FOLEY
FOLEY & LARDNER LLP

PYA

SESSION 2

AI and HIPAA

Trends Reshaping Compliance

January 22, 2026

Housekeeping

- Slides, handouts, and forms will be available in the **Resources panel**.
- You may enter questions in the **Q&A panel**.
  - If time allows, the presenters may answer questions, or they may contact you after the webinar.
- You can enlarge the panels, rearrange them, or close them to suit your preferences.
- If you run into any technical difficulties, step one is to refresh your browser.

Housekeeping (*continued*)

- **PYA is offering CPE and CHC credit.**
  - **CPE credit:**
    - You must be logged in for the entire duration of the session, and you must answer the three polling questions.
    - Once you successfully meet these requirements, you will see a CPE certificate available for download in the Continuing Education window; you will also receive a copy via email after the session.
  - **CHC credit:**
    - PYA will issue CHC credit certificates via email within 6 – 8 weeks following the event.

- **Foley and Lardner is offering CLE credit.**
  - **CLE credit:**
    - To be awarded CLE credit, you must be logged into the session for the entire duration of the program, and you must record the five-digit CLE code that will be announced later, on the attorney affirmation form located in the Resources panel.
    - You must sign and return the form after the session to LSHC Events at LSHCevents@foley.com
    - CLE credits will take 8 – 12 weeks to process.

Housekeeping (*continued*)

Please be sure to complete the “**CEU Survey**” found on your webinar dashboard so that we can determine the type of credit you are seeking.

Speaker Introductions

Jennifer Hennessy
Partner

Foley and Lardner LLP

150 East Gilman Street, Suite 5000
Madison, WI 53703

608.250.7420
jhennessy@foley.com

Jennifer Hennessy is a data privacy and cybersecurity attorney, advising clients ranging from multinational corporations to startups on all aspects of compliance with international, federal, and state data privacy and security laws. She is a partner in the firm's Technology Transactions, Cybersecurity, and Privacy Practice, a member of the Telemedicine and Digital Health Industry Team, the Health Care and Life Sciences Sector, and Innovative Technology Sector.

Jennifer assists covered entities and business associates in complying with Health Insurance Portability and Accountability Act (HIPAA) and advises organizations on compliance with federal law 42 C.F.R. Part 2 (Confidentiality of Substance Use Disorder Treatment Records), the EU's General Data Protection Regulation (GDPR), and state data privacy laws, including the California Consumer Privacy Act (CCPA).

She works with a broad array of clients in the telemedicine and digital health industry, most notably high-growth emerging companies and entrepreneurial technology groups. Her work focuses on health care privacy and security in digital health and multistate footprints. She also advises cash and self-pay telemedicine companies on privacy and security considerations.

Speaker Introductions

Chanley Howell
Partner

Foley and Lardner LLP

1 Independent Drive, Suite 1300
Jacksonville, FL 32202

904.359.8745
chowell@foley.com

Chanley Howell is a partner and intellectual property lawyer with Foley and Lardner LLP, where his practice focuses on a broad range of technology law matters. He is a member of the firm's Technology Transactions, Cybersecurity, and Privacy Practice and the Sports, Health Care and Automotive Industry Teams.

Chanley was named Innovator of the Year at Law.com's 2025 Florida Legal Awards. The annual Florida Legal Awards recognizes individuals and teams who have demonstrated leadership, innovation, and commitment to excellence across a wide array of practice areas. Highlighted in Jacksonville Magazine, Chanley was selected by his peers for inclusion in The Best Lawyers in America® in the field of Electronic Discovery and Information Management Law.

Chanley represents companies in a variety of technology law areas, such as Artificial Intelligence, mergers and acquisitions, software and technology agreements, data privacy and security compliance, and online/electronic contracts.

Speaker Introductions

Sarah Bowman
Principal, Healthcare Consulting

PYA, P.C.

6016 Brookvale Lane
Knoxville, Tennessee 37919

865.673.0844
sbowman@pyapc.com

Sarah is a nationally recognized revenue integrity, revenue management, and regulatory compliance expert. Her work often involves the intersection of coding and reimbursement into physician/hospital financial and strategic modeling, valuations, physician compensation, and productivity assessments.

Sarah specializes in regulatory compliance matters related to the 340B Program, proxy work relative value unit (work RVU) analyses, and initiatives related to black box payer reimbursement modeling.

Where Is AI in Health Care?

- Generative AI platforms tailored to healthcare workflows
- Growth in operational and administrative AI use cases
- Agentic AI and intelligent automation design
- Digital health integration: wearables, chatbots and remote care
- Advanced clinical AI applications: diagnostics and precision medicine

- Virtual assistants and patient chatbots
- Medical imaging and diagnostic assistance
- Predictive analytics and risk stratification
- Clinical Decision Support Systems (CDSS)
- Drug discovery and development optimization
- Natural Language Processing (NLP) and Electronic Health Record (EHR) automation
- Ai-augmented robotics and smart devices

Regulatory Developments and Compliance

FDA Risk-Based Regulatory Approach for AI/ML Systems

Guiding Principles of Good AI Practice in Drug Development

Considerations for the Use of AI in Regulatory Decision-Making

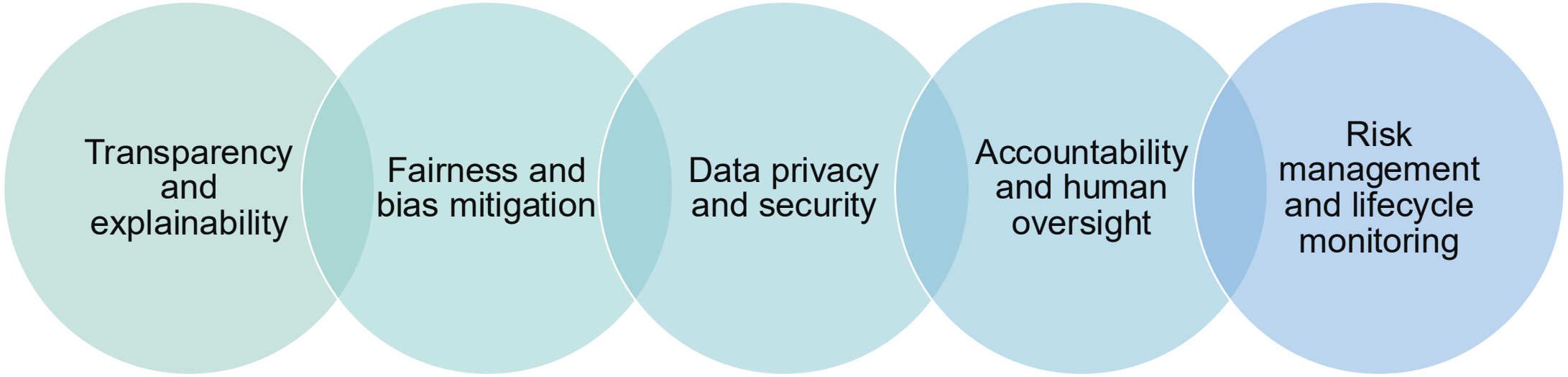
Artificial Intelligence and Machine Learning Software as a Medical Device (SaMD) Action Plan

Good Machine Learning Practice (GMLP) Guiding Principles

Regulatory Developments and Compliance

- Predetermined change control plans for adaptive AI/ML devices
- Lifecycle management and marketing submission for ai-enabled devices
- Transparency for machine learning-enabled medical devices principles
- FDA coordination across centers for AI in medical products
- Integration of AI regulation with existing U.S. healthcare laws

Common AI Compliance Themes



Connectors – Why They Change the Risk Profile

Connectors dramatically expand **blast radius**

Shift from “prompt-based disclosure” risk to **systemic over-exposure risk**

Risks introduced by connectors:		
Over-permissioning	**Lateral data movement**	**Indirect leakage through outputs**

Connectors – Why They Change the Risk Profile (*continued*)

- Governance must address:
  - Who can activate connectors
  - What repositories can be connected
  - Read-only vs. write-back permissions
- Connector activation treated as a **security-relevant event**
- Logging, access reviews, and kill-switches are essential

Employee Disclosure Obligations

- Employees need to be aware of:
  - Which AI tools are authorized for use
  - Which types of data are prohibited from being processed by AI
  - That the results generated by AI may sometimes be incorrect or partial

Employee Disclosure Obligations (*continued*)

Clear internal disclosures and training reduce:

- Compliance risk
- Employee misuse
- Inconsistent practices across teams

Alignment with:

- Code of Conduct
- InfoSec
- Privacy policies

Key Risks with AI Vendor Agreements

- Liability for AI outputs and errors
- Insufficient data privacy and security protections
- Inadequate indemnification and insurance coverage
- Lack of performance, bias, and safety guarantees
- Regulatory and compliance uncertainty

Polling Question #1

For your organization, what do you think is the top risk with respect to the use of AI?

1. Privacy and Security of PHI
2. Biased outcomes resulting in disparate access to health care and treatment
3. Hallucinations or inaccuracies resulting in adverse outcomes
4. Complying with emerging state and federal AI laws

FOLEY

FOLEY & LARDNER LLP

State Regulation of AI in Health Care

California

- California has passed multiple laws addressing the use of AI in health care in the past few years
  - Assembly Bill (AB) 3030 requires disclosures when generative AI is used to communicate patient clinical information, subject to exceptions when a licensed provider reviews the communication
  - AB 489 targets AI systems that could misrepresent themselves as licensed health care professionals, including in advertising or functionality
  - Senate Bill (SB) 1120 addresses AI use in utilization review and management functions in health coverage, emphasizing physician autonomy and auditability

Colorado and Texas

- Colorado:
  - SB24-205 imposes a risk-based structure, imposing duties for high-risk AI systems and obligations tied to foreseeable risks of algorithmic discrimination. Compliance date is June 30, 2026
- Texas:
  - SB 1188 requires health care practitioners using AI for diagnostic purposes to disclose that use and review AI-generated records consistent with medical record standards

Illinois

- Illinois House Bill (HB) 1806 prohibits licensed mental health professionals from using AI to:
  - Make independent therapeutic decisions;
  - Directly interact with clients in any form of therapeutic communication;
  - Generate therapeutic recommendations or treatment plans without review and approval by the licensed professional; or
  - Detect emotions or mental states.
- Also requires patient consent to use AI for “supplementary support”

FOLEY

FOLEY & LARDNER LLP

HIPAA Enforcement Initiatives:

Patient Right to Access

HIPAA Right of Access

- Individuals have a broad right to inspect and obtain a copy of their PHI maintained in a Designated Record Set
- CEs must:
  - Respond within 30 days
  - Provide individuals with all PHI included in a “Designated Record Set”
  - Provide access to PHI in the form and format requested
  - Charge only specified fees
  - Direct copies of PHI to third parties upon an individual’s request

HIPAA Right of Access Initiative

- In early 2019, OCR publicly promised to “vigorously enforce” the rights of patients to access and exercise control over their medical records
- Since the initiative’s announcement, OCR has settled over 50 “right of access” investigations

> *“A patient’s right to timely access their own health information is well-established by the HIPAA Privacy Rule. Health care entities must be responsive to their patients’ requests for their medical records. Patients should not have to file a complaint with OCR as a necessary step before receiving their records.”*
>
> – OCR Director, January 15, 2025

Right of Access Initiative – Settlements

- Affected covered entities ranged from large health care systems to smaller mental health care providers
- Alleged violations included failures to:
  - Provide timely access
  - Transmit PHI to third parties
  - Provide PHI in form and format requested
  - Charge proper fees
  - Properly deny access to psychotherapy notes
- Settlements ranged from $3,500 to $240,000, and required entities to undertake a corrective action plan (CAP) that incudes up to 2 years of monitoring

Access Case Study 1

1. Personal representative requested access to patient's records in April 2019
   - CE provided only part of the requested records
2. Personal representative filed a complaint with OCR in May 2020
   - OCR notified the CE of potential non-compliance with HIPAA Right of Access provisions
3. Same personal representative filed a second complaint with OCR in January 2021
   - OCR initiated investigation
4. CE did not provide all requested records until August 2021

Resolution: $200k penalty

Access Case Study 2

- Patient requested access to records multiple times by mail, telephone, and patient portal
  1) Dec. 30, 2020: Patient portal request
  2) April 25, 2021: Another patient portal request
  3) April 26, 2021: Mailed request
  4) May 23, 2021: Another patient portal request
  5) June 23, 2021: Patient filed a complaint with OCR
  6) Sept. 29, 2021: Records provided (*after* OCR had initiated an investigation)

Resolution: $60k penalty

(lowered from the initial $100k proposed by OCR; CE requested hearing before an ALJ, which resulted in the parties negotiating the settlement amount)

Polling Question #2

How long do Covered Entities have to respond to a patient request for access to PHI?

1. 15 days
2. 30 days
3. 45 days
4. 75 days

FOLEY

FOLEY & LARDNER LLP

HIPAA Enforcement Initiatives:

Security Risk Analysis

Security Risk Analysis (SRA)

- HIPAA Security Rule requires that HIPAA-regulated entities conduct "*an **accurate and thorough assessment of the potential risks and vulnerabilities** to the confidentiality, integrity, and availability of*" electronic PHI held by the entity and "*implement security measures sufficient to **reduce risks and vulnerabilities** to a reasonable and appropriate level*"
- Key takeaway: ensure the organization has an up to date and thorough risk analysis, as well as a risk management plan where identified risks and vulnerabilities are remediated in a timely manner

SRA Enforcement Initiative

- Since 2018, there has been a 264% increase in large breaches reported to OCR involving ransomware attacks
- Security Risk Analysis Enforcement Initiative announced in October 2024
- OCR settled multiple cybersecurity investigations over the past 12 months (penalties ranged from $10k – $1.5M)
- In 2025 alone, OCR settled 17 cybersecurity incidents
- OCR noted a failure to conduct a compliant SRA in those investigations

SRA Enforcement Initiative (*continued*)

"This enforcement initiative was created to focus select investigations on compliance with the HIPAA Security Rule Risk Analysis provision, a key Security Rule requirement, and the foundation for effective cybersecurity and the protection of electronic protected health information (ePHI)…OCR created the Risk Analysis Initiative ***to increase the number of completed investigations and highlight the need for more attention and better compliance with this Security Rule requirement****."*

– OCR Director Melanie Fontes Rainer

Provider – Ransomware Attack

- OCR received complaint that PHI maintained by provider on a server was accessible via the internet (i.e., unsecure server)
  - OCR notified provider
  - OCR found: (i) a failure to conduct an SRA; and (ii) failure to notify individuals of a breach
- Resolution: $25k penalty and two-year CAP

"Cybersecurity threats affect large and small covered health care providers. Small providers also must conduct accurate and thorough risk analyses to identify potential risks and vulnerabilities to protected health information and secure them."

– OCR Acting Director Anthony Archeval

Provider – CAP

- Notify affected individuals of a breach
- Conduct SRA:
  - Incorporate **all electronic equipment, data systems, programs and applications controlled, administered, owned, or shared by the provider** that contain, store, transmit or receive the provider's ePHI.
  - Must include "*a complete inventory of all electronic equipment, data systems, off-site data storage facilities, and applications that contain or store ePHI which will then be incorporated in*" the SRA
- Submit methodology, and then completed SRA, to OCR; conduct revised SRA if OCR requires it
- Do this annually for duration of CAP

Provider – CAP (*continued*)

- Develop enterprise Risk Management Plan to address risk and vulnerabilities identified in SRA, and submit to OCR for approval
- Revise HIPAA policies and submit to OCR for approval
- Review policies annually and submit revisions to OCR
- Enhance to HIPAA training
- Report all violations of policies and procedures to OCR
- Submit annual report of compliance to OCR

Business Associate – Ransomware Attack

- Business associate discovered part of network was infected with ransomware
  - Malware in network from Dec. 4-7, 2019 (4 days)
  - Cause: phishing email
  - Individuals affected: 170k
  - Reported to OCR: February 16, 2020 (i.e., appears to be timely)
  - OCR only lists the failure to conduct an SRA as the Covered Conduct

Resolution: $175k penalty and two-year CAP

Business Associate – CAP

- Conduct SRA:
  - Incorporate all electronic equipment, data systems, programs and applications controlled, administered, owned, or shared by the business associate or its affiliates that are owned, controlled or managed by the business associate that contain, store, transmit or receive the business associate's ePHI.
  - Must include "***a complete inventory of all electronic equipment, data systems, off-site data storage facilities, and applications*** *that contain or store ePHI which will then be incorporated in*" the SRA
- Submit methodology, and then completed SRA, to OCR; conduct revised SRA if OCR requires it
- Do this annually for duration of CAP

Business Associate – CAP (*continued*)

- Develop enterprise Risk Management Plan to address risk and vulnerabilities identified in SRA; submit to OCR for approval
- Revise HIPAA policies and submit to OCR for approval
- Enhance to HIPAA training
- Report all violations of policies and procedures or HIPAA to OCR immediately
- Submit annual report of compliance to OCR

Polling Question #3

What are the current HHS Enforcement Initiative(s)?

1. Right to Access
2. Security Risk Analyses
3. All of the above
4. None of the above

Additional Cybersecurity Settlements

- **$600k settlement + 2-year CAP** for breach affecting 190k individuals after 45 employee email accounts compromised by targeted phishing attack
- **$25k settlement + 3-year CAP** for (i) ransomware attack affecting 5k patients; and (ii) two former employees accessed PHI after employment ended
  - CAP included requirement to (i) review the current access credentials for all user accounts, members of its workforce, and other credentialed users that currently have been granted access to ePHI; and (ii) modify or terminate access, credentials, accounts or privileges to prevent inappropriate access to ePHI

CLE Code Announcement

If you are seeking CLE credit today, please complete the attorney affirmation form and return it to Life Sciences and Health Care Events (LSHCEvents@foley.com) immediately following the program.

4KBVZ: Four, Kilo, Bravo, Victor, Zulu

Questions?

Contacts

Jennifer Hennessy
Foley and Lardner LLP
Partner | Madison

T: 608.250.7420
E: jhennessy@foley.com

Chanley Howell
Foley and Lardner LLP
Partner | Jacksonville

T: 904.359.8745
E: chowell@foley.com

Sarah Bowman
PYA, P.C.
Principal | Knoxville

T: 865.673.0844
E: sbowman@pyapc.com

About Foley

Foley and Lardner LLP is a preeminent law firm that stands at the nexus of the Health Care and Life Sciences, Innovative Technology, Energy, and Manufacturing Sectors. We look beyond the law to focus on the constantly evolving demands facing our clients and act as trusted business advisors to deliver creative, practical, and effective solutions. Our 1,100 lawyers across 25 offices worldwide partner on the full range of engagements from corporate counsel to intellectual property work and litigation support, providing our clients with a one-team solution to all their needs. For nearly two centuries, Foley has maintained its commitment to the highest level of innovative legal services and to the stewardship of our people, firm, clients, and the communities we serve.

FOLEY.COM

About PYA

For over 40 years, PYA has helped guide healthcare organizations through complex regulatory compliance challenges. PYA offers a comprehensive range of services—designing and evaluating compliance programs, conducting risk assessments, serving as an Independent Review Organization, supporting providers facing investigations or payer audits, advising on reimbursement and revenue management, providing fair market value compensation opinions, and analyzing impacts from acquisitions and affiliations. A nationally recognized healthcare management consulting and accounting firm, PYA serves clients in all 50 states from offices in six cities. PYA consistently ranks among *Modern Healthcare's* Top 20 healthcare consulting firms and *INSIDE Public Accounting's* "Top 100" Largest Accounting Firms.

PYAPC.COM

FOLEY
FOLEY & LARDNER LLP

PYA