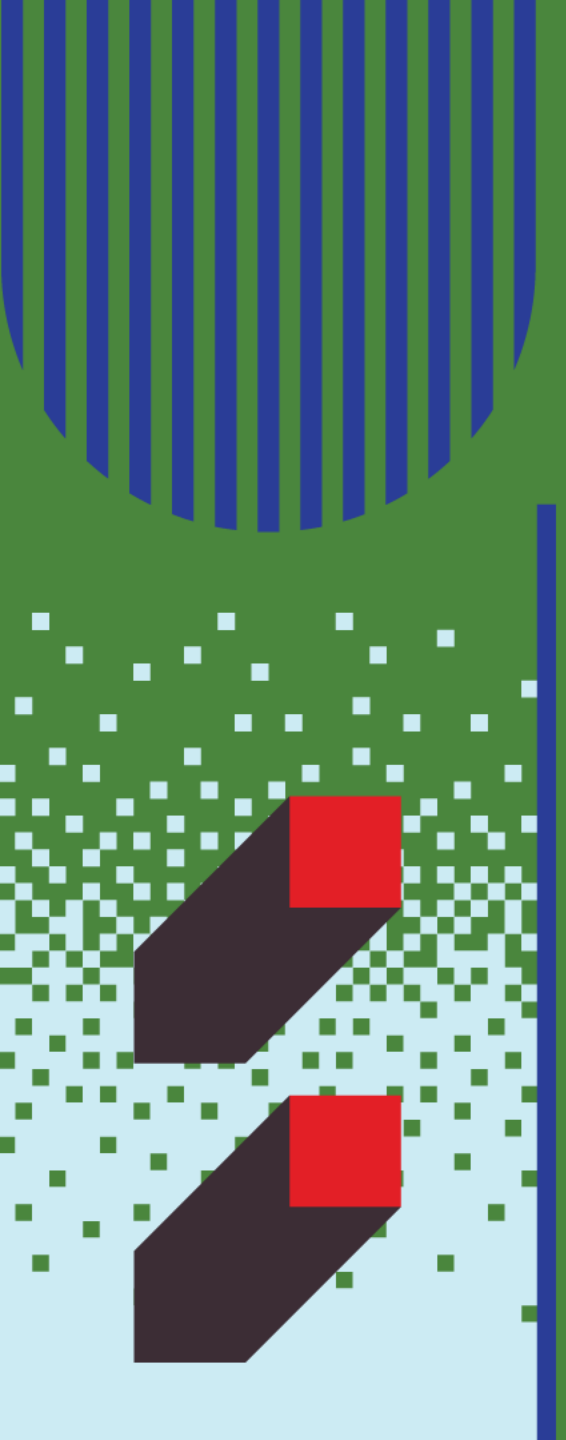


IAPP Global Summit 2026

Privacy | AI governance | Cybersecurity law

Conference 30-31 March

Workshops 1 April

Training 1-2 April

WASHINGTON, DC

#IAPPSummit26

HIPAA IS NOT ENOUGH!

Navigating the Complex Healthcare Privacy Landscape in 2026

WELCOME AND INTRODUCTIONS

Jason Loring, JD, CIPP/US, CIPM, FIP

Partner & Co-Chair, Privacy, Data Strategy and AI, Jones Walker LLP

Nikole Davenport, JD, LLM, CIPP/US, CIPM, FIP

Director, Privacy, Forvis Mazars

Eric Dentler, JD, CIPP/US, CIPP/E, CIPP/C, CIPM, FIP

Sr. Counsel, Data Privacy & Enablement, McKesson Corp.

TODAY'S AGENDA

Part I:
The Regulatory Landscape

- Beyond HIPAA: State Privacy Laws
- Data Exemptions
- Enforcement Trends
- Private Rights of Action
- AI in Healthcare

Part II:
Practical Compliance

- Key Steps for Compliance
- Privacy Assessment and AI Governance Frameworks
- Key Takeaways
- Q&A and Discussion

The Regulatory Landscape

Beyond HIPAA

The Emerging Problem

Healthcare data ecosystems have evolved far beyond HIPAA's original scope. Across enforcement, litigation and AI governance, healthcare organizations are now being penalized for data practices that are entirely outside HIPAA's scope.

Expanded Data Types

- Wearable device data
- Mental health apps
- Consumer genomics
- AI-generated insights
- Social determinants

New Entities

- Non-HIPAA tech platforms
- Health data brokers
- AI/ML service providers
- Telehealth platforms
- Research collaborators

Complex Rules

- State privacy laws
- Health-specific statutes
- FTC/FCC enforcement
- Private rights of action
- International transfers

State Privacy Laws: The New Baseline

Health-Specific State Laws

Washington My Health My Data Act
Broadest definition of "consumer health data"

New York Health Information Privacy Act
Strict consent requirements for non-HIPAA entities

Nevada SB370
Consumer health data privacy protections

Exemption Evolution

From Broad Entity Exemptions:
"If you're covered by HIPAA, you're exempt"

To Narrow, Data-Level Exemptions:
"Only HIPAA-regulated data is exempt"

Key States:
California, Connecticut, Minnesota, Montana and Oregon

Practical Impact: Data Exemptions

Many U.S. State privacy laws provide exemptions for entities subject to federal privacy laws, including HIPAA, GLBA, FCRA, FERPA, DPPA and FCA.

For example, consider a hospital system in California:

HIPAA-Regulated Data

(CCPA Exempt)

✓ Patient medical records
✓ Treatment information
✓ Billing data for healthcare
✓ Clinical trial data

Non-HIPAA Data

(CCPA Applies)

⚠ Employee HR data
⚠ Marketing preferences
⚠ Website analytics
⚠ App usage data

Risks for Healthcare Entities

2026 Compliance Concerns

- Website & Patient Portals
- Vendor & Digital Ecosystem Risk
- Biometric Data Risk
- Privacy Policy Mismatch
- AI Recording & Ambient Listening
- HIPAA-Adjacent but Not HIPAA-Defensible Risk

Non-HIPAA Privacy Risk Heat Map Table

RISK CATEGORY	LIKELIHOOD	IMPACT	VELOCITY	OVERALL RISK
Website & PatientPortal Tracking (Pixels, Analytics)	Very High	Very High	Fast	Critical
Privacy Policy / Practice Mismatch	High	High	Fast	Critical
Biometric Data (Workforce & Patient)	MediumHigh	Very High	Medium	Critical
AI Recording & Ambient Listening	Medium	Very High	Fast	Critical
VendorDriven Data Flows (Adtech, SaaS, AI)	High	High	Medium	High
State Consumer Privacy & Wiretap Statutes (General)	Medium	High	Medium	High
Traditional Data Breach Class Actions (State Law)	Medium	Medium	Slow	Moderate

Website Tracking

- Cookies & Pixels
- Largest Volume of Non-HIPAA Privacy Cases

Website tracking & pixel litigation (largest volume of cases)

Legal theories used:

Federal Electronic Communications Privacy Act (ECPA)

State wiretap laws

- California Invasion of Privacy Act (CIPA)
- Florida Security of Communications Act (FSCA)
- Pennsylvania Wiretapping Act

State consumer-protection statutes

Common-law breach of confidentiality

What triggered lawsuits:

Healthcare websites and patient portals embedded:

- Meta/Facebook Pixel
- Google Analytics
- Session replay or marketing APIs

These tools allegedly transmit medical-related web activity (conditions searched, appointment requests, portal usage) to third parties without consent

State AGs: Aggressive Enforcement

Even without comprehensive privacy laws, state AGs are acting:

Enzo Biochem (2024)
$4.5M - NY, NJ, CT
Largest state AG penalty
Data security failures

Albany ENT (2024)
$500K + $2.25M invest.
NY AG - Ransomware
213K patients affected

NY-Presbyterian (2024)
$300K - NY AG
Pixel tracking
54K affected

Healthline Media (2025)
$1.55M - CA AG
Largest CCPA settlement
Health website tracking

Orthopedics NY (2025)
$500K - NY AG
Cybersecurity failures
656K affected

Comstar (2026)
$515K - MA, CT AGs
Parallel AG + OCR
586K affected

Key Takeaway: State AG enforcement continues strong into 2026. Major healthcare actions in 2023-2026 exceeded **$12M in fines** plus mandated cybersecurity investments. Parallel enforcement (state AG + OCR) is increasingly common.

HIPAA/OCR Enforcement

OCR settlements remain compliance corrective, while state AG and private actions increasingly impose punitive and prescriptive remedies.

OCR Enforcement Actions - HIPAA

- OCR resolved 12 settlements in 2025 addressing privacy and security HIPAA violations.

Common Compliance Issues

- Issues include inadequate risk analysis, insufficient breach notifications, and lack of staff training.

Proactive Compliance Strategies

- Prioritize audits, employee training, and incident response to mitigate privacy risks effectively.

Regulatory Trends

- Regulators focus on proactive compliance rather than reactive responses to enhance resilience.

Enforcement: Multi-Agency Convergence

FTC: Section 5 Enforcement

Avast: $16.5M penalty for reselling browsing data
Focus: Unfair/deceptive practices, GLBA violations

HHS OCR: HIPAA Enforcement

12 settlements in 2025: focus on risk analysis, breach notification, and workforce training

FCC: TCPA & Robocalls

1,200+ providers disconnected in 2025
Key for healthcare: SMS consent, marketing calls

SEC: Cybersecurity & Privacy

$3.55M penalty for inadequate data security
Focus: Regulation S-P (GLBA financial institutions)

Private Rights of Action

Federal Laws Enabling Class Actions

Video Privacy Protection Act (VPPA)
PII from video viewing without consent.

Telephone Consumer Protection Act (TCPA)
Unsolicited calls/texts, auto-dialers.

Electronic Communications Privacy Act
Wiretap, tracking pixels and session replay.

Fair Credit Reporting Act (FCRA)
Credit data accuracy post-breach.

State Laws Enabling Class Actions

California Invasion of Privacy Act (CIPA)
Digital tracking, pixels and chatbots.

Illinois BIPA
Biometric data: fingerprints, facial scans.
Statutory damages per violation.

Washington My Health My Data Act
Health data privacy violations.

AI-Specific Privacy Risks

Data Collection

- Training data provenance
- Consent for AI processing
- Purpose limitation erosion
- Synthetic data risks
- Re-identification from de-identified data

Processing & Use

- Automated decisions
- Inferred health data
- Model interpretability
- Bias and fairness
- Vendor AI processing
- Examples include appointment prioritization, documentation tools and patient engagement chatbots

Security & Control

- Prompt injection attacks
- Data exfiltration via API
- Model inversion attacks
- Third-party AI tools
- Cloud AI services

AI Regulatory Landscape

EU AI Act (applies globally)

- Risk-based classification system
- High-risk: healthcare, employment decisions
- Transparency and documentation requirements

California: Multiple AI Laws

- Automated decision tech provisions in CPRA
- AI watermarking (AB 3211)
- Behavioral advertising restrictions

Colorado AI Act

- First comprehensive state AI law
- Algorithmic discrimination protections
- Impact assessments for high-risk systems
- Consumer rights: opt-out, explanations

Federal Activity

- Executive Orders
- FTC Section 5 enforcement authority
- FDA guidance for AI/ML medical devices
- NIST AI Risk Management Framework

Practical Steps

Tips for Compliance

Key Steps for Compliance

1. **Update Data Inventories**
   Segregate HIPAA vs. non-HIPAA data.
   Identify AI-generated or AI-processed data.

2. **Assess Geographic Reach**
   Map state privacy law applicability.
   Review entity vs. data exemptions.

3. **Audit Vendor Ecosystem**
   Identify AI/ML service providers.
   Review marketing tech stacks and analytics tools.

4. **Modernize BAAs**
   Assess multi-jurisdictional requirements.
   Add AI-specific terms and limitations.

Focus: Risk-based prioritization; start with patient-facing systems and high-volume data flows

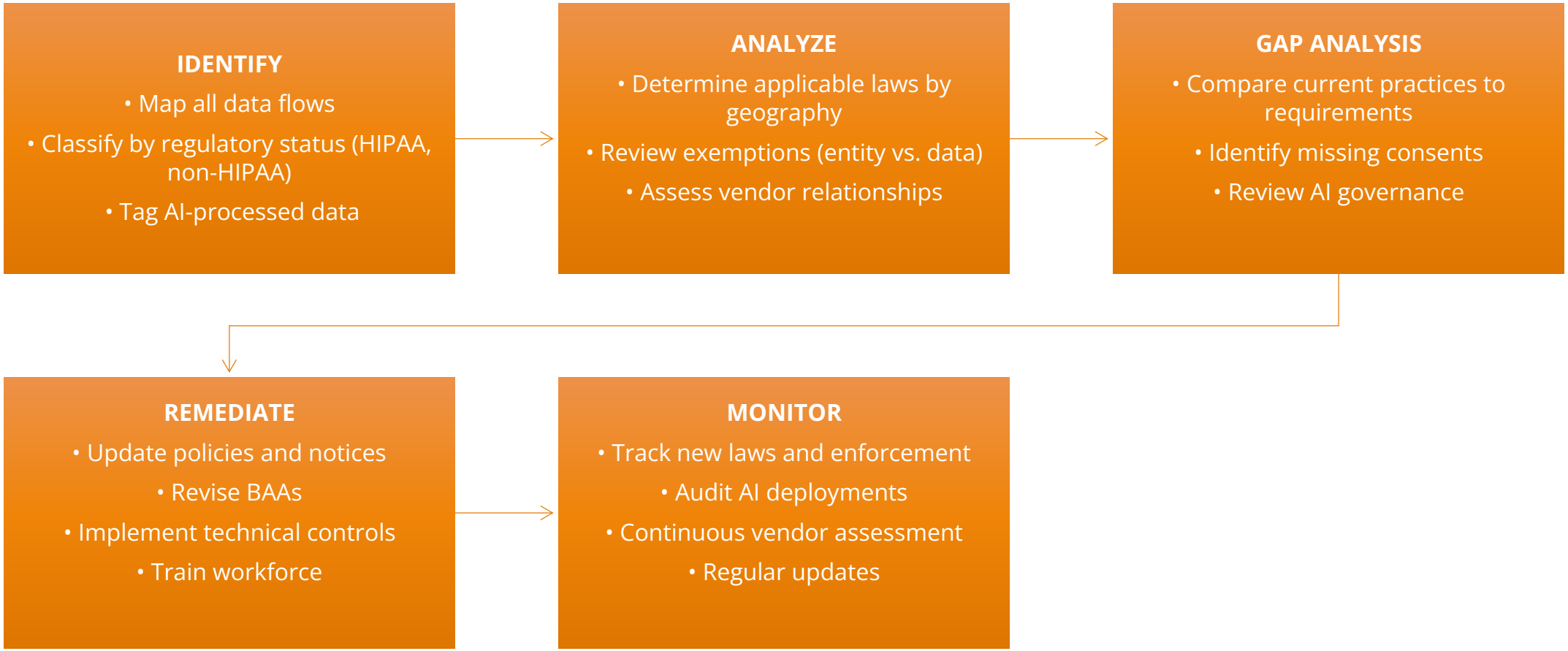
2026 Privacy Compliance Checklist

- ✓ Treat the HIPAA Security Rule NPRM as “directionally final”
- ✓ Modernize risk analysis → risk management (this is OCR’s core focus)
- ✓ Build and maintain a defensible ePHI asset inventory & data flow map
- ✓ Enforce baseline technical controls everywhere
- ✓ Prepare for revived HIPAA audits (not just complaint investigations)
- ✓ Update Right of Access workflows
- ✓ Ensure full compliance with 42 CFR Part 2 alignment (effective now)
- ✓ Elevate HIPAA governance to the board and executive level

How to Assess Privacy for Healthcare

Frameworks

Privacy Assessment Framework



Private Privacy Litigation Reality For Healthcare Entities

Evolving Litigation Landscape

In 2025, plaintiffs' firms bypassed HIPAA, targeting modern healthcare technologies in lawsuits.

High-Risk Technologies

The most expensive cases involved websites, marketing tech, portals, biometrics, and AI tools in healthcare.

Compliance Blind Spots

Lawsuits arose from teams deploying tools outside HIPAA risk assessments, including marketing and HR divisions.

HIPAA Limitations

HIPAA compliance alone does not shield healthcare systems from privacy lawsuits under non-HIPAA laws.

AI Governance Framework

Risk-based approach to AI in healthcare

Intake & Assessment

- AI use case questionnaire
- Risk classification
- Data flow mapping
- Vendor due diligence
- Privacy impact review

Contractual Controls

- Data use limitations
- Training restrictions
- Output ownership
- Model explainability
- Security requirements
- Breach protocols

Ongoing Monitoring

- Performance monitoring
- Bias testing
- Incident response
- Model retraining review
- Regulatory updates
- Annual reassessment

KEY TAKEAWAYS

1. **HIPAA is a Floor, Not a Ceiling**
   State privacy laws, health-specific regulations and AI requirements layer on top.

2. **Entity Exemptions Are Disappearing**
   Data-level exemptions mean healthcare orgs must comply with state laws for non-PHI.

3. **AI Creates New Privacy Risks**
   From training data to inferred health information to automated decisions.

4. **Private Rights of Action Are Real**
   Class actions under BIPA, CIPA, VPPA and TCPA can pose significant financial exposure.

5. **Vendor Management is Critical**
   BAAs must evolve to cover multi-jurisdictional and AI-specific requirements.

RESOURCES AND CONTACT INFORMATION

Key Regulatory Resources

- IAPP State Privacy Law Tracker
- HHS Office for Civil Rights (OCR)
- FTC Privacy & Data Security Updates
- NIST AI Risk Management Framework
- Washington MHMDA Implementation
- California CPPA Regulations
- EU AI Act Official Text

Speaker Contact Information

Jason Loring, CIPP/US, CIPM, FIP
jloring@joneswalker.com

Jones Walker AI Law & Policy Navigator
www.ailawblog.com

Nikole Davenport, CIPP/US, CIPM, FIP
nikole.davenport@forvismazars.com

Eric Dentler, CIPP/US/E/C, CIPM, FIP
eric.dentler@mckesson.com

How Did Things Go?
(We Really Want To Know)

Did you enjoy this session? Is there any way we could make it better? Let us know by filling out a speaker evaluation.

1. Open the IAPP Events app.
2. Select **IAPP Summit 2026**.
3. Tap "Schedule" on the bottom navigation bar.
4. Find this session. Click "Rate this Session" within the description.
5. Once you've answered all three questions, tap "Done".

Thank you!