2025 PUBLIC HEALTH LAW CONFERENCE

Connection. Collaboration. Community.

Privacy Officer Peer Group: Privacy at the Crossroads: Adapting to New Regulations and Developments

The Network for Public Health Law

Privacy Officer Peer Group

Phyllis Jeden, J.D.

Deputy Director,

Network for Public Health Law, Mid-States Region

William G. Hardison III

Administrative Project Manager,

Network for Public Health Law, Mid-States Region

About The Network

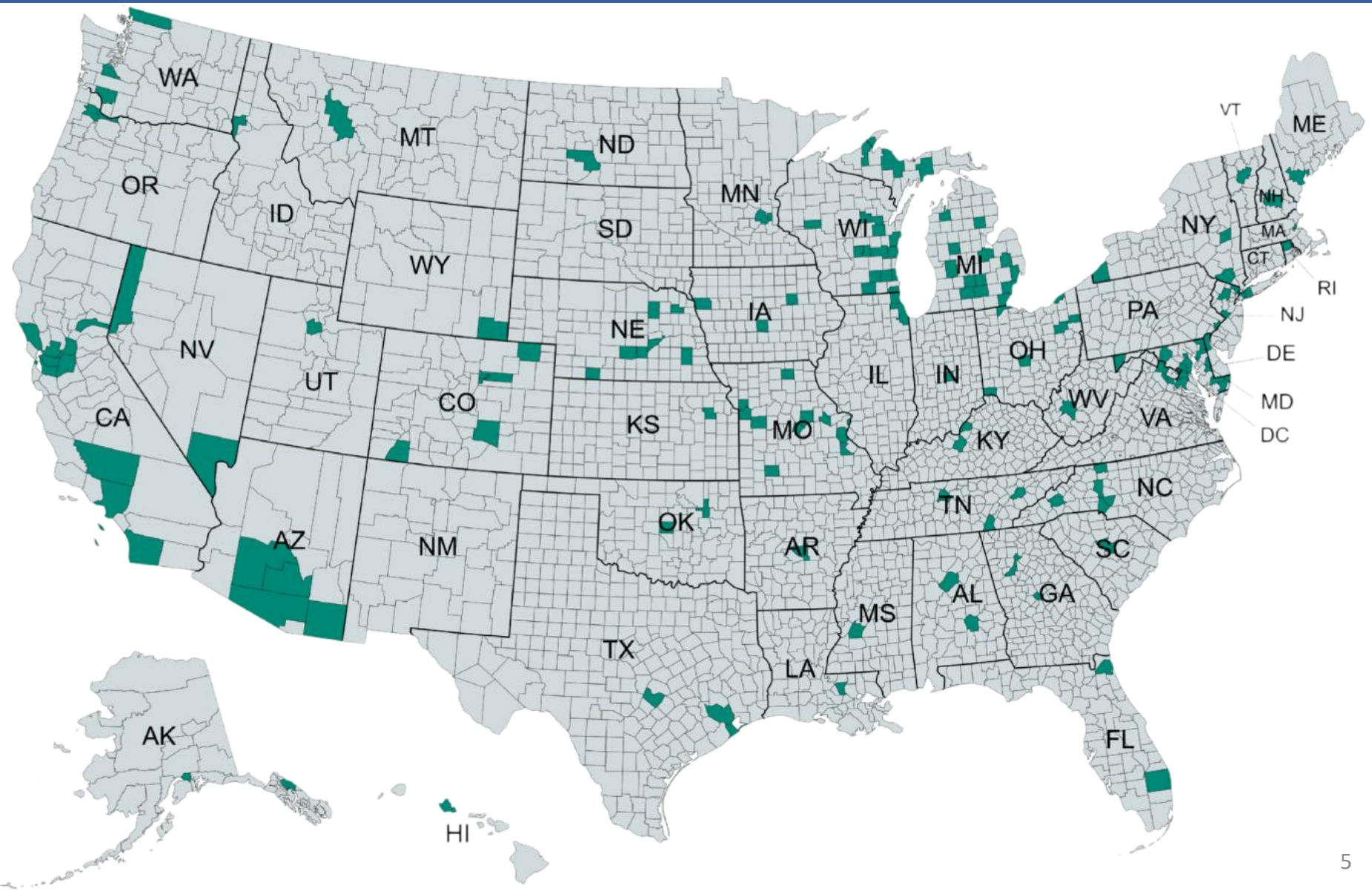
- The Network provides visionary leadership in the use of law to promote, protect and improve health and advance health equity.
- We work with local, tribal, state and federal public health officials and practitioners, as well as attorneys, policymakers, advocates and community organizations.
- We provide information, resources, consultation and training, as well as opportunities to connect.

The Fine Print

The Network promotes public health and health equity through non-partisan educational resources and technical assistance. Any materials provided in this presentation or through the Network's online resources are intended solely for informational purposes, and do not constitute legal advice. The Network's provision of these materials does not create an attorney-client relationship.

For legal advice, attendees should consult with their own counsel.

POPG Member Jurisdictions



The Network for Public Health Law

Agenda

- Welcome and Introductions
- Session Presentation- **Privacy at the Crossroads: Adapting to New Regulations and developments**
- Breakout Groups
- Report Out
- Closing

POPG Co-Chairs

Caterina Pañgilinan, MBA, CIPP-US, CIPM, CHPC, CHC. Caterina has over 25 years of experience in privacy, governance, risk management and compliance leadership within the private, not-for-profit, and public sectors. Currently, she serves as Maryland's State Chief Privacy Officer within the Maryland Department of Information Technology, where she leads the agency's privacy program, develops privacy policy, and provides advice to Executive departments on best privacy practices. Previously, she held the position of the Maryland Health Benefit Exchange's Chief Compliance and Privacy Officer.

Stephanie Elzenga, JD, Stephanie has served as the General Counsel for the Arizona Department of Health Services (ADHS) since April 2024. In this capacity, she leads the Department's legal functions and provides strategic counsel to the ADHS Director and leadership team. Before becoming General Counsel at ADHS, Stephanie was an in-house attorney at the Arizona Health Care Cost Containment System (AHCCCS), the state's Medicaid agency, where she held the position of Deputy General Counsel for Procedural Due Process and Compliance.

Session Speakers

Stephen Murphy, JD, Director, **Network for Public Health Law – Mid-States Region**

Meghan Mead, JD, Deputy Director, **Network for Public Health Law – Mid-States Region**

2024 UPDATES TO 42 CFR PART 2

42 CFR Part 2: 2024 Updates

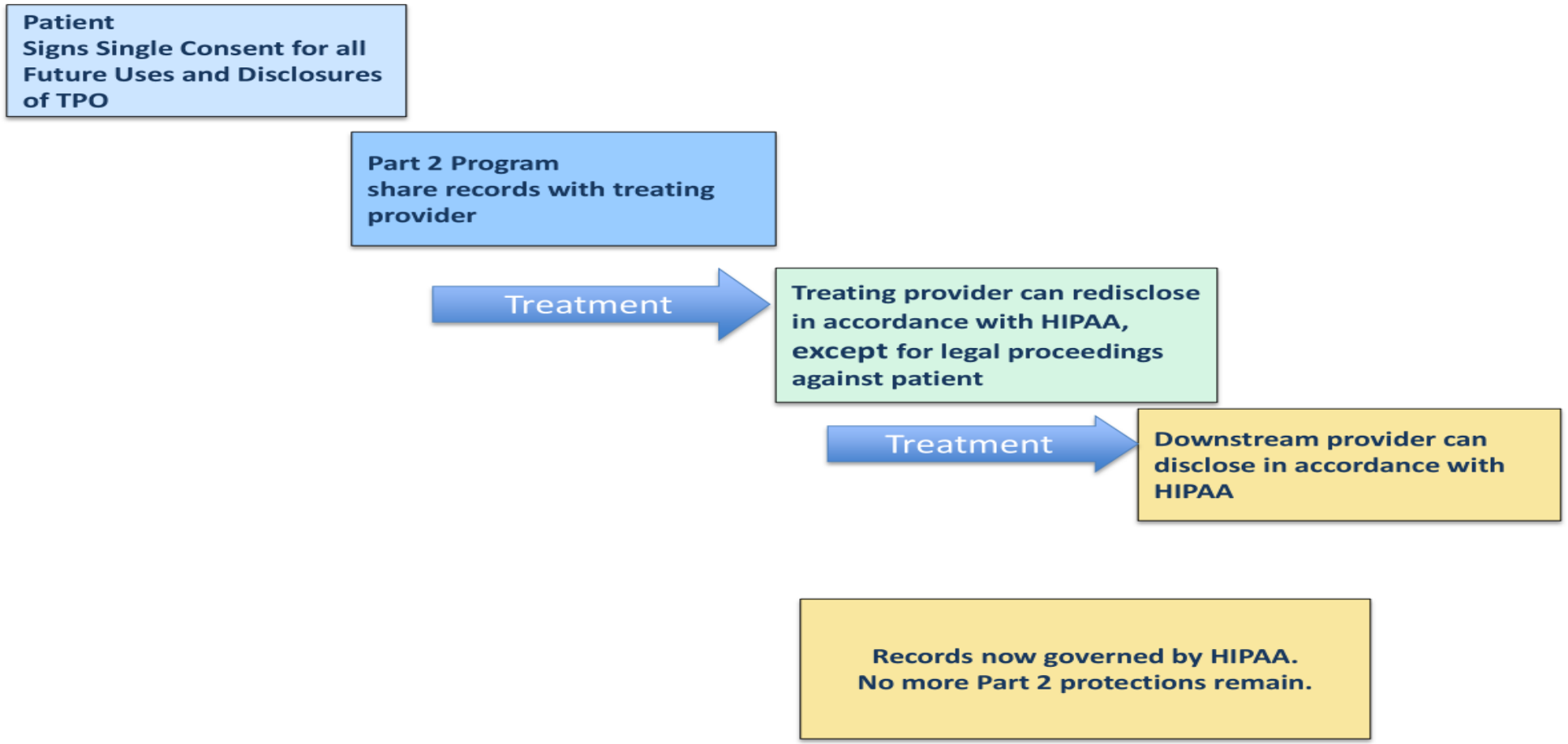
- Implements required changes from the CARES Act
  - More alignment between HIPAA and Part 2
  - Improve care coordination
- Effective date April 16, 2024
- Compliance date **February 16, 2026**
- The changes will affect every Part 2 program!

What is the same?

- Who is a Part 2 program
  - See Section 2.11
- Requirement for written consent for most disclosures
- Exceptions to consent (mostly)

TPO Consent

- TPO Consent
  - Single consent for all future uses and disclosures of TPO
  - No expiration date required
  - HIPAA covered entities and business associates can redisclose in accordance with HIPAA, except for legal proceedings against patient
  - As records move downstream, Part 2 protections disappear


Patient
Signs Single Consent for all Future Uses and Disclosures of TPO
Part 2 Program
share records with treating provider
Treatment
Treating provider can redisclose in accordance with HIPAA, except for legal proceedings against patient
Treatment
Downstream provider can disclose in accordance with HIPAA
Records now governed by HIPAA.
No more Part 2 protections remain.

No Combining Consent

- No combining certain consents
  - Substance use disorder counseling notes
  - Legal proceedings (criminal, civil, administrative, and legislative)
- HIPAA and Part 2 compliant consent template
  - Template: Consent for Uses and Disclosures of Part 2 Records | Focus:PHI

SUD Counseling Notes and Public Health

- SUD Counseling Notes
  - New definition analogous to psychotherapy notes under HIPAA
  - Substance Use Disorder Counseling Notes | Focus:PHI
- De-identified data can be shared with public health for public health purposes

Required Notice to Accompany Disclosures

Each disclosure made with the patient's written consent must be accompanied by:

- 1. the statement “42 CFR part 2 prohibits unauthorized use or disclosure of these records”, and
- 2. a copy of the consent or clear explanation of the scope of the consent.
- Notice to Accompany Disclosures of Information | Focus:PHI

Patient Rights

- Part 2 programs must have a complaint process for patients (§ 2.4)
  - Can submit to program or HHS
- Notice of Privacy Practices (2.22)
  - coe-phi-template-patient-notice-for-part-2-programs-2025.pdf

Patient Rights cont.

- Right to request restrictions on records (§ 2.26)
- Right to an accounting of disclosures (§ 2.25)

Policies and Procedures

- Part 2 programs and lawful holders must develop formal policies and procedures to protect patient records.
  - Applies to paper and electronic records.
  - Exceptions for friends, family and caregivers who are lawful holders.

Breach and Enforcement

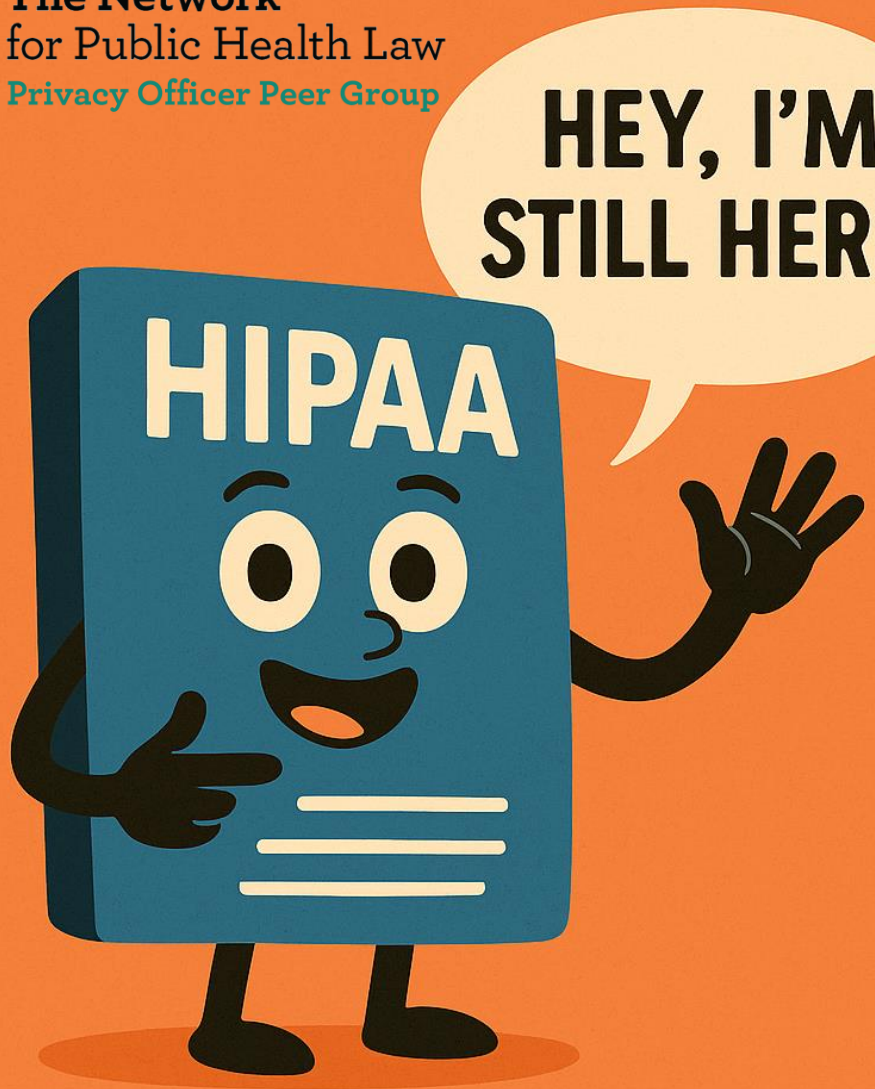
- HIPAA breach notification rule extended to Part 2 programs.
  - A breach includes uses and disclosures that violate Part 2.
  - Part 2 providers must notify patients and the secretary of HHS of a breach of patient records.
- Civil monetary penalties (like HIPAA)
  - Most enforcement moved from HHS to DOJ (except criminal)

Where to start?

- Update Notice of Privacy Practices and Consent Form
  - Use the templates
- Update policies and procedures
  - If HIPAA CE, update existing ones
- **Train staff!**
- Implementation Fact Sheet | Focus:PHI
- Reach out with questions!

The Network for Public Health Law

Privacy Officer Peer Group



Agenda

- HIPAA enforcement actions
- OCR's HIPAA Right to Access Initiative
- HIPAA Final Rule to Support Reproductive Health Care Privacy
- State efforts to protect data from inappropriate access or use


HIPAA
ENFORCEMENT
ACTIONS

OCR Enforcement Overview

- HIPAA Privacy Rule Compliance Date: April 2003
- Complaints Received: 374,321+
- Compliance Reviews Initiated: 1,193+
- Cases Resolved: 370,578 (99%)
- Civil Money Penalties & Settlements: 152 cases
- Total Dollar Amount: $144,878,972

No Violation or Early Resolution

- No Violation Found: 15,561 cases
- Early Intervention & Technical Assistance: 67,873 cases
- Not Eligible for Enforcement: 255,953 cases
- Reasons: OCR lacks jurisdiction, complaint withdrawn or untimely, activity permitted under HIPAA

Most Common Compliance Issues

- Impermissible uses/disclosures of PHI
- Lack of safeguards for PHI
- Lack of patient access to PHI
- Lack of administrative safeguards for ePHI
- Use/disclosure beyond the “minimum necessary” standard

Entities Most Often Subject to Enforcement

- General hospitals
- Private practices & physicians
- Pharmacies
- Group health plans
- Outpatient facilities


HIPAA ENFORCEMENT
ACTIONS - LAST 12 MONTHS

Entity Types

- Ambulatory Surgery Centers
- Behavioral Health Providers
- Specialty Medical Practices
- Radiology Groups
- Regional Health Systems
- Retail Health-Related Businesses
- Public Academic Medical Centers

Common Violation Types

- Failure to conduct accurate and thorough risk analysis
- Delayed breach notification (beyond 60-day HIPAA requirement)
- Impermissible disclosure of PHI (e.g., public portals)
- Insufficient safeguards against ransomware and phishing
- Failure to provide timely patient access to records

Ransomware & Cybersecurity Incidents

- Syracuse ASC – Ransomware, 6.5-month delay in notification
- Deer Oaks – Ransomware + public exposure of discharge summaries
- Neurology Practice – Ransomware, no risk analysis
- Northeast Radiology – Unsecured PACS server exposed imaging data
- Warby Parker – Credential stuffing attack

Breach Notification Failures

- Many cases involved late notifications to individuals and HHS
- Syracuse ASC – 6.5-month delay
- PIH Health – Delay after phishing attack affecting ~190,000 people
- OCR enforces 60-day rule strictly

Trends & Takeaways

- Risk analysis failures are the most common underlying problem
- Cyber incidents common
- Technical safeguards and timely notifications remain weak points
- OCR settlements usually include multi-year Corrective Action Plans
- Diverse entity types: large health systems to small practices

Reference

- Data compiled from HHS OCR enforcement announcements (2024–2025)
- https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html

OCR HIPAA Enforcement Actions – Government & Public Health Entities

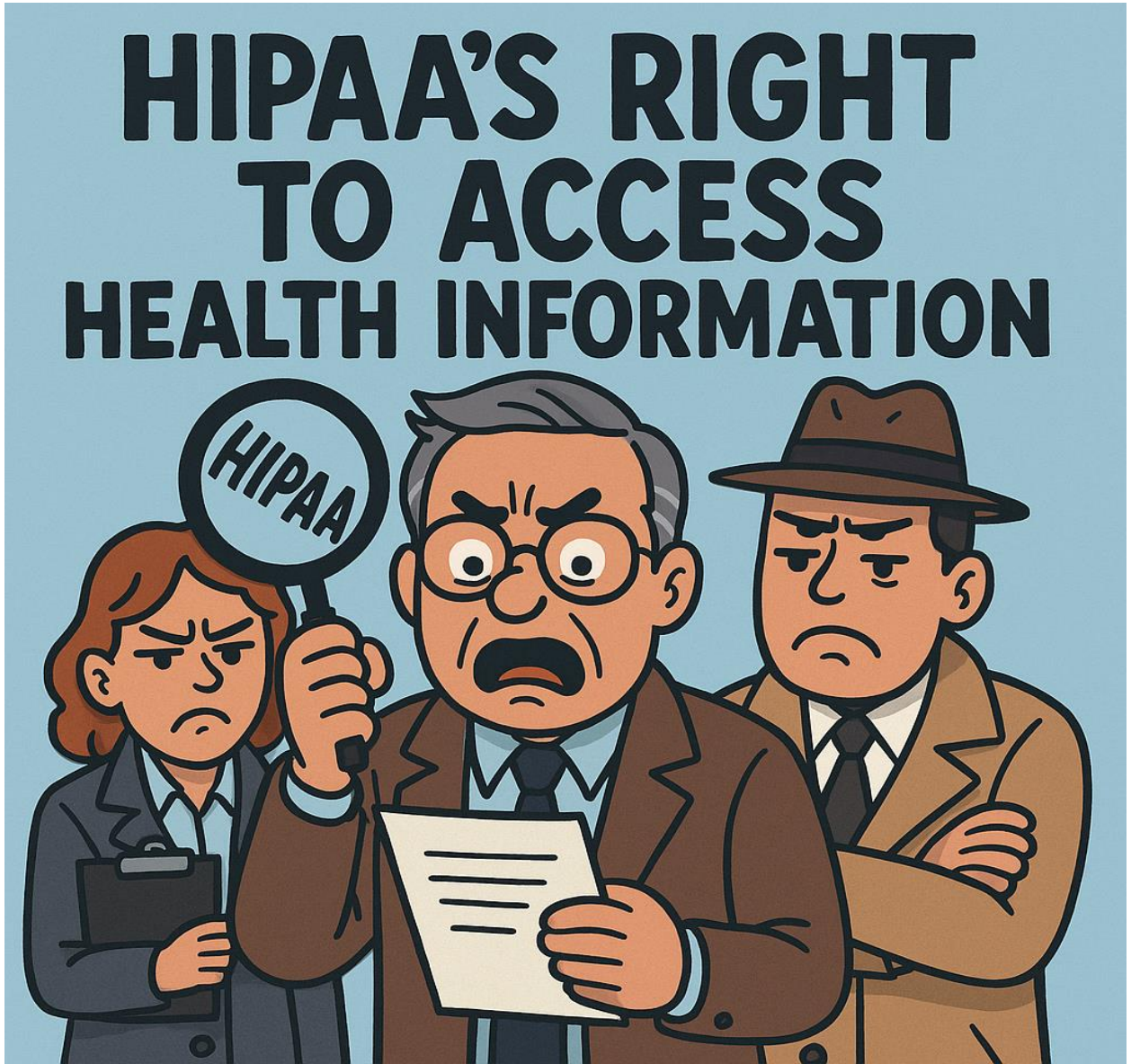
Government and Public Health Entities

- Alaska DHHS (2009): $1.7M settlement – No risk analysis, no encryption, no training
- Texas Health and Human Services Commission (2015): $1.6M CMP – No access controls, no risk analysis
- Guam GMHA (2018/2023): $25K settlement – No risk analysis, ransomware, unauthorized access

Key Themes & Insights

- Government/public health entities are not exempt from HIPAA enforcement
- Risk analysis failures and missing technical safeguards are central to violations
- Large penalties reflect systemic noncompliance; smaller penalties still require multi-year CAPs
- All entities must prioritize HIPAA compliance regardless of size or public/private status

OCR's Right of Access Initiative


HIPAA'S RIGHT
TO ACCESS
HEALTH INFORMATION
HIPAA

Right of Access Cases

- **Oregon Health & Science University** – March 6, 2025
  $200,000 penalty for failure to provide timely access to patient records
- **Memorial Healthcare System** – January 15, 2025
  $60,000 "to resolve pending admin litigation" in right of access case
- **Rio Hondo Mental Health Center** – November 19, 2024
  $100,000 penalty for failure to provide timely access to patient records
- **Gums Dental Care** – October 17, 2024
  $70,000 civil monetary penalty for failure to provide timely access to patient records

Purl v. HHS
The unraveling of the HIPAA Reproductive Health Privacy Rule

Purl v. HHS

The unraveling of the HIPAA Reproductive Health Privacy Rule

Background & Rule Details

- 2024 Final HIPAA Rule to Support Reproductive Health Care Privacy
  - Response to *Dobbs v. Jackson Women's Health*
  - Prohibited disclosure of reproductive health information for investigating or penalizing lawful care
  - Required pre-disclosure attestations ensuring PHI would not be used for prohibited purposes
  - Added definition of person and public health

Court's Ruling

- U.S. District Court (N.D. Texas) vacated the Reproductive Health Rule nationwide
  - Conflict with state laws on child abuse reporting and public health investigations
  - HHS redefined statutory terms beyond congressional authority
  - Applied Major Questions Doctrine – HHS lacked clear authority over politically significant reproductive health regulations

Implications & Next Steps

- Specialized protections from 2024 Rule no longer enforceable
- HIPAA Privacy Rule still protects reproductive health information
- Some state laws impose additional protections over repro
- Recommended:
  - Review and update policies, NPPs, BAAs, and training to reflect vacated rule
  - Maintain compliance with other HIPAA provisions and applicable state laws

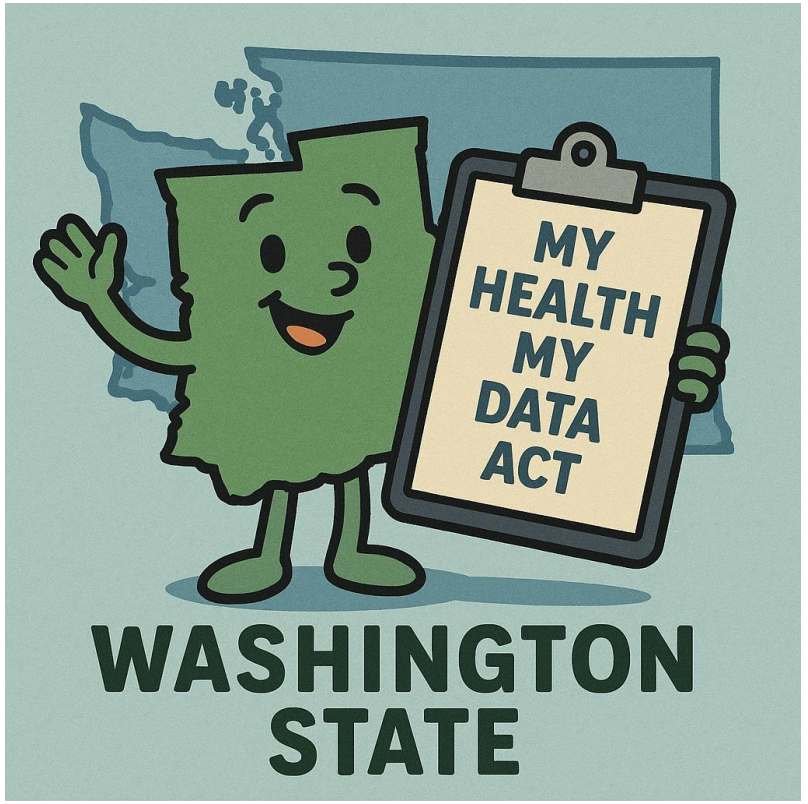
State Efforts to Protect Data from Inappropriate Access, Use or Disclosure

State efforts to protect data from inappropriate access or use

- State-by-state patchwork
- Increased activity around repro and gender affirming care
- CA, CT, DE, IL, MA, NJ, NM, NY, DC have passed shield laws around repro

State efforts to protect data from inappropriate access or use

- Consumer health data remains a concern
- Not typically protected by HIPAA
- Washington's My Health My Data Act
- Nevada's SB370 similar comprehensive health data privacy acts
- 19 states have consumer privacy laws
  - CA CPRA protections for sensitive data, including health data
  - VA amended Consumer Protection Act to prohibit obtaining/selling/disclosing repro health data without consent of consumer



State efforts to protect data from inappropriate access or use

- NY Health Information Privacy Act (Bill) SB 929
  - Privacy protections for "regulated health information"
  - Limits on collection/use, individual rights, consent, safeguards
  - No private right of action
  - Civil penalties up to $15,000 per violation/20% revenue

Questions?
Contact Stephen and Meghan

Stephen at smurphy@networkforphl.org
Meghan at mmead@networkforphl.org

Robert Wood Johnson Foundation

The Network for Public Health Law

The Network for Public Health Law is a national initiative of the Robert Wood Johnson Foundation.

Breakout Groups

Roundtable Topics

1. What privacy risks keeps you awake at night most?
2. Keep this to yourself! Shared privacy blunders and what we learned
3. Managing my privacy team of one. How I get the job done all by myself!
4. Part II provisions that are just plain tricky

Report Out

Thank you!

Upcoming POPG Peer Learning Sessions

- December 10th from 3-4 p.m. EST
- (Second Wednesday of Every Third Month)

PEER GROUP LISTSERVS

- **State Health Department Privacy Officers:** send an email to: privacy_officers@umich.edu
- **Local Health Department Privacy Officers:** send an email to localpopg@umich.edu
  - You can use the listserv to ask questions of your fellow privacy officers and to share ideas, relevant updates and resources
  - Only peer group members may use listservs
- **Questions:** Phyllis Jeden, Senior Attorney, pjeden@networkforphl.org or William Hardison, Project Manager, whardison@networkforphl.org

Thank you!

Upcoming POPG Peer Learning Sessions

- December 10th from 3-4 p.m. EST
- (Second Wednesday of Every Third Month)

SIGN UP FOR THE PEER GROUP LISTSERVS

State Health Department Privacy Officers

Local Health Department Privacy Officers:

2025 PUBLIC HEALTH LAW CONFERENCE

Connection. Collaboration. Community.

Please take this survey to evaluate conference sessions.

The Network for Public Health Law

THANK YOU