Healthcare Trust Institute

HIPAA & Health IT Privacy

A Beginner's Guide to HIPAA, Information Blocking & State Privacy Laws

HIPAA's Two Core Rules

HIPAA is comprised of two fundamental rules that protect health information

Privacy Rule

Controls how Protected Health Information (PHI) is **used and disclosed**

Gives patients rights to access, amend, and receive accounting of disclosures

45 CFR Parts 160, 164

Security Rule

Protects **electronic PHI (ePHI)** through administrative, physical, and technical safeguards

Requires risk assessments, access controls, encryption, and audit logs

45 CFR Part 164

What Is Protected Health Information?

The core data HIPAA is designed to protect

Protected Health Information (PHI)

Any individually identifiable health information that is created, received, maintained, or transmitted by a Covered Entity or Business Associate, in any form or medium.

What Counts as PHI?

1. **Patient Names**
2. **Dates of Birth**
3. **Social Security Numbers**
4. **Medical Records**
5. **Lab Results**
6. **Insurance IDs**

Key Point: PHI includes information in **any form** — electronic (ePHI), paper, or oral — that can identify an individual.

Healthcare Trust Institute

Who Must Comply?

Two categories of organizations are regulated under HIPAA

Covered Entities

Organizations **directly regulated** by HIPAA that handle PHI as part of their core operations

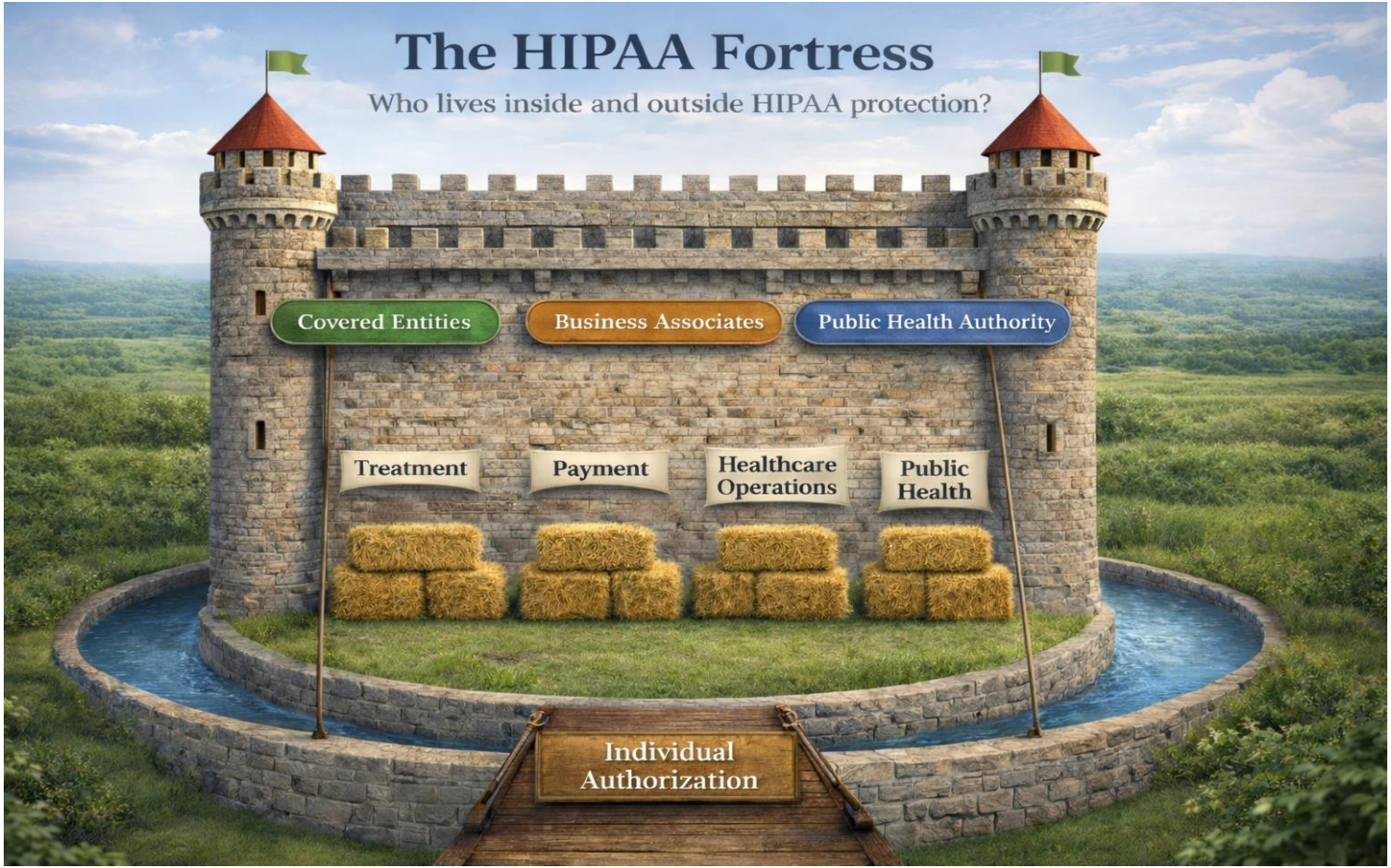
- Health Plans
- Healthcare Providers
- Healthcare Clearinghouses

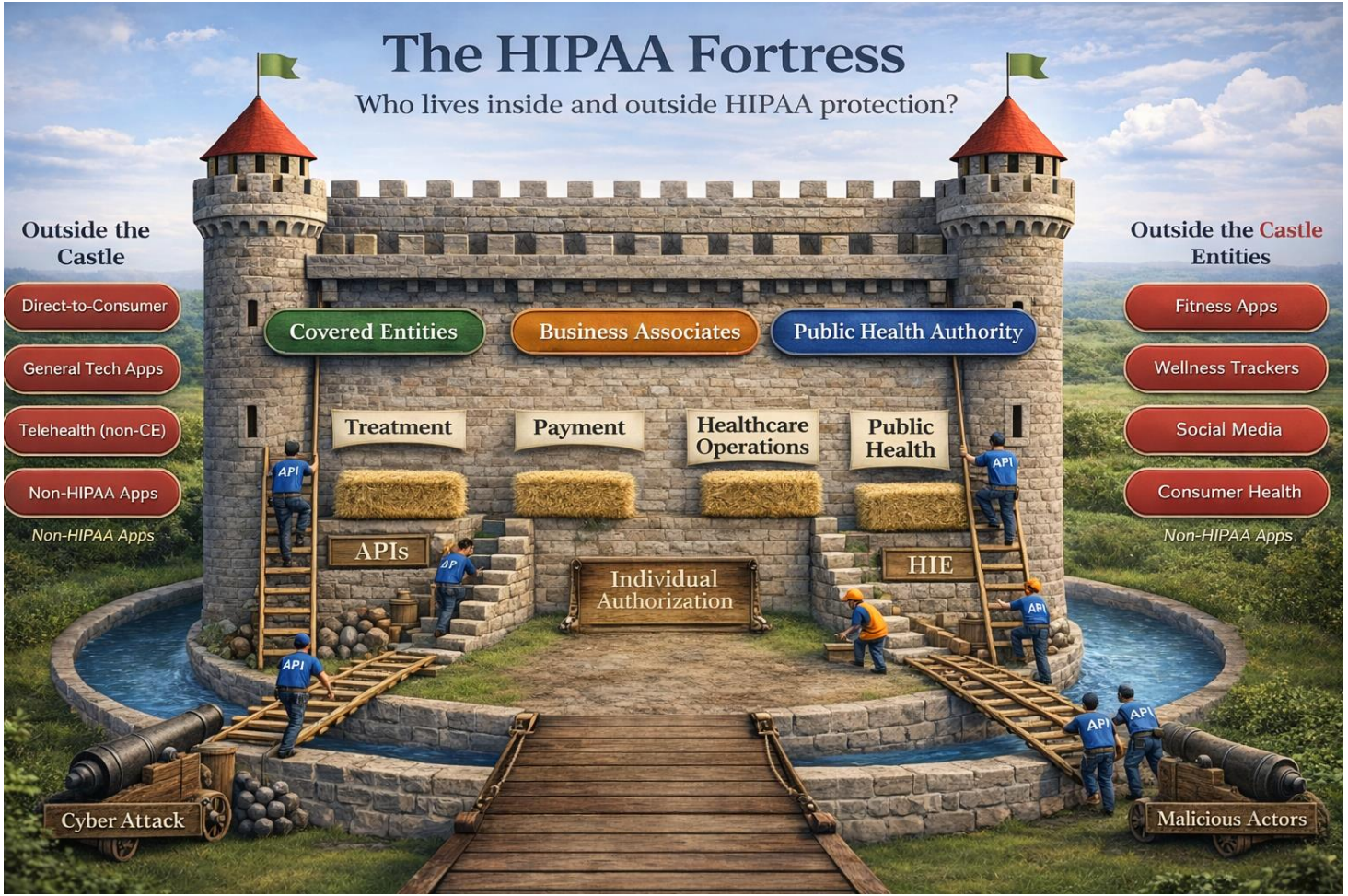
Business Associates

Third parties that **handle PHI on behalf** of a Covered Entity

- IT Service Providers
- Billing Companies
- Cloud Storage Vendors

Bound by Business Associate Agreements (BAAs)


The HIPAA Fortress
Who lives inside and outside HIPAA protection?
Covered Entities
Business Associates
Public Health Authority
Treatment
Payment
Healthcare Operations
Public Health
Individual Authorization


The HIPAA Fortress
Who lives inside and outside HIPAA protection?
Outside the Castle
Direct-to-Consumer
General Tech Apps
Telehealth (non-CE)
Non-HIPAA Apps
Non-HIPAA Apps
Outside the Castle Entities
Fitness Apps
Wellness Trackers
Social Media
Consumer Health
Non-HIPAA Apps
Covered Entities
Business Associates
Public Health Authority
Treatment
Payment
Healthcare Operations
Public Health
APIs
Individual Authorization
HIE
API
Cyber Attack
Malicious Actors

HIPAA vs. 21st Century Cures Act

HIPAA

PHI may be shared

Sharing is permitted, not required

vs

21st Century Cures Act

EHI must be shared

Unless an exception applies

The Three Types of "Actors" Under the Cures Act

Entities subject to information blocking regulations

Healthcare Providers

Hospitals, physicians, clinics, nursing facilities, and other providers who deliver care

Subject to disincentives determined by HHS

Health IT Developers

Developers of certified health IT (e.g., EHR vendors) who build systems that manage EHI

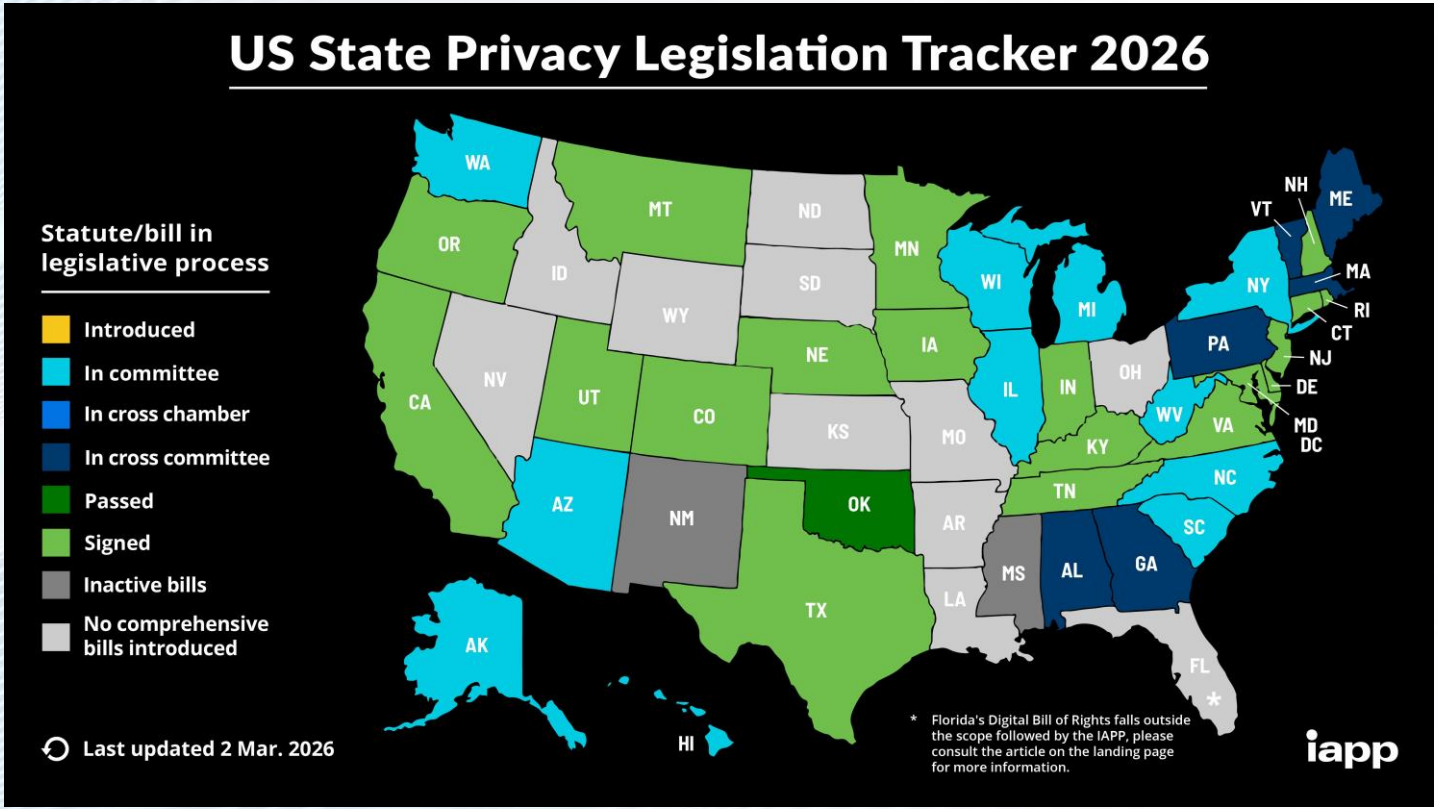
Up to $1M per violation in civil penalties

HIEs / HINs

Health Information Exchanges and Health Information Networks that facilitate data sharing

Up to $1M per violation in civil penalties

State Privacy Laws



Healthcare Trust Institute