



SESSION 2

## Trends in Healthcare Privacy and Security:

Cybersecurity, Patient Rights, and Reproductive Healthcare Information

January 23, 2025

Let's Talk Compliance

# 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:**

- The Compliance Certification Board (CCB)<sup>®</sup> has approved this event for Live CCB CEUs. PYA will issue CHC credit certificates via email within 6 – 8 weeks following the event.

- **Foley & 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](mailto: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 & Lardner LLP**

150 East Gilman Street, Suite 5000  
Madison, WI 53703

608.250.7420

[jhennessy@foley.com](mailto: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 & Digital Health Industry Team, the Health Care & 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



## Barry Mathis

Principal, Information Technology

**PYA, P.C.**

2220 Sutherland Avenue  
Knoxville, Tennessee 37919

800.270.9629  
[bmathis@pyapc.com](mailto:bmathis@pyapc.com)

Barry has over three decades of experience in the information technology (IT) and healthcare industries as a CIO, CTO, senior IT audit director, and IT risk management consultant.

He has planned and managed complicated HIPAA security reviews and audits for some of the most sophisticated hospital systems in the country. Barry is a visionary, results-oriented, senior-level healthcare executive with demonstrated experience in planning and implementing information technology solutions. He is adept at strategic development, project and crisis management, and negotiation.

Barry's strong technical capabilities combined with outstanding presentation skills have made him a sought-after speaker at many conferences and events.

# Presentation Overview

- A refresher on HIPAA's right for individuals to access their own information
- HIPAA's reproductive healthcare information amendments
- Trends in healthcare cybersecurity:
  - Proposed updates to the HIPAA Security Rule
  - Announcement of HHS Security Risk Analysis enforcement initiative
  - Recent U.S. Department of Health and Human Services (HHS) ransomware settlements
- Effective strategies for cyber event response, including the role of Artificial Intelligence (AI)
- Managing cyber risks with third-party vendors



---

# HIPAA's Right of Access



# HIPAA Right of Access

- Individuals have a broad right to inspect and obtain a copy of their Protected Health Information (PHI) maintained in a Designated Record Set.
- Covered Entities (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, HHS publicly promised to “vigorously enforce” the rights of patients to access and exercise control over their medical records.
- Since the initiative’s announcement, HHS has settled over 50 “right of access” investigations.

# Right of Access Initiative: Settlements

- Affected covered entities ranged from large healthcare systems to smaller mental healthcare 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 that includes up to 2 years of monitoring.



---

# Reproductive Healthcare Information

# Prohibited Activities

- PHI cannot be used or disclosed for any of the following activities:
  - To conduct a criminal, civil, or administrative investigation into any person for the mere act of seeking, obtaining, providing, or facilitating reproductive healthcare
  - To impose criminal, civil, or administrative liability on any person for the mere act of seeking, obtaining, providing, or facilitating reproductive healthcare
  - To identify any person for either of the above purposes

# Reproductive Healthcare

- Prohibition applies where the activity is in connection with any person seeking, obtaining, providing, or facilitating reproductive healthcare and the entity has determined the reproductive healthcare is lawful or otherwise protected by law.
  - *Presumed* to be lawful unless have actual knowledge to the contrary or requestor provides factual information demonstrating a “substantial factual basis” that the reproductive healthcare was unlawful.
- Reproductive healthcare = defined broadly to mean healthcare that affects the health of an individual in all matters relating to the reproductive system and to its functions and processes.

# Attestation Requirement for Disclosures

- Must obtain an attestation before using or disclosing reproductive healthcare information to:
  - Health oversight agencies
  - Law enforcement
  - Coroners or medical examiners
  - In judicial or administrative proceedings (including in response to subpoenas and court orders)
- Attestation must include a statement that the information will not be used for the Prohibited Activities and be signed by the person requesting the information, among other elements.
- HHS has published a model attestation.

# What Should Entities Do?

- Audit processes for reviewing and disclosing information pursuant to a request for medical records to understand what, if any, changes are necessary.
- This will need to include a process to ensure an attestation is obtained for all disclosures to health oversight agencies, law enforcement, or coroners or medical examiners, or in judicial or administrative proceedings *where any reproductive healthcare information is involved*, even if reproductive healthcare is not the focus of the request.



# Challenges

- Two lawsuits in Texas
  - State of Texas v. HHS
  - Purl v. HHS
- Enforcement under the Trump Administration





---

# Trends in Healthcare Cybersecurity

# Proposed Rule to Update HIPAA Security Rule

- On January 6, 2025, HHS published its proposed updates to the HIPAA Security Rule to strengthen requirements for HIPAA regulated entities to safeguard electronic health information from cybersecurity threats.
- The HIPAA Security Rule was drafted in 2003 and has not been substantively updated since that time.
- Healthcare organizations generally use other more sophisticated frameworks (e.g., the NIST Cybersecurity Framework, ISO 27001/27002, SOC2, etc.) to build out their cybersecurity program.
- Comments to the proposed rule are due March 7.
- Unclear how the Trump administration will view these proposed updates (although the first Trump administration was focused on cybersecurity).

# Key Proposed Updates

- Eliminates “required” versus “addressable” implementation specifications
- Requires a written inventory of technology assets and a network map
- More specificity for the risk analysis, which would be required annually
- Expands the technical safeguards, requiring encryption, multifactor authentication, patch management, network segmentation, configuration management, disabling network ports, vulnerability management and penetration testing
- Would require updates to Business Associate Agreements (BAAs):
  - Business associates would need to notify covered entities when activating the contingency plan.
  - Covered entities must annually obtain from business associates a written analysis and certification of compliance with the Security Rule’s technical safeguards.

# Security Risk Analysis Enforcement Initiative

- First settlement under the initiative was in October 2024 (ransomware attack).
- HHS Office for Civil Rights (OCR) Director Melanie Fontes Rainer stated: “*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.*”
- Key takeaway: Ensure your 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.

# Ransomware Settlements

- Since 2018, there has been a 264% increase in large breaches reported to OCR involving ransomware attacks.
- OCR settled multiple ransomware investigations in recent months.
  - Penalties ranged from \$90k – \$950k.
- OCR noted a failure to conduct a compliant risk analysis in those investigations.

---

# **Effective Strategies for Cyber Event Response**

## Including the Role of AI

# Preparation and Planning

## ■ Develop an incident response plan

- Create a comprehensive plan that outlines the steps to take during a cyber incident.
- Ensure it includes roles and responsibilities, communication protocols, and escalation procedures.
- Ensure the plan addresses all stakeholders.

## ■ Regular training and simulations

- Conduct regular training sessions and simulations to ensure that all team members are familiar with the plan and can execute it efficiently, this helps in identifying gaps and improving the plan.



# Detection and Analysis

- **Implement monitoring systems**

- Use advanced monitoring tools to continuously watch for suspicious activities.
- This includes network monitoring, endpoint detection, and intrusion detection systems.

- **Analyze incidents**

- When an incident occurs, perform a thorough analysis to understand its scope, impact, and root cause.
- This helps in making informed decisions on how to respond and prevent future incidents.

# Containment, Eradication, and Recovery

- **Contain the incident**

- Quickly isolate affected systems to prevent the incident from spreading.
- This may involve disconnecting systems from the network or disabling certain services.

- **Eradicate the root cause**

- Identify and eliminate the root cause of the incident.
- This could involve removing malware, patching vulnerabilities, or addressing misconfigurations.

- **Recover systems and data**

- Restore affected systems and data from backups.
- Ensure that systems are fully functional and secure before bringing them back online.

---

## AI in Cyber Event Response

# AI in Cyber Event Response

## ■ Enhanced threat detection

- Implement AI-driven tools that can analyze large volumes of data to identify threats.
- Machine learning algorithms can detect anomalies and patterns that may indicate a cyberattack.

## ■ Automated incident response

- Use AI to automate repetitive tasks in the response process, such as isolating affected systems, applying patches, or generating reports.
- This reduces response time and minimizes human error.

## ■ Predictive analysis

- Leverage AI to predict potential threats based on historical data.
- This helps in taking proactive measures to strengthen defenses and prevent incidents before they occur.

# Additional Tips

- **Collaboration and communication**

- Ensure effective communication and collaboration among all stakeholders, including IT, security, management, and external partners.

- **Continuous improvement**

- Regularly review and update your incident response plan based on lessons learned from past incidents and changes in the threat landscape.

- **Compliance and reporting**

- Ensure compliance with relevant regulations and standards.
- Maintain detailed records of incidents and responses for reporting and auditing purposes.

---

## **Managing Cyber Risks with Third-Party Vendors**

# Assessing Vendor Risk

- **Conduct thorough due diligence**

- Evaluate the vendor's security policies and practices.
- Review the vendor's compliance with relevant regulations.

- **Risk assessment**

- Identify and assess potential risks associated with the vendor.
- Classify vendors based on the level of risk they pose.

# Establishing Security Requirements

- **Define security requirements**
  - Clearly outline security requirements in contracts and agreements.
  - Include provisions for regular security assessments and audits.
- **Continuous monitoring**
  - Implement continuous monitoring of the vendor's security practices.
  - Ensure timely updates and patches to address vulnerabilities.



# Incident Response and Communication

- **Incident response plan**

- Develop a joint incident response plan with the vendor.
- Ensure clear communication channels for reporting incidents.

- **Regular communication**

- Maintain regular communication with the vendor on security matters.
- Conduct periodic reviews and updates to the incident response plan.

# Questions?



# Contacts



**Jennifer Hennessy**

Foley & Lardner LLP  
Partner | Madison

**T: 608.250.7420**

**E: [jhennessy@foley.com](mailto:jhennessy@foley.com)**



**Barry Mathis**

PYA, P.C.  
Principal | Knoxville

**T: 800.270.9629**

**E: [bmathis@pyapc.com](mailto:bmathis@pyapc.com)**

# About Foley

Foley & Lardner LLP is a preeminent law firm that stands at the nexus of the Health Care & 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**

ATTORNEY ADVERTISEMENT. The contents of this document, current at the date of publication, are for reference purposes only and do not constitute legal advice. Where previous cases are included, prior results do not guarantee a similar outcome. Images of people may not be Foley personnel.

© 2025 Foley & Lardner LLP

# 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**

