - To the government
    - Annually, in the CE's breach notification log; and
    - Right away, if the breach involves more than 500 people
  - To the media, if the breach involves more than 500 people
  - May name individuals or BA in notification

# Consequences of a Breach

- Potential bad press
- Financial costs of breaches:
  - Attorney and consultant fees
  - Computer forensic analysis
  - Extra staff time
  - Employee discipline and termination/HR costs
  - Potential penalties (breach reporting is where the government gets much of its information on who is noncompliant)

# Employee Sanctions

- A CE is required by law to sanction employees who violate the HIPAA Privacy or Security Rule
- Any violations of HIPAA will be handled under CE's employee discipline policy, similar to other employee discipline issues
- Sanctions for using or disclosing PHI could include termination of employment, depending on the nature of the violation

# Hypothetical 1

- The patient's chart, with name clearly displayed, is attached to the outside door of examining room for passersby to notice. Is this a HIPAA violation? A breach?

# Hypothetical 2

- Patient brings spouse to every appointment, and spouse sits in the exam room each time. Spouse calls for results of patient's biopsy. May the CE disclose the results to spouse?

# Hypothetical 3

- A hospital employee sees his neighbor at the hospital one morning and later posts on the neighbor's Facebook page, "It was great to see you today!" Is this a HIPAA violation? A breach?

# Hypothetical 4

- A clinic sends an itemized bill to the wrong mailing address; the bill includes the patient's name, CPT codes for services received and patient due amounts. Is this a HIPAA violation? A breach?

# Hypothetical 5

- A clinic sends a group email to patients who may be interested in weight management counseling. The sender fails to “blind copy” the recipients; instead, all of the recipients are visible to each other. Is this a HIPAA violation? A breach?

# Hypothetical 6

- A fitness app developer asks a primary care clinic for a patient list so that the app developer can provide information about the app to patients who have asked the clinic for fitness resources. May the clinic provide the list to the fitness app developer?

# Presenters

**Marguerite Ahmann**
612.492.7495
mahmann@fredlaw.com

**Briar Andresen**
612.492.7057
bandresen@fredlaw.com

**Katherine Ilten**
612.492.7428
kilten@fredlaw.com