CHLPI

CENTER *for* HEALTH LAW *and* POLICY INNOVATION

HARVARD LAW SCHOOL

HIPAA:
A JOURNEY, NOT A DESTINATION

Center for Health Law and Policy Innovation
Harvard Law School

February 22, 2022

Agenda

- Why should I care about patient privacy laws?
- HIPAA basics
- What does HIPAA require?
- Where do we go from here?

Why Engage With HIPAA?

- You want to partner with a health care entity to provide their patients or members with certain services.
- Complying with patient privacy obligations and expectations will likely require some additional resources.
  - Financial, staff expertise, time

Privacy Obligations vs. Expectations

HIPAA	Partners	Client/ Mission
What the law requires	What health care partner requests	What serves the client
	What health care partner requires	What the client expects
	What CBO partner can do	What serves the mission

Implications on a Partnership May Change Over Time…

Depends on partnership activities

Depends on PHI shared

Depends on law that is evolving

WHAT IS HIPAA?

- Federal body of law mandating the protection and confidential handling of **Protected Health Information** by **Covered Entities** and their **Business Associates**

There are also other privacy laws:

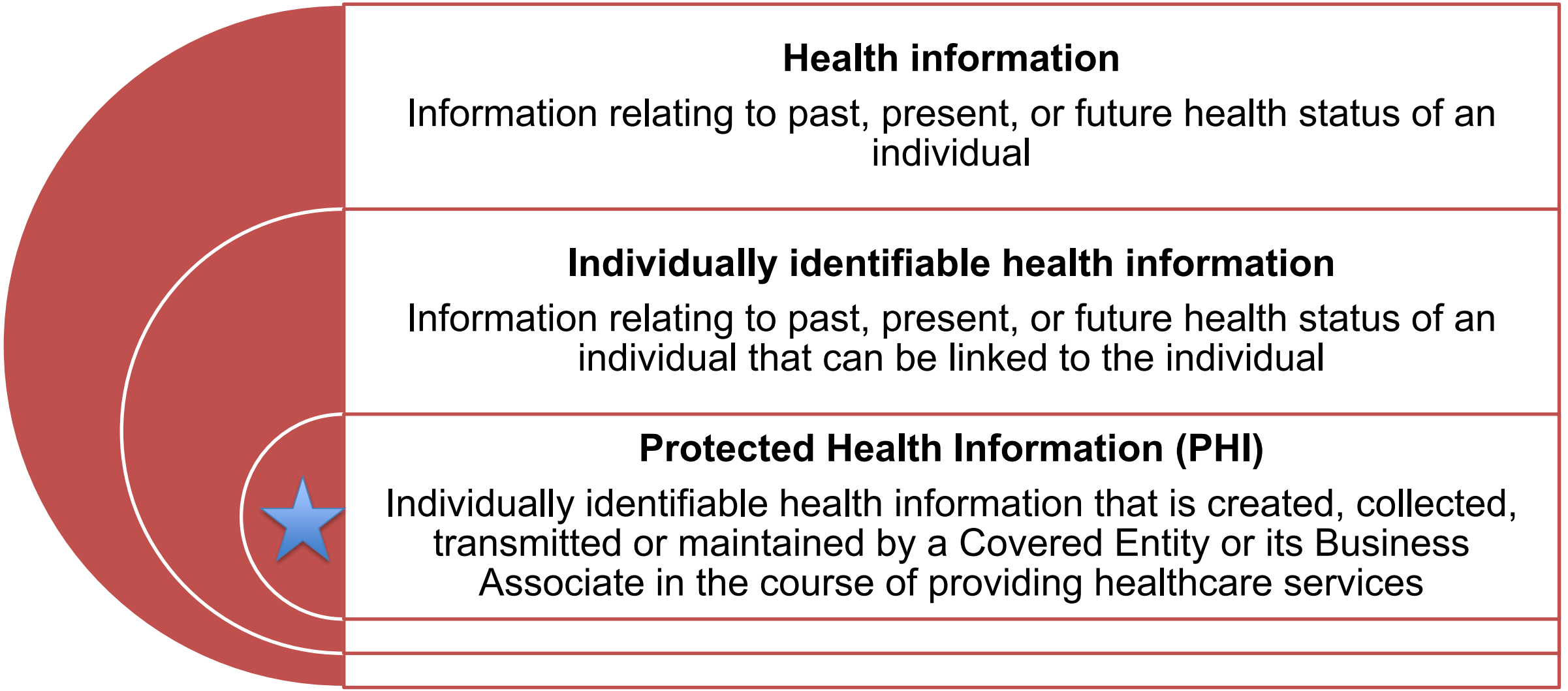
- **State law**
- **42 CFR Part 2 (substance use disorder patient records)**
- **Sarbanes Oxley (public companies)**

Who Needs to Comply With HIPAA?

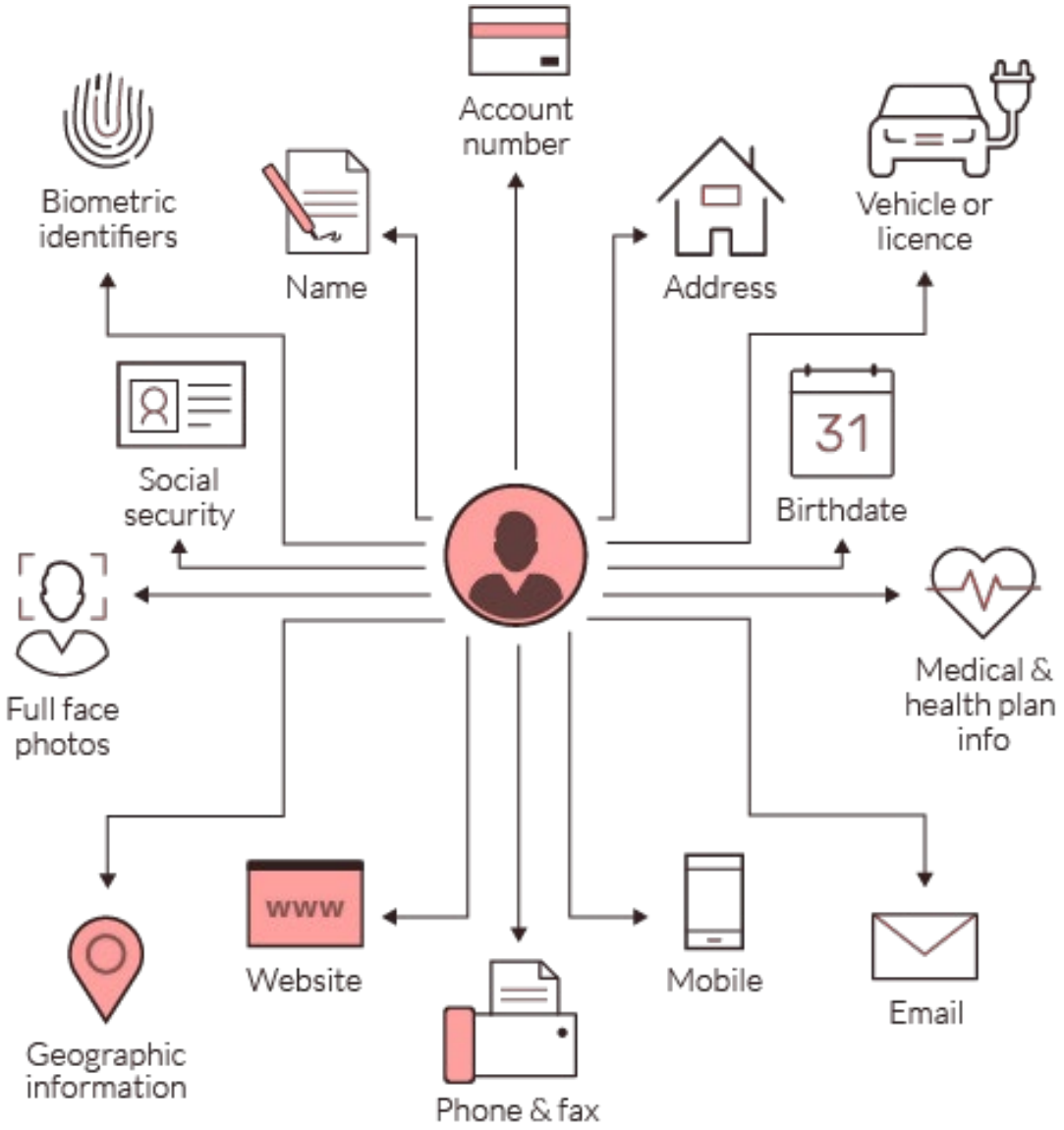
- "Covered Entities"
  - Health care providers who conduct certain standard electronic transactions
    - Including transactions relating to claims, eligibility
  - Health plans
  - Health care clearinghouses

- "Business Associates" of Covered Entities
  - Organizations that work with PHI "for or on behalf of" a Covered Entity

What Information is Protected Under HIPAA?



What Makes Information "Identifiable"?



What Does HIPAA Require?

- HIPAA's patient privacy requirements can be lumped into three big buckets:
  - Privacy Rule
  - Security Rule
  - Breach Notification Rule

What Does HIPAA Require?

- HIPAA's requirements can be lumped into three big buckets:
  - **Privacy Rule**
    - Defines and limits permitted uses and disclosures—the circumstances in which a Covered Entity (and Business Associates) may use or disclose an individual's PHI
    - Requirements to ensure patient rights to their information
    - Minimum necessary principle

Permitted Disclosures

- Patient driven information sharing
  - The general rule is that an individual's consent is required for a covered entity to disclose PHI.

- Exceptions:
  - Disclosures for treatment purposes
  - Disclosures to business associates
  - Disclosures under certain research / evaluation arrangements

Patient Authorization

- HIPAA requires that a valid written authorization include several components

PATIENT AUTHORIZATION TO DISCLOSE HEALTH INFORMATION

A copy of this completed form must be provided to the patient

Pursuant to the Health Insurance Portability and Accountability Act, 45 C.F.R. Parts 160, 164

1. Authorization

I hereby authorize _____ (HIPAA Covered Entity, hereafter known as COVERED ENTITY) to disclose protected health information as described in this authorization.

2. Extent of Authorization

I authorize the release of the following types of information in my health record (check all the apply): _____

Note: List the types of PHI collected by the health care provider that will be shared under this Authorization. Examples of information that grantees may want to include are:
-Names
-Street address, city, county, and zip code
-Birth date
-Height
-Weight
-BMI
-Medications
-Blood pressure
-Blood glucose
-A1c

Patient Authorization

- Patient driven information sharing
  - The general rule is that an individual's consent is required for a covered entity to disclose PHI.

- Exceptions:
  - Disclosures for treatment purposes
  - Disclosures to business associates
  - Disclosures under certain research / evaluation arrangements

Treatment Exception

- Under the "Treatment Exception," a health care provider may share information with a community-based organization or social services organization where the disclosure is "a necessary component of, or may help further, the individual's health or mental health care."
- BUT: We only have one example of how this applies.
  - Treatment Exception permits a health care provider to share the fact that a specific individual needs mental health care supportive housing with an agency that arranges these services.
    - Source: U.S. Dep't. of Health & Human Servs., *FAQ 3008: Does HIPAA permit health care providers to share protected health information (PHI) about an individual with mental illness with a third party that is not a health care provider for continuity of care purposes?*, HHS.GOV, https://www.hhs.gov/hipaa/for-professionals/faq/3008/does-hipaa-permit-health-care-providers-share-phi-individual-mental-illness-third-party-not-health-care-provider-continuity-care-purposes/index.html (last visited April 22, 2021).

Research and Data Sharing

- CBOs can independently collect data; if the CBO is not a covered entity or business associate, the data is not subject to HIPAA.
  - HOWEVER! Review state privacy laws and IRB requirements.
- Patients/clients can authorize release of PHI for research purposes.
- Health care provider can **de-identify data** prior to using it for research; no PHI = no issue.

Table 1. Example of Protected Health Information		
Patient Name	Date of Birth	Diagnosis
Jane Doe	September 29, 1987	Diabetes
John Doe	May 4, 1979	Diabetes
June Doe	November 18, 1983	Hypertension

Table 2. Example with Generalized Values		
Participant Number	Age Range	Diagnosis
1	< 35 years	Diabetes
2	35-45 years	Diabetes
3	35-45 years	Hypertension

- Health care partner can share a "limited data set" with no HIPAA "direct identifiers" if the parties have shared a **Data Use Agreement** (DUA).
- IRB has waived the requirements for HIPAA authorization.

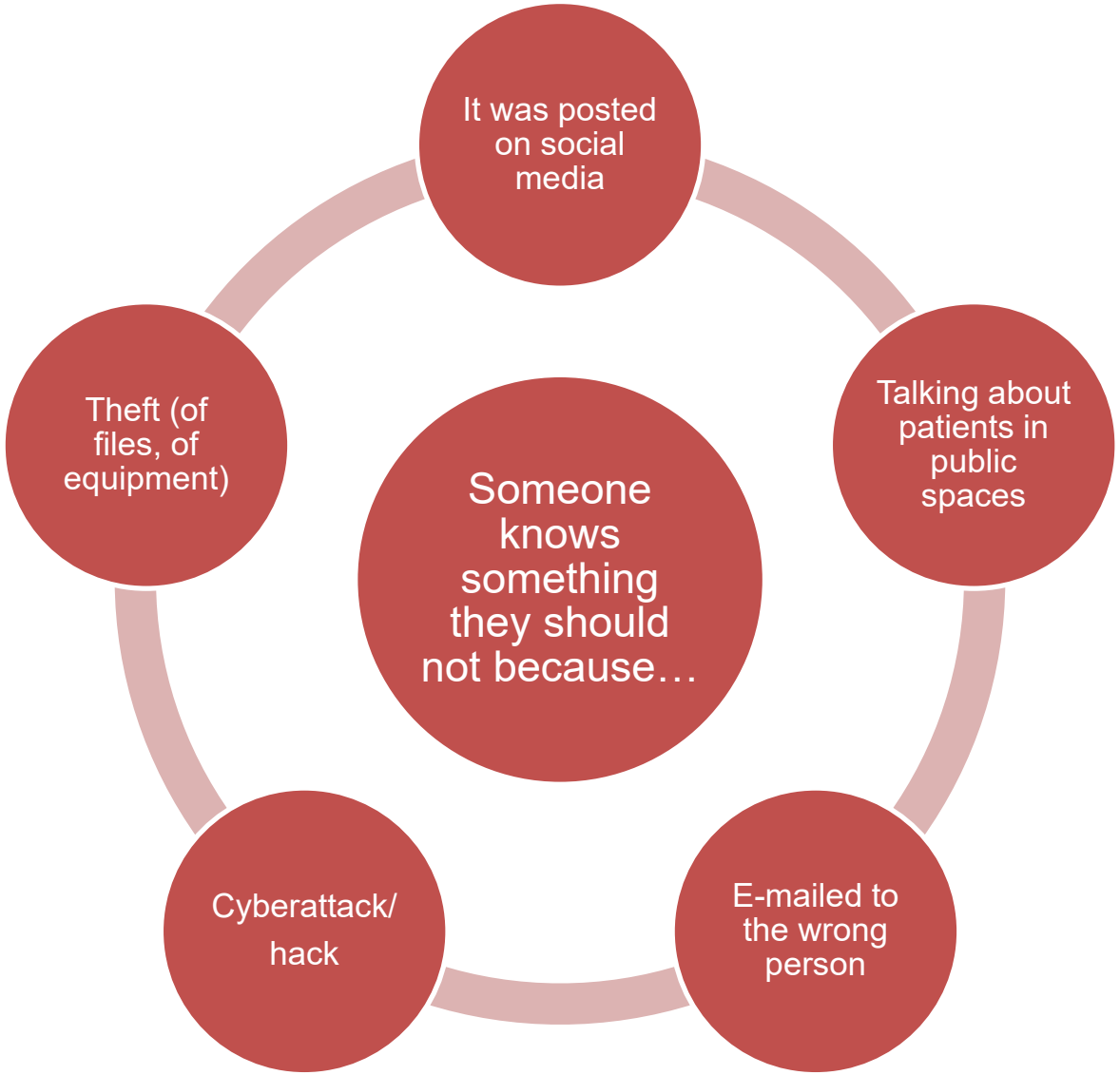
Business Associate

- Business Associates of a Covered Entity are responsible for complying with HIPAA requirements via the terms of a Business Associate Agreement (BAA) signed by the parties.
- Can you use a patient-driven model for your partnership?
- Read every part of the Business Associate Agreement carefully and ask for clarification.
- Conduct a realistic assessment of whether your organization is able to meet the responsibilities and obligations described in the contract.
- Can your health care partner support you in being ready to contract?

What Does HIPAA Require?

- HIPAA's requirements can be lumped into three big buckets:
  - Privacy Rule
  - **Security Rule**
    - Administrative, physical, and technical safeguards to ensure the security, confidentiality, and integrity of PHI

Common Issues



What Does HIPAA Require?

- HIPAA's requirements can be lumped into three big buckets:
  - Privacy Rule
  - **Security Rule**
    - Administrative, physical, and technical safeguards to ensure the security, confidentiality, and integrity of PHI

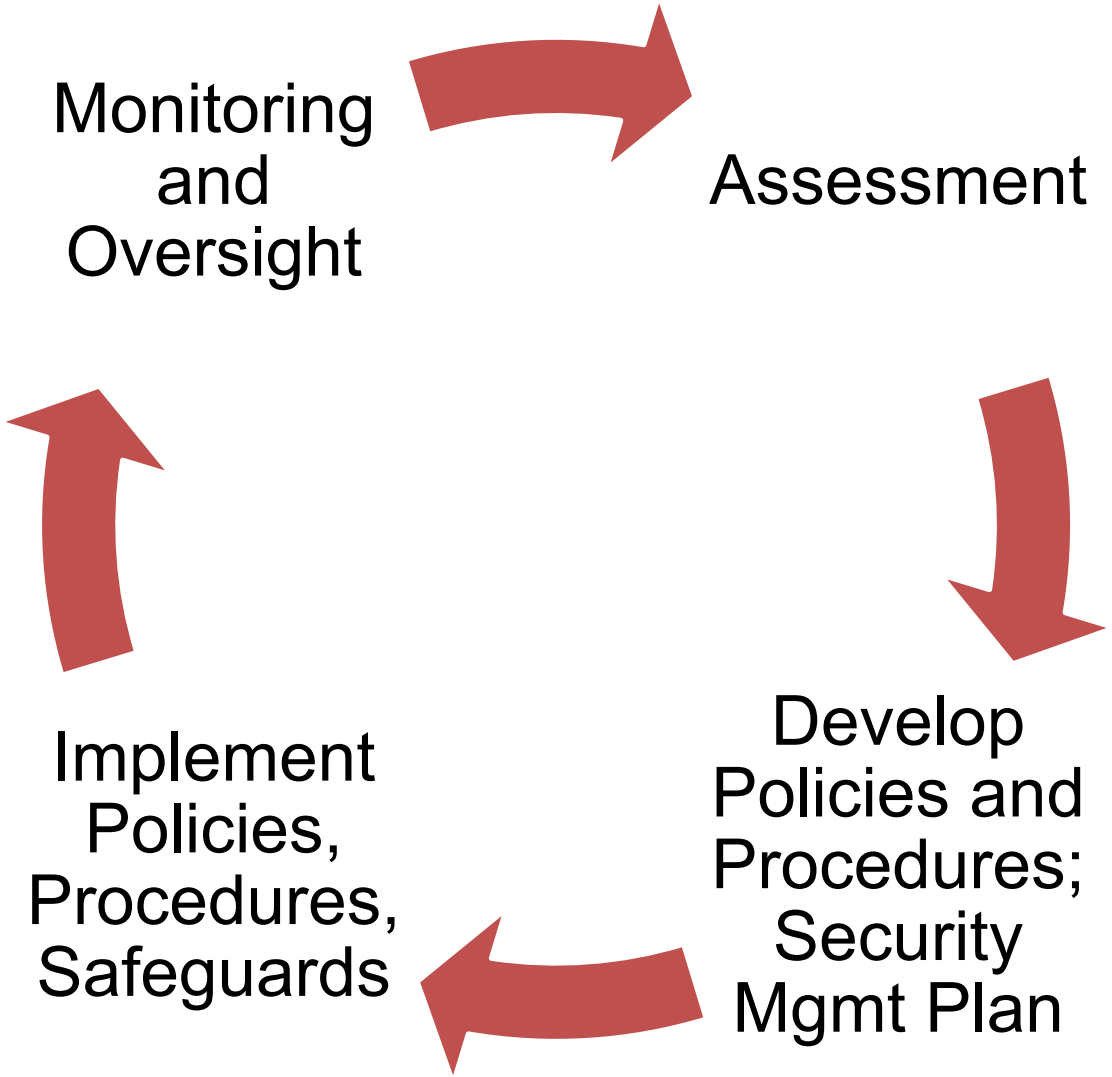
Examples:

- Password protections on electronic devices (administrative)
- Restricting and monitoring access to systems containing PHI (administrative)
- Storing files and electronic devices in locked cabinets (physical)
- Sending encrypted messages (technical)

What Does HIPAA Require?

- HIPAA's requirements can be lumped into three big buckets:
  - Privacy Rule
  - Security Rule
  - **Breach Notification Rule**
    - Requirements to inform affected parties of a "breach" - unauthorized access to unsecured PHI

What Does Compliance Look Like?



Where Do We Go From Here?

- Identify organizational leads to review the interaction between information needs, information sharing across partners, and patient privacy law
- Implement an appropriate privacy/security program