HEALTH INNOVATION ALLIANCE

Federal Health Data and Privacy Regulation Overview

NCOIL

November 17, 2022

Agenda

1. Intro
2. Federal Interoperability Policy
3. Federal Laws Governing Health Data
4. HIPAA Overview
5. Regulation of Covered Entities
6. Enforcement of HIPAA
7. HIPAA v. Non-HIPAA
8. Rise of Consumer Privacy
9. State Activity
10. FTC Actions
11. American Data Privacy and Protection Act
12. Take Aways
13. Questions & Discussion

Federal Interoperability Policy

Current and previous administrations identified interoperability, information blocking, and consumer PHI access as priorities

Utilized regulatory authority to promulgate and finalize several rules

Rules have similar goals, but lack harmony in achieving those stated goals

Rules of Note:

1. **21st Century Cures Act: Interoperability, Information Blocking and the ONC Health IT Certification Program Final Rule**
2. **CMS Interoperability and Patient Access Final Rule**
3. **Modifications to the HIPAA Privacy Rule to Support, and Remove Barriers to, Coordinated Care and Individual Engagement**
4. **Transparency in Coverage Final Rule**

Federal Laws Governing Health Data

HEALTH INNOVATION ALLIANCE

1 Health Insurance Portability and Accountability Act (HIPAA)

- Limitations and Penalties for *covered entities*
- Treatment, Payment, and Health Care Operations (TPO)

2 Confidentiality of Substance Abuse Treatment Records (Part 2)

- Patient consent for every disclosure unless patient consents to HIPAA

3 Genetic Information Nondiscrimination Act (GINA)

- Prohibition on discrimination related to genetic information
- Enforced by EEOC

4 Federal Trade Commission (FTC) Act

- Unfair and deceptive trade practices
- Health Breach Notification Rule

5 Family Educational Rights and Privacy Act (FERPA)

- Access to educational records, including student medical treatment at on-campus facility

6 Others (Common Rule, FDA Regulations, etc.)

HIPAA Overview

Passed in 1996 and signed into law by President Clinton

- Statute required Secretary of HHS to regulate if Congress did not act.
- (Congress did not act.)

Major provisions related to health data (45 CFR Part 164; also some in Part 160):

Privacy Rule

- Use and disclosure of protected health information (PHI) for treatment, payment, and healthcare operations (TPO)

Security Rule

- Safeguards required for "electronic protected health information"

Breach Notification Rule

- Required notification in case of breach

Regulation of Covered Entities

“Covered Entity”

- A health plan.
- A health care clearinghouse.
- A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

“Business Associate”

- Entity handling PHI on behalf of covered entity
- Examples: claims processing, quality assurance, electronic health record vendor, etc.
- Must enter business associate agreement (BAA)

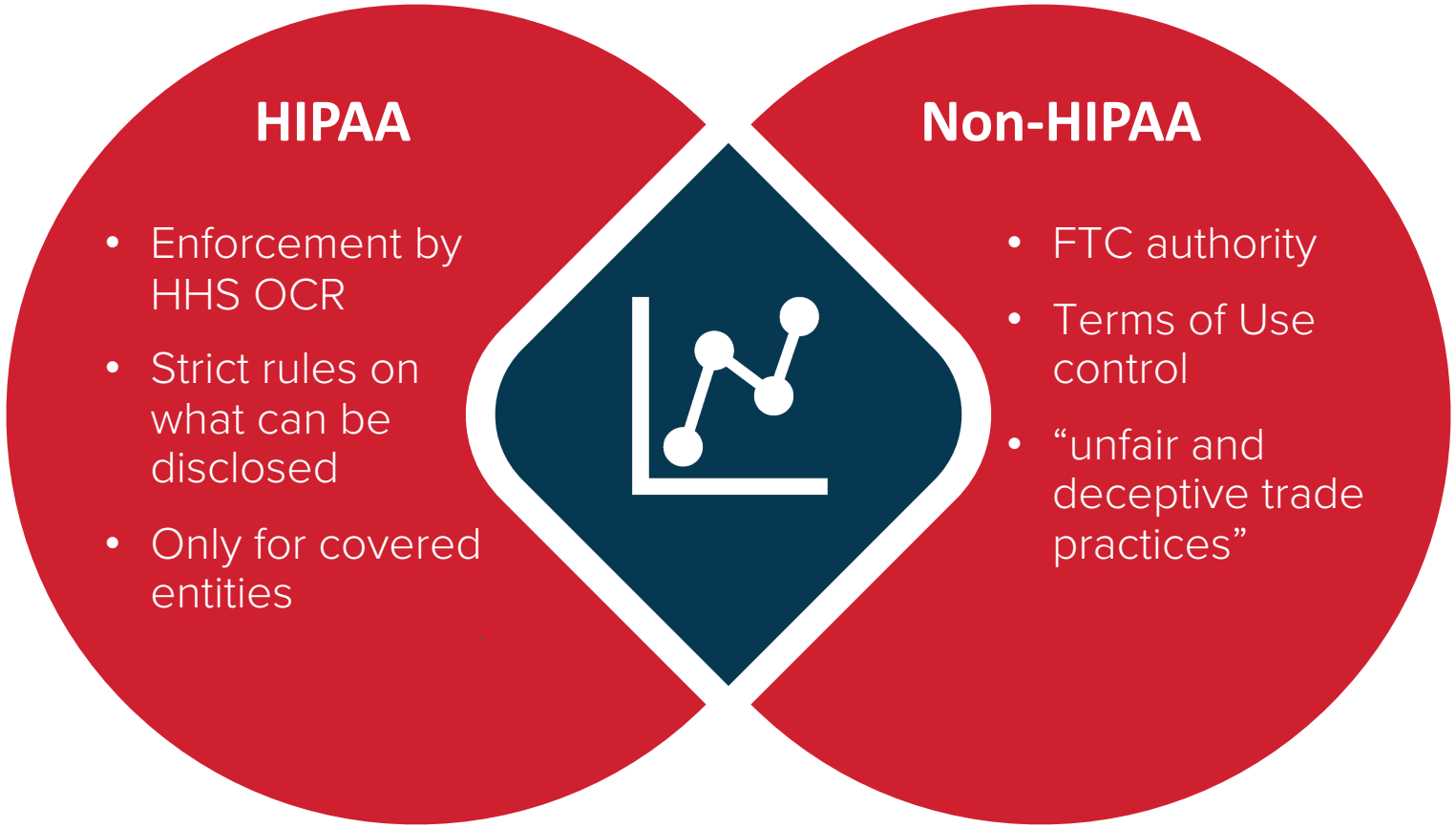
Non-covered Entity

- Everyone else

Enforcement of HIPAA

- HHS Office for Civil Rights (OCR) as of September 30, 2022:
  - “Since the compliance date of the Privacy Rule in April 2003, OCR has received over 309,475 HIPAA complaints and has initiated over 1,053 compliance reviews. We have resolved ninety-seven percent of these cases (300,427).”
- Largest fine was in 2018 to Anthem for $16M related to PHI being hacked in in December 2014 and January 2015.
- Right of Access Initiative – As of December 2021, OCR imposed 25 penalties for HIPAA Right of Access violation totaling $1,564,650.

HIPAA v. Non-HIPAA



Rise of Consumer Privacy

EUROPE'S GDPR

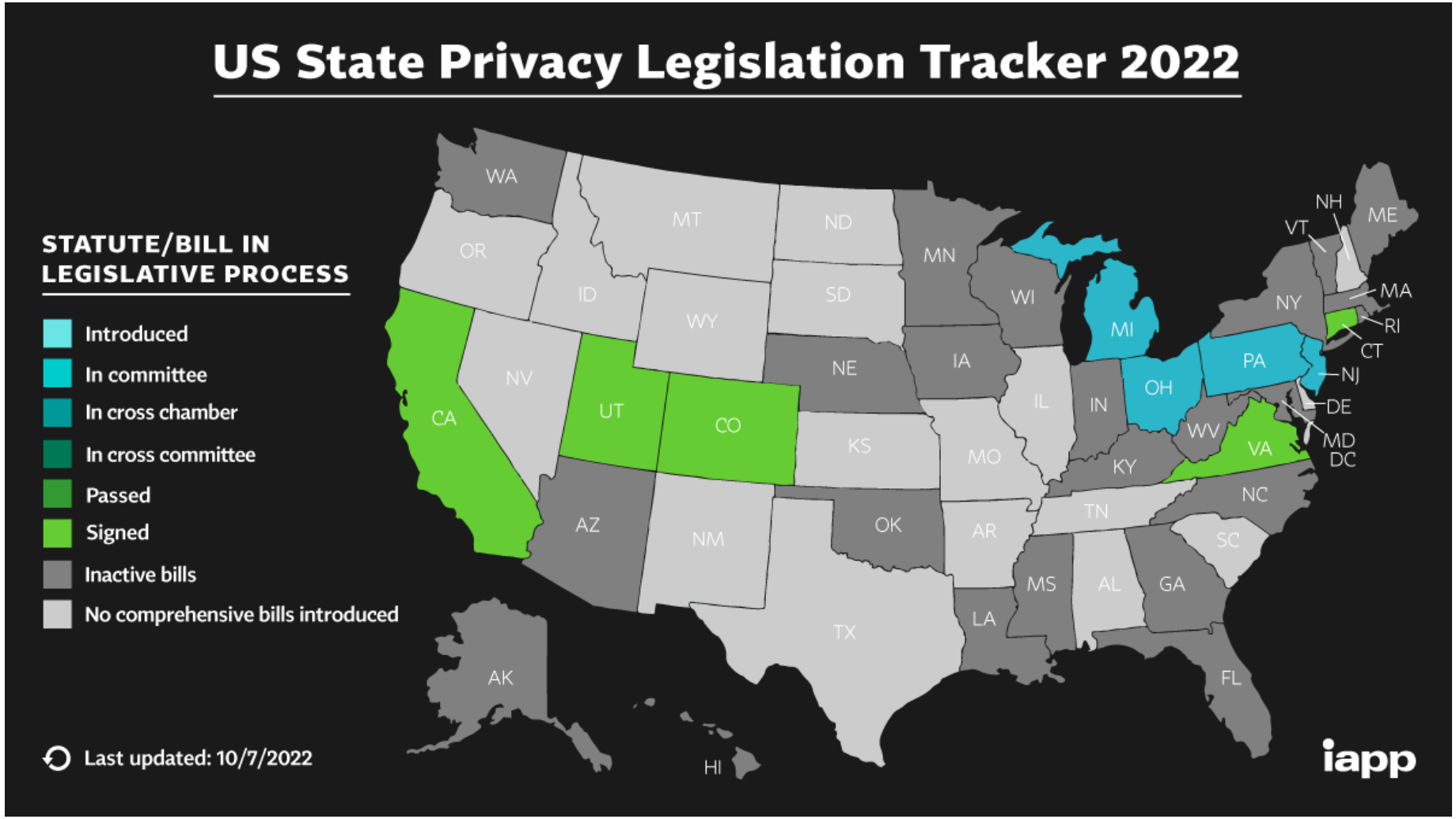
- Right of access
- Right to correct data
- Right to be erased
- Data portability

CALIFORNIA'S CCPA & CPRA – ENFORCEMENT BEGAN IN JULY 2020

- Right of access
- Right to have data deleted
- Right to know what's being collected
- Right to know whether data is sold and to whom
- Right to prevent sale of information

OTHER STATES

State Activity



HEALTH INNOVATION ALLIANCE

FTC Actions

- **Health Breach Notification Rule**
  - Revised Interpretation adopted September 15, 2021
  - Vendors of personal health records (PHR)
    - "identifiable health information on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual"
  - PHR related entity
  - Third party service provider
- **Advanced Notice of Proposed Rulemaking** – August 11, 2022
  - "Cracking Down on Commercial Surveillance and Lax Data Security Practices"

American Data Privacy and Protection Act

- Pallone and CMR with Wicker; Cantwell a no
- E&C passed; House “may” consider this year, but **California Conundrum**
- Bill includes –
  - Data minimization principle – some data you just can’t collect and use
  - Separate category of sensitive information, including treatment
  - Carves out HIPAA (kind of)
  - Federal preemption but not really because “state law preservation”

What Health Innovation Alliance is asking for:

1. **Fix de-identification**
2. **Include HIA privacy commission report**
3. **Create one federal privacy standard & remove the state preservation clause**
4. **Remove the private right of action**

HEALTH INNOVATION ALLIANCE

Take Aways

- Health data soon will flow to places it has not before, and there are no consistent rules in place
- States are acting
- Congress is stalled
- Administration is acting
- Private sector is exploring self-regulation
- Health-specific concerns
  - Need for health data to be liquid: innovation, research, patient safety
  - Patchwork of requirements

Questions & Discussion

HEALTH INNOVATION ALLIANCE

440 1st St, NW; Suite 430
Washington, D.C. 20001
WWW.HORIZONDC.COM
Brett Meeks
bmeeks@horizondc.com