HIPAA, Not HIPPO. Two As, One P

- Health Insurance Portability and Accountability Act
- Primary federal law protecting health information
- Governs the permissible uses and disclosures of health information that identifies the subject of the information
- Covers only information created, received or maintained by or on behalf of health care providers and health plans
- Often thought of as a restrictive law; actually quite permissive
- Note that HIPAA serves as a floor rather than a ceiling; if a state law is more restrictive or stringent than HIPAA, it governs

Once Upon a Time…
HIPAA Statute (Public Law 104-191)

- Passed by Congress in 1996
- Designed to improve the efficiency and effectiveness of the health care system
- Aimed to modernize the flow of information as more of it became digital
- Among other things, required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge

The Juicy Stuff: HIPAA Regulations

1. Privacy Rule

   - Applies to providers (doctors), health plans (insurers) and health care clearinghouses (known as "*covered entities*") and their contractors ("*business associates*")
   - Sets limits and conditions on the uses and disclosures of protected health information (PHI) without patient authorization
   - Gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections

2. Security Rule

   - Establishes a national set of security standards for protecting health information
   - Provides technical and non-technical safeguards that covered entities must put in place to secure individuals' electronic PHI

HIPAA Regulations (cont.)

3. Enforcement Rule

   - Newer – part of HITECH in 2009
   - Strengthens civil and criminal enforcement of the HIPAA rules
   - Significantly increased civil monetary penalties for violations
   - Office for Civil Rights at HHS has responsibility for HIPAA violations

4. Breach Notification Rule

   - Requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured PHI
   - Breach is defined as the acquisition, access, use, or disclosure of PHI in a manner not permitted by the Privacy Rule which compromises the security or privacy of the PHI

Privacy Rule – Who and What Does it Cover?

1. **Covered Entity** – health care providers (doctors), health care plans (insurers), and health care clearinghouses
2. **Protected Health Information (PHI)** – *"Individually identifiable health information"* held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral

   → *"Individually identifiable" is broadly defined*
3. **Business Associate** – a contractor of a covered entity that performs services and handles PHI on its behalf

   → *If you don't handle or couldn't potentially be exposed to PHI, don't need a business associate agreement*

Privacy Rule – Who/What Does it NOT Cover?

- Data created or held by a person or company that is not a covered entity

- Data that is not individually identifiable

  → Data that has been de-identified is no longer covered by HIPAA

  → Two ways under HIPAA that data can be de-identified: (1) expert determination and(2) compliance with safe harbor (removal of 18 types of identifiers)

Privacy Rule – Who/What Does it NOT Cover?

- Data you generate is not covered by HIPAA (unless it is later transmitted to a covered entity)
  →This includes most data on your computer or phone, like the info you upload into a calorie-counting app, a fitness tracker, or your order history on Amazon
  →YOU are not a HIPAA-covered entity
- Most apps and tech companies are not HIPAA covered entities in their own right
- Most employers are not HIPAA-covered entities, even if they provide health care coverage to their employees

→ *Once data leaves a HIPAA-covered entity, either for a required or permitted purpose, or because an individual authorized the disclosure, and goes to a non-HIPAA covered entity or person, the law and its protections no longer apply*

Business Associates

- What are the types of things Business Associates do?
  - claims processing
  - data analysis
  - utilization review
  - billing
- Business Associate Agreement
  - When a covered entity hires a Business Associate to perform services on its behalf that involve handling of PHI, or even potential exposure to PHI, the Privacy Rule requires that the covered entity include certain protections for the information in a *business associate agreement (BAA)*
  - BAAs have to specify precisely how the BA will and will not use CE data
  - Business Associates are subject to the Privacy Rule, and follow the same rules as covered entities with respect to PHI

Uses and Disclosures Under the Privacy Rule

- In general, the Privacy Rule prohibits Covered Entities (and their Business Associates) from using or disclosing PHI, UNLESS:
  1. (1) the Privacy Rule permits or requires such a use or disclosure; or
  2. (2) the individual who is the subject of the information (or the individual's personal representative) authorizes the use/disclosure in writing

  → *Patients can verbally request copies of their own health information and direct disclosures to family members/caregivers*

Permitted Disclosures of Health Data under HIPAA – "TPO" (without patient authorization)

- Treatment
  - Provision, coordination, or management of health care
  - Consultation between health care providers
  - Referral of a patient from one health care provider to another
- Payment
  - Various activities related to obtaining payment or reimbursement, obtaining premiums, providing benefits or determining coverage/eligibility
- Health care operations (broadest category)
  - Certain administrative, financial, legal, and quality improvement activities of a covered entity that are necessary to run its business and to support the core functions of treatment and payment
  - Includes staff evaluations, case management and care coordination

Uses and Disclosures Under the Privacy Rule

- In general, the Privacy Rule prohibits Covered Entities (and their Business Associates) from using or disclosing PHI, UNLESS:
  1. (1) the Privacy Rule permits or requires such a use or disclosure; or
  2. (2) the individual who is the subject of the information (or the individual's personal representative) authorizes the use/disclosure in writing

  → *Patients can verbally request copies of their own health information and direct disclosures to family members/caregivers*

Other Permitted Disclosures of Health Data under HIPAA (without patient authorization)

- Required by law
- Public health activities
- Victims of abuse, neglect or domestic violence
- Health oversight activities
- Law enforcement purposes
- Decedents
- Cadaveric organ, eye, or tissue donation
- Research
- Serious threat to health or safety
- Essential government functions
- Workers' compensation

What's New?

- Changes to the Part II regulations finalized in July 2020
  - Confidentiality of Substance Use Disorder Patient Records, 42 CFR Part 2
  - Changes designed to support care coordination and beef up privacy of sensitive records.
  - Congress included legislation to align Part 2 with HIPAA for the purpose of treatment, payment and operations in the Coronavirus Aid, Relief, and Economic Security Act (CARES Act) in March of 2020; we expect rulemaking enacting these changes soon
- CMS/ONC interoperability and information blocking rules
  - Implement provisions of the 21st Cures Act of 1996
  - Both final rules were issued on March 9, 2020 and became effective on April 5, 2021, after a pandemic-related delay
- HIPAA Notice of Proposed Rulemaking
  - Released in December of 2020; comment period closed in May of 2021
  - First major proposed updates to HIPAA since the HITECH Act in 2009

ONC Final Rule

1. The ONC rule requirements focus on two main areas: HIT certification and information blocking
2. ONC's only major statutory requirements was to establish exceptions, which they did, that represent 'reasonable and necessary' activities that do not constitute information blocking and to establish a public reporting system
3. ONC went a step further than the statute to require actors – including HIEs – to make electronic health information available to patients and any entity of their choosing, including third-party applications

→ *This will increase the amount of health information flowing out of the health care system and thus LOSING HIPAA protections*

CMS Final Rule

1. CMS is requiring Medicare Advantage organizations, Medicaid and CHIP FFS programs, Medicaid managed care plans, CHIP managed care entities, and Qualified Health Plan (QHP) issuers on Federally Facilitated Exchanges (FFEs) to implement and maintain a standards-based Patient Access API. Payers must allow third-party applications to retrieve, with the approval and at the direction of the current enrollee, certain data

2. While Trump HHS used Cures as impetus for new regulations, CMS only major statutory requirement was to establish 'appropriate disincentives' for providers who were found to be engaging in information blocking

HIPAA NPRM Overview

- Focused on clarifying and amending existing HIPAA provisions to facilitate the delivery of coordinated, value-based care
  - Proposed revisions expand and make clearer the circumstances under which and the people to whom information can be disclosed, specifically for care coordination purposes
  - Strengthen patient access to health information and shorten timeframes
  - Aim to decrease administrative burdens (e.g., Notice of Privacy Practices)

HIPAA NPRM Overview (cont.)

- Part of previous administration's push to increase information flow, and to get health data into the hands of patients and care-givers
- Comes two years HHS' OCR issued an RFI on how the agency could update the HIPAA Privacy Rule to make it easier to share PHI among health care providers, payers, patients and caregivers
- Also driven by the pandemic, during which issues of privacy and public health took on new significance
- Comes on heels of the Interoperability and Information Blocking rules, which also are focused on expanding individual access to health data
- New administration hasn't officially pulled back on it, but not even on regulatory agenda for 2022; unclear what if anything will happen with it

HIPAA and Covid

- When Covid was declared a public health emergency, HHS relaxed its enforcement discretion when it comes to telehealth
  - During the PHE, covered health care providers subject to HIPAA can communicate with patients and provide telehealth services through remote communications technologies that may not fully comply with HIPAA requirements, and in a manner that may not be fully HIPAA-compliant.
  - OCR currently will not impose penalties for noncompliance with HIPAA Rules against covered health care providers in connection with the good faith provision of telehealth during the COVID-19 nationwide public health emergency
- eHI held a webinar re: vaccine "passports" and associated privacy issues last year; application of HIPAA to vaccine information and status is dependent on whether or not holder of that information is a covered entity

What's Next?

- Increasingly, health data lies outside of the traditional healthcare system
  - Web-browsers, wearables, health and wellness apps
  - Data sent from HIPAA covered entities to individuals via third-party apps (new info blocking/interop rules just discussed)
- It seems likely that, rather than overhaul HIPAA, new federal comprehensive privacy legislation is on the way (*when* is anyone's guess!)
  - May be modeled in some ways after Europe's GDPR
  - Some states are getting ahead of the feds (California's CCPA; Virginia's VCDPA)
  - These laws differ from HIPAA with respect to purpose (protection of personal data (broadly defined) v. health data) and scope of coverage (any entity that handles personal information as defined by the laws is covered)