May 8, 2025

Riding the Privacy Rollercoaster: Considerations and Strategies for Health Data Privacy Compliance and Risk Mitigation in Uncertain Times

Melissa Levine
Hogan Lovells US LLP

Anna Park
Masimo

Privacy + Security Forum

Speakers

Privacy+ Security Forum

Melissa Levine

Partner
Hogan Lovells US LLP
Melissa.Levine@hoganlovells.com

Anna Park

VP, Compliance Officer & Data Privacy Counsel
Masimo
Anna.Park@Masimo.com

Agenda

Privacy+ Security Forum

- Current Landscape
- Federal Enforcement Areas to Watch
- State Enforcement Areas to Watch
- What to Do and Watch
- Risk Mitigation Strategies

Shifting and Evolving Landscape

Privacy+ Security Forum

- Significant shift in enforcement priorities and focus at federal level
- RIFs impacting staffing and agency resources
- State laws continuing to evolve
- Increased attention of State AGs
- Disrupters as many agency heads

HIPAA and OCR

HIPAA Rules

- Recent changes to HIPAA Privacy Rule around reproductive health and substance use disorder data
- Security Rule NPRM
- Prior NPRM from previous Trump administration OCR may have renewed focus

OCR

- OCR investigations and enforcement continue
- Enforcement largely focused on data breaches and security violations
- HHS gets to keep the fines OCR collects and may use the money to fund other priority HHS initiatives
- Less attention on web tracking expected
- Unclear if HIPAA compliance audits are going forward

HIPAA Security Rule NPRM

HIPAA NPRM

- Proposes **significant** revisions to the Security Rule's existing requirements pertaining to administrative, physical, and technical safeguards
- Public comments on the NPRM were due March 7, 2025
- Shifts away from the historical focus on flexibility of approach
    - Clarifies that HIPAA Security Rule **provisions are all requirements**, even for ones previously interpreted as optional (i.e., addressable vs. required under the existing Rule)
    - Defines **more granular and prescriptive requirements** to implement, maintain, and document regulated entities' implementation of the required security measures
- Increases accountability with new requirements to review and test written policies/procedures/controls **at least once every 12 months** or in response to environmental or operational changes, and modify as reasonable and appropriate

HIPAA Security Rule NPRM

Privacy+ Security Forum

- Proposal would require regulated entities to conduct and maintain:
  - Accurate and thorough written inventory
  - Network map of the entity's electronic information systems and all technology assets that may affect the confidentiality, integrity, or availability of ePHI
- Provides more specificity around risk analysis and risk management
- Expectation of encryption (in transit and at rest) and MFA, with some limited exceptions
- New obligation on business associates to provide written verification every 12 months that they deployed required technical safeguards through a written analysis of business associate's information systems
- Expansion of HIPAA Security Rule requirements to plan sponsors
- Additional onerous controls and testing requirements

HIPAA Repro and SUD

- Final rule, requirements were effective 12/12/2024 except NPP changes (effective 2/16/2026)
- Limits use and sharing of PHI potentially related to reproductive health
- Requires obtaining of attestation for certain disclosures of PHI potentially related to reproductive health
- Reproductive health broadly defined
- Requires changes to NPPs and policies, including to address SUD data
- Entities also incorporating changes into BAAs
- Will require notice and comment rulemaking to overturn/change in new administration unless court overturns (e.g., Texas case)
- May not be enforced by OCR under new administration

FTC and Federal AI Regulation

FTC

- New FTC chair will shift FTC enforcement focus and priorities
- Likely less enforcement of the more extreme positions of the prior administration's FTC, including on web tracking
- Increased focus on enforcement under COPPA

**Loper Bright decision impact resulting in less agency deference

Federal AI Position

- Shift at the federal level towards a deregulatory AI stance
  - Biden administration EO rescinded by the Trump administration
  - Trump administration EO "removes barriers" and promotes AI development as a matter of global economic competitiveness
- FTC aiming to foster AI innovation
- AI litigation likely to continue: claims of bias, discrimination, lack of transparency, improper use of data, data scraping

Current State of AI Regulation

Privacy+ Security Forum

- **Existing Federal laws**
  - HIPAA
  - Section 5 of the FTC Act
- **ONC Rule for decision support interventions in certified health IT**
  - Predictive decision support interventions integrated into certified health IT
  - Nutrition label on risk management (design, development, training, evaluation of predictive DSIs) for HCPs to understand limits or biases and confirm testing/validation
  - Describe data governance, how data acquired, managed and used
  - Evaluate and mitigate risks regarding accuracy, bias and safety
- **FDA draft guidance on use of AI**
  - Use of AI in research studies for drug and biological products
- **State AI laws (e.g., CO, CA)**
- **State AG guidance issuances (e.g., NJ, CA, OR)**

DOJ Data Security Program

- DOJ's Data Security Program (DSP) took effect April 8, 2025
- Imposes prohibitions or broad restrictions on brokerage transactions and vendor, employment or investor agreements involving access to bulk U.S. sensitive data by covered persons or countries of concern
  - Includes genomic and certain other 'omic data, health data
  - Particular impact on cross-border health sciences and clinical research
  - America First policy indicates enforcement focus on transactions involving China
- Covered data is broad—even includes fully de-identified or anonymized data
- Narrow exemptions
- Disruptive to deeply interconnected global operations
- Enforcement will be relaxed through July 8, 2025, for entities undertaking good faith efforts to comply

State Privacy Law

Enforcement Trends

- Class action litigation likely to continue regarding data breaches, security deficits, and web tracking
- State AGs have demonstrated a renewed interest in enforcing existing privacy laws in the absence of federal legislation
- State AGs are using existing privacy and consumer protection laws to regulate AI

Legislative Trends

- State laws likely to increase to fill federal void in certain areas
- New consumer health privacy laws have been enacted or will go into effect in 2025 (MD, NY, VA) with increasing restrictions and becoming more onerous
- States continue to consider AI legislation

State Law Developments

- 4 states have enacted data privacy laws specific to "consumer health data"
  - Connecticut Data Privacy Act ("CTDPA"), as amended by Senate Bill No. 3, *in effect*
  - Maryland Online Data Privacy Act, *effective October 1, 2025*
  - Nevada Revised Statutes 603A.400 *et seq.*, *in effect*
  - Washington My Health My Data Act ("WMHMDA"), *in effect*
- "Consumer health data" covers a broader range of information than traditional "health information" definitions under other laws
- DC and New York have proposed similar bills

State Law Developments

- **Notice obligations**
  - Distinct disclosure requirements for privacy policies
  - WMHMDA requires a separate website privacy policy
- **Opt-in consent** required for uses and disclosures of data that may be permissible under other state privacy laws
- **Consumer rights** must be offered (e.g., right to know, deletion)
- "Sales" of consumer health data requires a **written authorization**
- **Limited exemptions** for HIPAA regulated entities and data and research activities/data
- **Private right of action** under WMHMDA

What to do and Watch?

- **DOJ DMP Compliance**
  - Assess any transfers of or access to data and biospecimens to countries of concern, notably China
  - Assess any OUS access by vendors to sensitive data, even if not COC
  - Know where sensitive bulk data may be and where flows/access
  - Implement additional policies and processes
- **HIPAA compliance and Security**
  - Repro health requirements may ultimately be amended or negated by court
  - Security Rule compliance using NPRM as a guide on likely OCR thinking
  - **Avoid misleading statements** or promises around HIPAA compliance
- **Monitor FTC enforcement priorities**
  - While web tracking less of a focus, lawsuits continue and will be an issue under state laws
  - Less extreme FTC interpretations of consent and sensitive data—focus more on state law
- Address **privacy and security** more generally and assess **enhancements to security** and developing industry standard and expectations around security controls and responsibility
- Handle **data breach response** carefully and timely and, for large data breaches, with eye toward potential litigation

How to Mitigate Risk in 2025

- Document reasonable compliance in gray areas, show responsible steps taken
- **AI Risk Mitigation Themes**
  - Monitor legislation
  - Data Governance
  - Documentation, documentation, documentation
  - Transparency/Consent
  - Training, testing and validation
  - Mitigate risks of bias, discrimination, confabulations, hallucinations
  - Monitoring of outputs; “human-in-the-loop”
  - Data privacy and security considerations
- **Security** controls
- Careful and thoughtful **due diligence on vendors** and **documentation** of such
- Consent for **web tracking/cookies** and notice/transparency
- **Monitor** relevant state law developments and enforcement trends, and key litigation focus

Questions & Contacts

Melissa Levine

Partner
Hogan Lovells US LLP

Anna Park

VP, Compliance Officer & Data Privacy Counsel
Masimo