“HIPPA”

How
Idiots
Protect
Private (healthcare)
Accounts

Rachel Park Hurt

Arnett, Draper & Hagood, LLP

Security, Privacy, and Breach Notification

- The Health Insurance Portability and Accountability Act. This law is the first comprehensive Federal protection for the privacy of personal health information, passed by Congress in 1996, and implemented in April 2003. The most recent revision was in 2013, with the HIPAA Omnibus Final Rule.
- The Health Insurance Portability and Accountability Act (HIPAA) Security, Privacy, and Breach Notification Rules safeguard the privacy of sensitive health information and give patients certain rights to their health information.
- HIPAA compliance is mandatory.

The Purpose

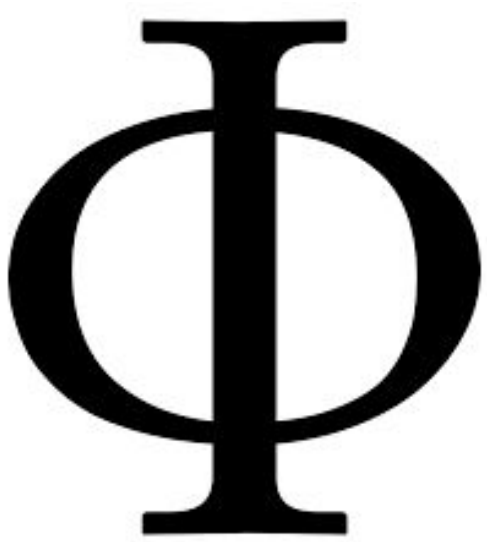
- HIPAA is a federal law enacted to:
  - Protect the privacy of a patient's personal and health information;
  - Provide for electronic and physical security of personal and health information; and
  - Standardize the means by which medical records are disseminated.

What Health Information is Covered

- Individually Identifiable Health Information which includes any information that is:
  - Spoken
  - Written
  - Electronic
  - Related to:
    - Past, Present, or Future Treatment of physical or mental health conditions;
    - Past, Present, or Future physical or mental health condition;
    - Past, Present, or Future Payment of healthcare;
    - Healthcare operations.

What is Protected Health Information (PHI)?

- Information that can be used directly or indirectly to identify an individual
- Includes **Individually Identifiable Health Information** (IIHI) such as:
  - Name
  - Address
  - Birthdates
  - Social security number
  - E-mail addresses
  - Account or Medical record numbers
  - Photographic images
  - Medical Record Numbers
  - Certification/License numbers
  - Phone or Fax numbers
  - Any “other” identifying number, characteristic or code



Patient Rights a.k.a. The Privacy Rule

- HIPAA gives individuals certain rights involving how their PHI is used. By regulation, individuals have the rights to:
  - Access, inspect, and copy their PHI (for example, the individuals' medical and billing records) that is part of a designated record set;
  - Amend or correct PHI that is wrong or incomplete;
  - Obtain an accounting of disclosures of an individual's own PHI;
  - **Request restrictions concerning certain uses or disclosures of PHI; and**
  - Ask that communications of PHI from a health plan be sent using alternative methods.

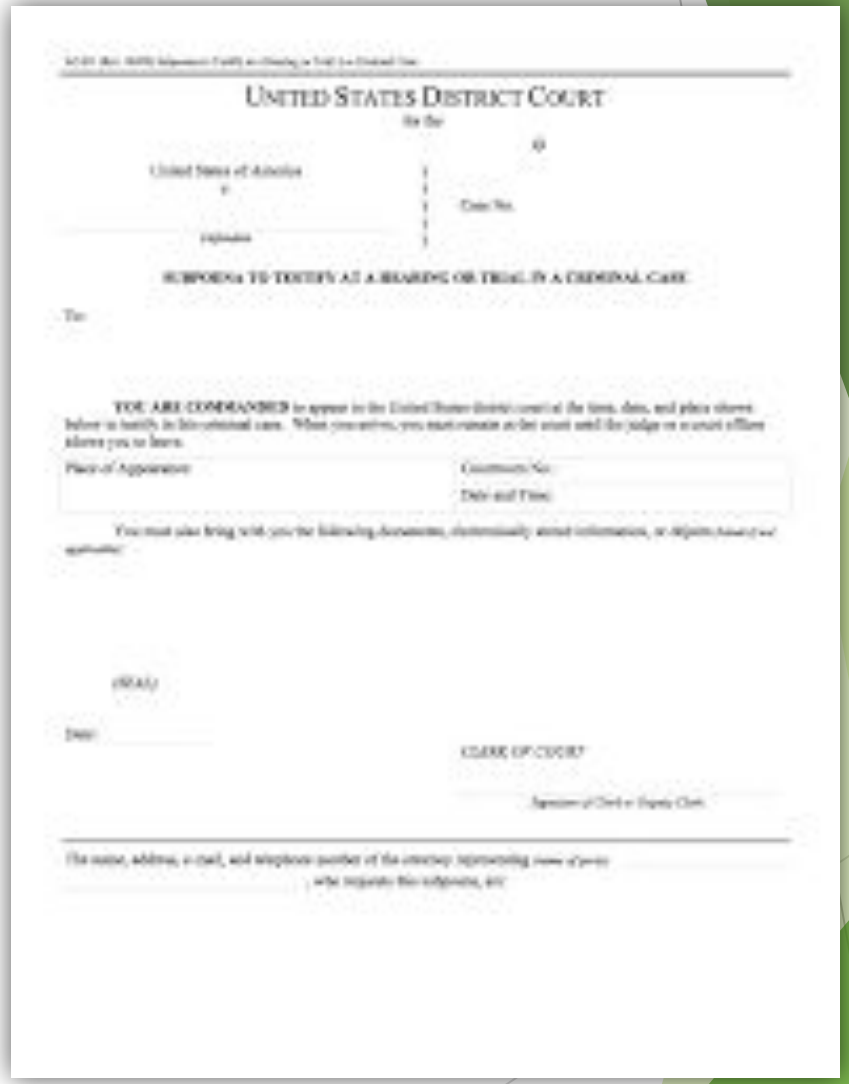
Why Do I Care (if you made it 7 slides before asking, congratulate yourself)

1. Attorneys are likely to handle PHI in practice areas like personal injury, insurance defense, malpractice, and elder law. However, attorneys in other areas may also deal with PHI and therefore need to follow HIPAA's security and data privacy standards.
2. You need to know Rules…to get the Records…
3. HIPAA applies to: all entities that provide, bill or pay for medical care or process medical information. These include the following:
   - Health care providers
   - Health Plans
   - Clearinghouses
   - Business associates

Requesting Records

Option 1

- A Court-Ordered Subpoena
  - An Order for Medical Records, signed by the Judge
  - The most straightforward way to obtain records, in the State of Tennessee, by a Tennessee Judge
  - The order should include:
    - Patient
    - Provider who can provide, or a broad enough description to include all providers
    - A time frame (can be all time)
    - Properly signed
    - All parties listed on the Order (the caption)



UNITED STATES DISTRICT COURT

Requesting Records, Cont.

Option 2

- Subpoenas Issued by an Attorney
  - Must serve the Subpoena on all counsel once served on Entity.
  - Must be signed by attorney and Court issuing.
  - Must give Plaintiff (or whoever's records you are requesting) opportunity to object…
    - Technically, Entity needs "satisfactory assurances" that:
      - A good faith attempt was made to provide written notice of the subpoena to the patient (or their legal counsel), acknowledge that Patient has the right to object, that time for objecting has passed, and that the Patient did not object;
      - All parties have agreed to a QPO to maintain confidentiality of the information requested, will only be used for the stated purposes, and will be destroyed after the lawsuit ends; OR
      - A valid HIPAA authorization is attached…(this one is stupid because if you had a HIPAA authorization, why subpoena????).
  - Most onerous approach for legal counsel. Drives up attorney fees. Unnecessary in most cases.

Requesting Records, cont.
Option 3

- Get a signed HIPAA authorization.
  - Easy for Plaintiff counsel
  - Easy for Victim counsel
- Harder for Defendant/Defense attorneys because need one for each medical provider. Have to go back to Plaintiff counsel with each new HCP identified.
- Best option for out-of-state medical records.
- Make sure you have the correct person signing, with proof that she is the correct person.
  - Personal Representative (probate records)
  - Spouse (death certificate)
  - Parent (birth certificate)
  - Patient (obviously)

Does HIPAA even apply to me?

- HIPAA's requirements apply directly to "covered entities," which are defined as:
  - Health plans;
  - Health care providers that carry out certain kinds of transactions electronically; and
  - Health care clearinghouses.
- HIPAA's requirements also apply to organizations that perform services for HIPAA covered entities – known as "business associates." Covered entities can disclose PHI to their business associates ***only if*** the covered entities obtain certain assurances (through a contractual agreement) that the business associate will appropriately protect the PHI.

Business Associates

- A “business associate” is a person or entity, other than a member of the workforce of a covered entity, who performs functions or activities on behalf of, or provides certain services to, a **covered entity** that involve access by the business associate to protected health information.
- For my med mal folks…
  - Who has access:
    - Copying services
    - Experts
    - Consultants
    - Client
    - Private Investigators
    - IT/Cloud/Data storage
- The definition of business associate under HIPAA's regulations expressly includes attorneys who perform legal services for a HIPAA-covered entity (for example, a health plan), if the attorneys are not members of the covered entity's workforce.

Who Doesn’t Care About HIPAA…

- The following entities (or types of coverage) are not directly subject to HIPAA's requirements, though some of the entities may need to comply indirectly:
  - Life insurers;
  - Employers/health plan sponsors;
  - Workers' compensation and disability insurance;
  - Most schools and school districts;
  - Many state agencies like child protective service agencies (though some state child health plans are covered);
  - Most law enforcement agencies; and
  - Plaintiff law firms???

Plaintiff Law Firms…My thoughts…

HIPAA COMPLIANT AUTHORIZATION FOR THE RELEASE OF PATIENT INFORMATION PURSUANT TO 45 C.F.R. § 164.508

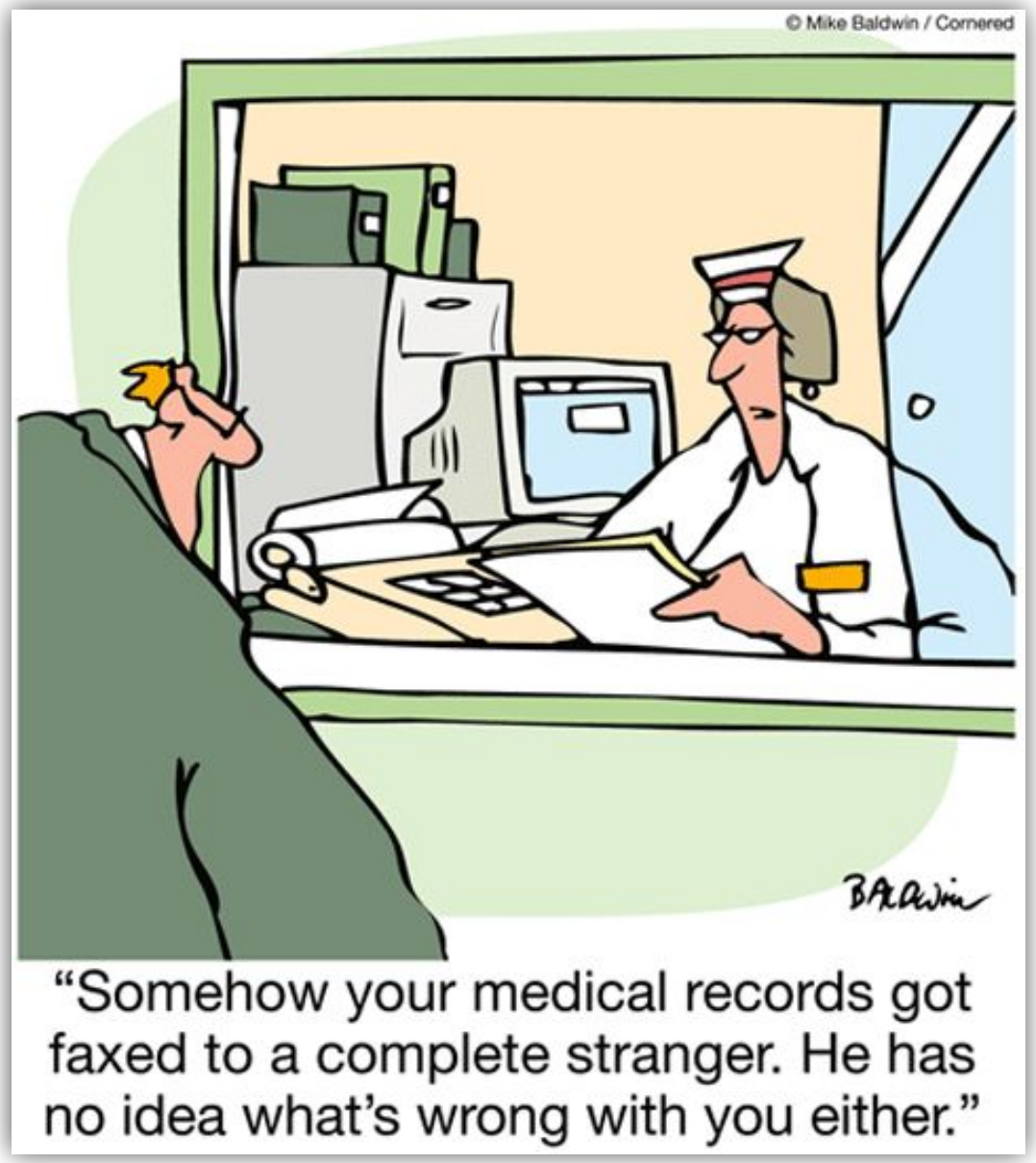
RE: Patient Name:
Address:
Date of Birth:
Social Security Number:

I authorize and request, _____ ("medical provider") to disclose all protected health information, as provided below. I expressly request that the designated record custodian of medical provider disclose full and complete protected medical information, including:

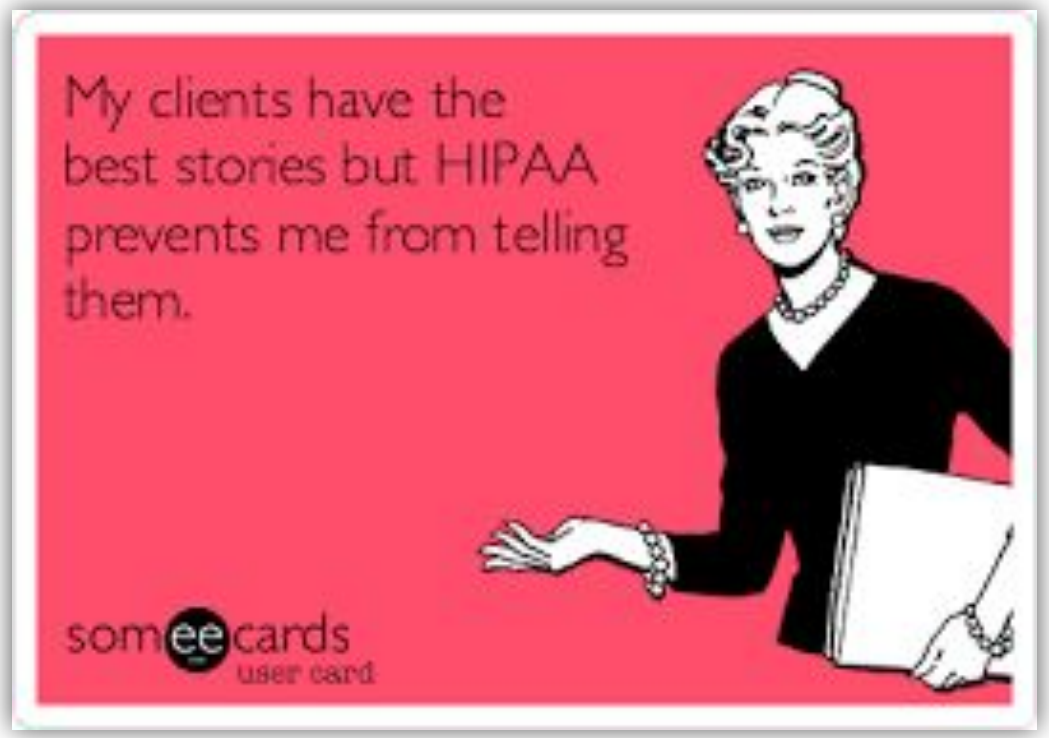
…

The information released in response to this authorization may be re-disclosed to other parties and may no longer be protected by federal law.

Yes…


© Mike Baldwin / Cornered
"Somehow your medical records got faxed to a complete stranger. He has no idea what's wrong with you either."

Maybe No…


My clients have the best stories but HIPAA prevents me from telling them.
someecards
user card

Nope…

Seriously, Stop it…

The Privacy Rule

- The Privacy Rule also recognizes the importance that entities and persons play in essential public health activities.
- The Privacy Rule permits covered entities to disclose protected material, without authorization, to such persons or entities for the public health activities below:
  - Child abuse or neglect
  - Quality, safety, or effectiveness of a product or activity regulated by the FDA
  - Persons at risk of contracting or spreading disease
  - Workplace medical surveillance

Okay, *this* is why you really care…

- **HIPAA non-compliance may result in severe penalties and correction requirements**
- The following non-exhaustive list reflects some of the more common HIPAA compliance failures that have resulted in HHS enforcement actions:
  - Failing to obtain a business associate agreement before disclosing PHI.
  - Failing to erase hard drives containing PHI, especially if the hard drives are later stolen or otherwise removed from the covered entity's or business associate's premises.
  - Failing to terminate access to PHI by unauthorized individuals (especially former employees and third parties).
  - Keeping records in unsecured locations (for example, employees' vehicles) and/or on unsecured laptops and other mobile devices.
  - Keeping or transmitting PHI in unencrypted form.
  - Improper disposal of PHI (for example, abandoning PHI in publicly accessible trash receptacles).
  - Improper disclosures of PHI (for example, resulting from malicious malware and disclosures to the public without obtaining a patient's authorization).
  - Failing to obtain satisfactory assurances from third-party vendors/business associates.
  - Not restricting disclosures of PHI to the “minimum necessary”.

Penalties and Punishment…

- HIPAA violations typically result in fines. The amount of the penalty depends on the seriousness of the violation, as follows:
  - Tier one —$120 to $30,113 per violation. Tier one fines could be applied where the non-compliant law firm was unaware (and could not reasonably have been aware) of the violation.
  - Tier two —$1,205 to $60,226 per violation. Tier two fines could be applied where the non-compliant party was unaware of (but there was reasonable cause for) the violation.
  - Tier three —$12,045 to $60,226 per violation. Tier three fines could be applied where the violation was caused by willful neglect but was corrected promptly.
  - Tier four —$60,226 per violation. Tier four fines could be applied where the violation was caused by willful neglect and was not corrected promptly.
- Moreover, if a law firm violates HIPAA multiple times in one calendar year…yikes!
- HIPAA non-compliance can have other effects on a law firm. For example, a HIPAA violation can destroy client relationships. It can also result in consequences for legal malpractice insurance and compliance with a firm's professional conduct obligations.
- Hassle, Headaches, and Harassment

Common Violations

- Understanding where things often go wrong will help your law firm comply with HIPAA. Some of the most common areas where an attorney or law firm might violate their HIPAA obligations are:
  - Failing to enter into a HIPAA-compliant business associate agreement.
  - Failing to obtain satisfactory assurances from third-party vendors and business associates.
  - Inappropriately disclosing or disposing of PHI.
  - Insufficient firm-wide risk management processes or analyses (including employee training).
  - Failing to report a HIPAA breach to HHS and other authorized entities or exceeding the 60-day deadline for issuing breach notifications.

Your (Employer's) Responsibility

- The best way to avoid HIPAA violations is to understand your HIPAA obligations. Understanding business associates' physical, technical, and administrative safeguards is a good starting point.
  - Administrative: Implementing policies and procedures to prevent and detect HIPAA violations. Training on HIPAA compliance for all staff members is essential.
  - Technical: Controlling access to systems that contain PHI. Passwords, encryption, and other technical safeguards are key components of this requirement.
  - Physical: Ensuring the security of offices, networks, data, and technology. Limit access as much as possible within your firm. For example, leaving a laptop that contains PHI in a public area (such as a cafe) represents a HIPAA violation.

Employer Checklist

- To avoid HIPAA violations, start by implementing the following HIPAA checklist for law firms:
  - Enter business associate agreements with clients and subcontractors (where appropriate).
  - Ensure you are complying with the administrative, physical, and technical requirements for data protection under HIPAA.
    - Administrative: Ensure staff know how to deal with PHI and have policies and procedures in place addressing HIPAA compliance;
    - Physical: Security measures limiting physical access to systems or areas containing PHI.
    - Technical: Encryption, unique usernames and passwords, and other technologies that protect data.
  - If a breach occurs, notify the Office for Civil Rights (OCR) promptly and cooperate with any questions or investigations.
  - Consider law firm practice management software that helps manage HIPAA compliance for law firms.

Useful Links…

- https://www.healthit.gov/topic/privacy-security-and-hipaa/health-it-privacy-and-security-resources-providers - Education
- https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html - BA agreement
- https://www.hipaajournal.com/hipaa-compliance-checklist/ - HIPAA Checklist
- https://www.law.cornell.edu/cfr/text/45/160.103 - HIPAA Definitions
- https://www.law.cornell.edu/cfr/text/45/160.103 - The Language of the Act
- https://www.nexsenpruet.com/assets/htmldocuments/uploads/1417/doc/Born,_J_-_SCALA_HIPAA_for_Law_Firms_April_14_2016.pdf - 80-slide PowerPoint… probably has the answer.
- https://lawpracticecle.com/wp-content/uploads/woocommerce_uploads/2019/11/LawPracticeCLE_HIPAA-Law-for-Lawyers-A-Must-Know-Guide-to-New-Compliance-Requirements_Course-Manual.pdf - Just kidding… a 351-slide PowerPoint… definitely has the answer!

Credit

- The content of these slides was “borrowed” heavily from:
  - Clio
  - The University of Alabama School of Nursing
  - HHS
  - Thomson Reuters