FOLEY
FOLEY & LARDNER LLP

PYA

SESSION 2

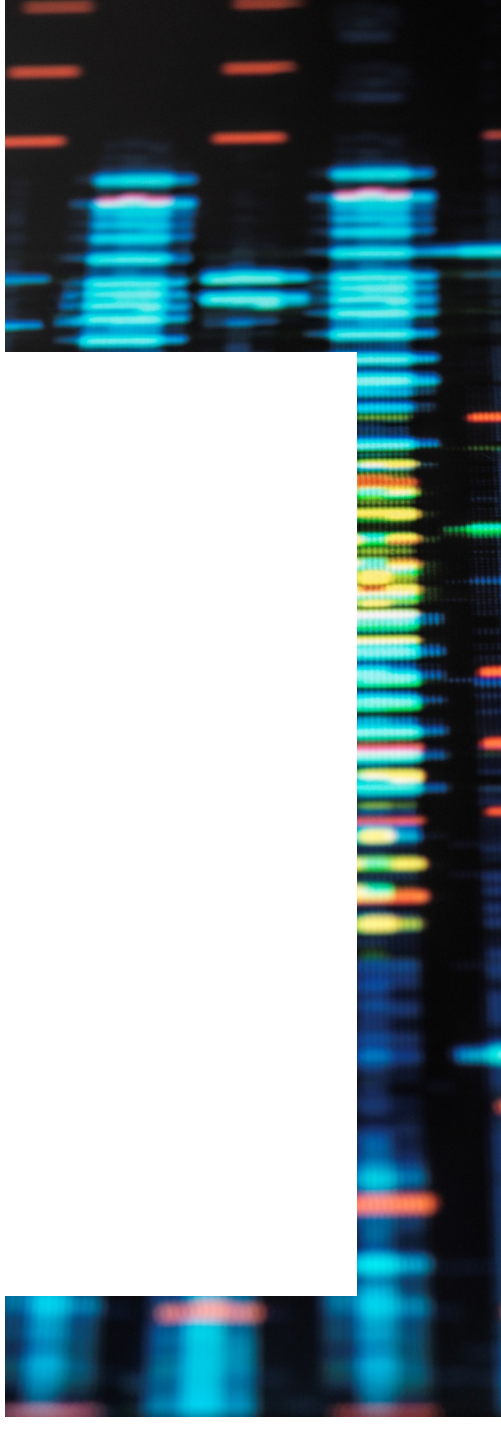
# Privacy, Security, and Artificial Intelligence: Patient Rights, Tracking Technologies, and Cybersecurity

January 18, 2024


FOLEY.COM

# Agenda

- Challenges and trends regarding the **use of AI** in the health care space.
- Considerations on the use of **tracking technologies** in the health care space.
- Recent trends in **health care cybersecurity**, including a discussion of health care related dark web activity.
- A refresher on HIPAA's **right for patients to access their own information**, in light of HHS' HIPAA Right of Access Initiative.
- Other trends in recent **HHS investigation settlements**.



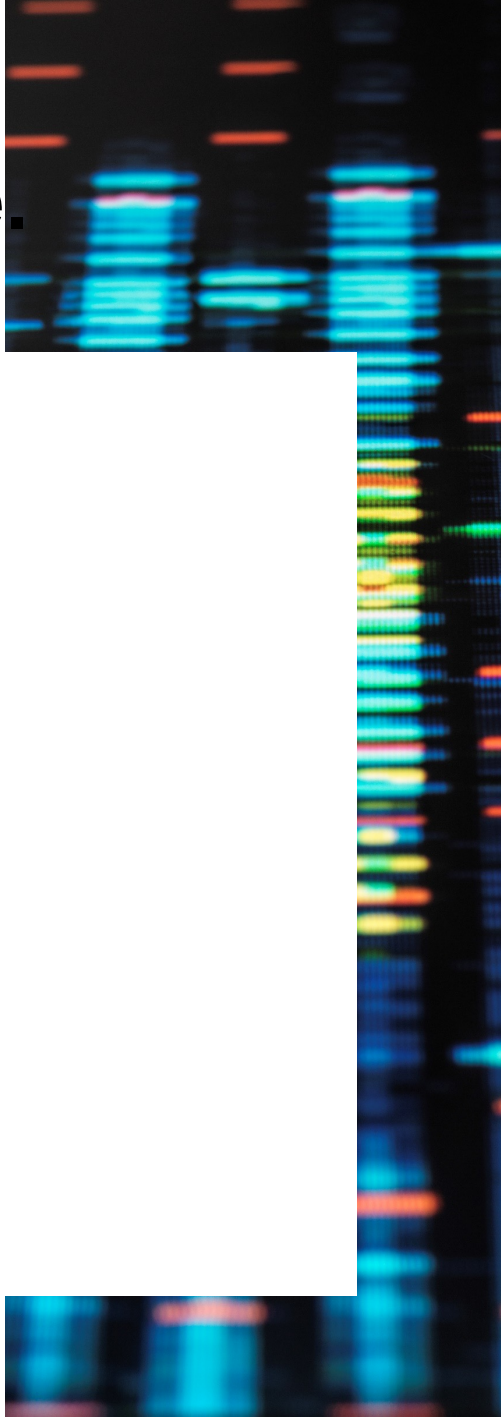
FOLEY

FOLEY & LARDNER LLP

PYA

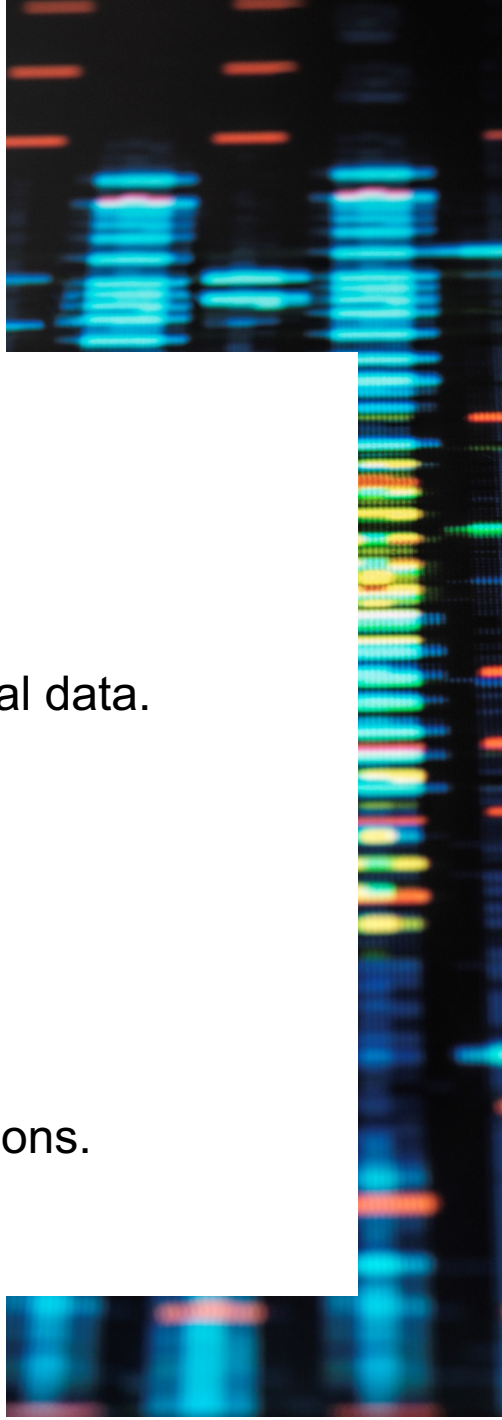
# AI: Challenges and Trends

# Key Challenges in Implementing AI in Healthcare.



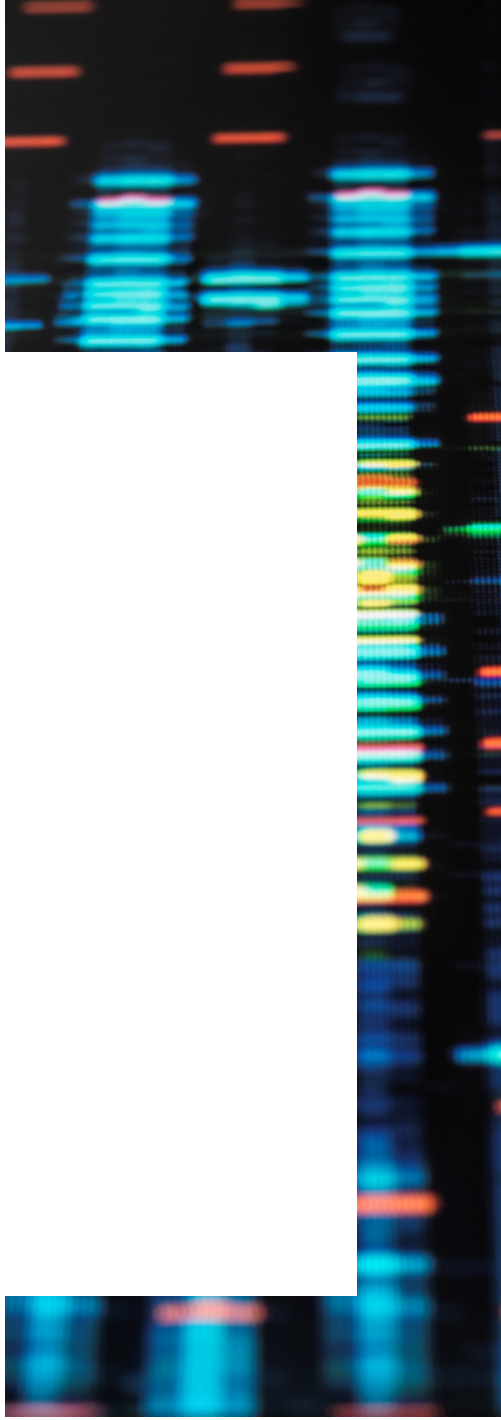
- **Data Privacy and Security**
  - Healthcare data is sensitive and must be protected.
  - AI systems must adhere to strict security measures to prevent data breaches.
- **Data Quality and Integration**
  - AI relies on high-quality data, but healthcare data is often fragmented and inconsistent.
  - Integrating data from various sources is challenging but essential for AI applications.
- **Regulatory Compliance**
  - Healthcare is heavily regulated, and AI systems must meet regulatory standards.
  - Ensuring compliance with laws like HIPAA is a complex task.
- **Ethical Concerns**
  - AI decisions can have life-altering consequences, raising ethical questions.
  - Bias, fairness, and transparency in AI algorithms are ongoing concerns.

# Trends Shaping the Future of AI in Healthcare



- **Predictive Analytics**
  - AI is used to predict diseases, patient outcomes, and healthcare trends.
  - Early diagnosis and proactive care are made possible through predictive analytics.
- **Personalized Medicine**
  - AI enables the tailoring of treatment plans based on an individual's genetic and medical data.
  - Precision medicine improves patient outcomes and reduces side effects.
- **Telemedicine and Remote Monitoring**
  - AI-driven telemedicine platforms provide accessible healthcare services.
  - Remote monitoring of patients using AI improves chronic disease management.
- **Drug Discovery and Development**
  - AI accelerates drug discovery by analyzing vast datasets and simulating drug interactions.
  - This leads to faster development of new treatments.

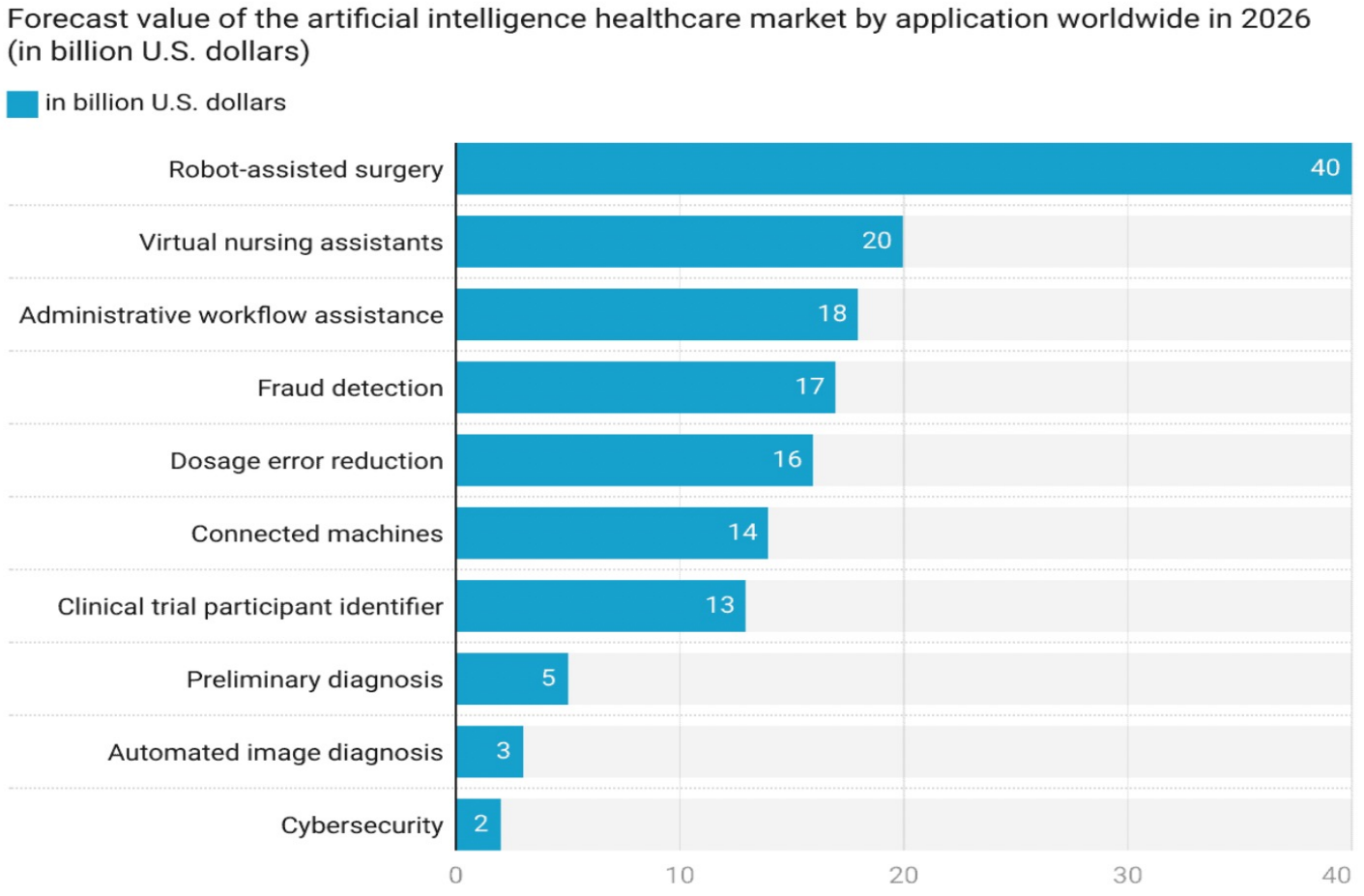
# Trends Shaping the Future of AI in Healthcare

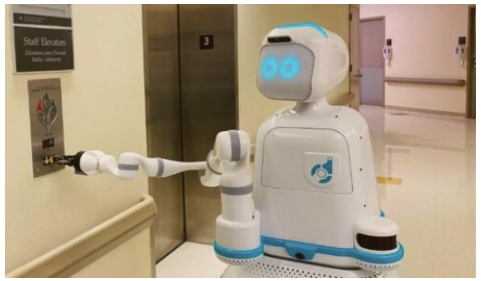


- 99% of healthcare leaders anticipate tangible cost savings as a result of investing in AI.
- 96% says AI plays a crucial role in the efforts to reach the organization's equity goals.
- 39% believe AI presents opportunities to ease administrative burdens.
- 72% of healthcare leaders trust AI to support non-clinical tasks.

Data included in a 2022 survey conducted by Optum. https://indd.adobe.com/view/7dbdcc49-f92e-4d5e-9ae3-dbc8661f23a4

# Global Healthcare Artificial Intelligence Market Value 2026, by Application

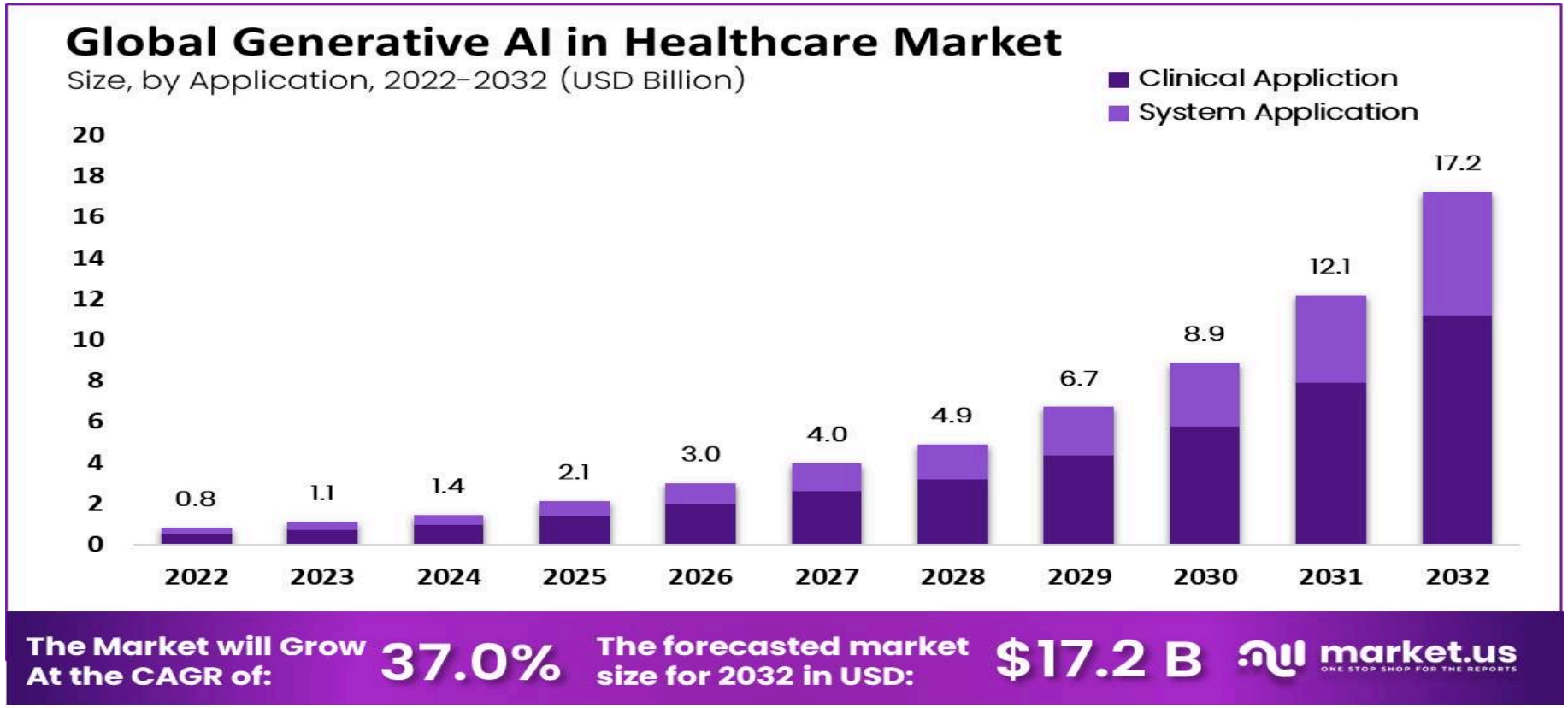




FOLEY & LARDNER LLP | PYA

# AI predicted spending in Healthcare



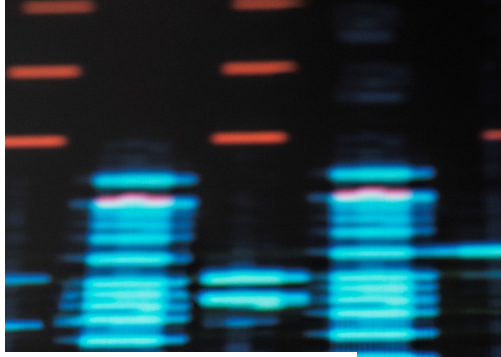

Data pulled from scoop.market.us.com

FOLEY
FOLEY & LARDNER LLP

PYA

# Tracking Technologies in the Health Care Space

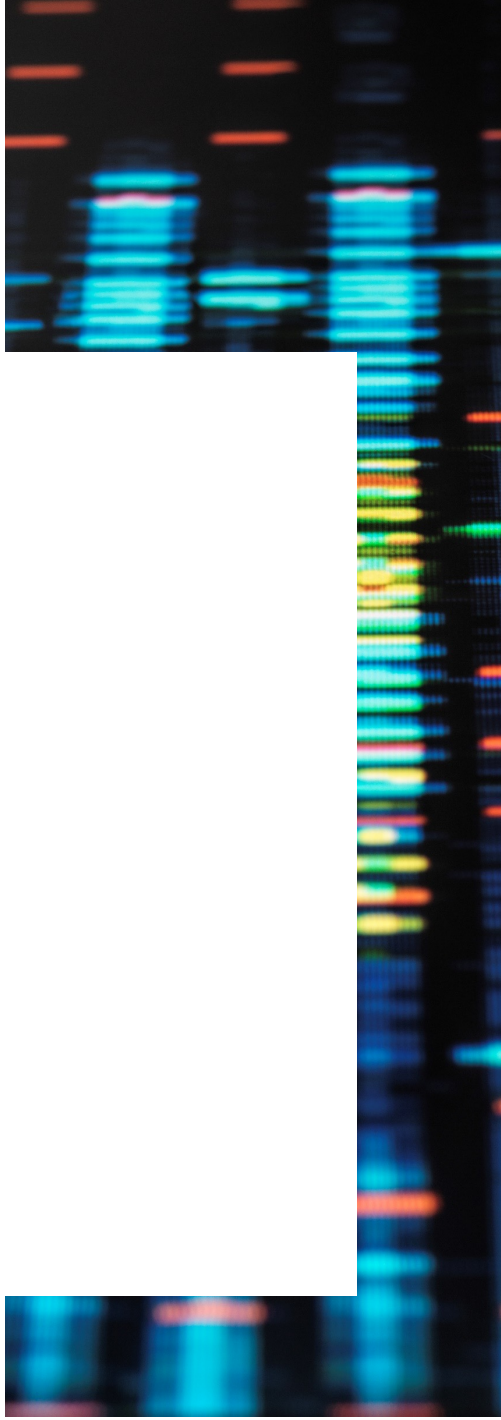
# History Leading Up To OCR Bulletin



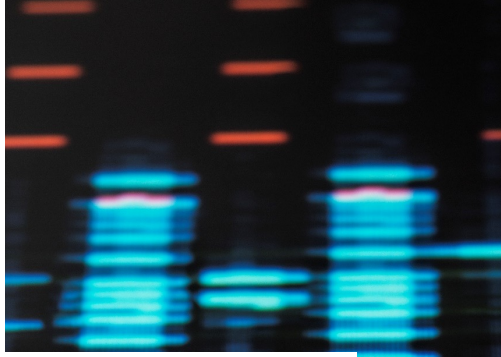
- **January 2021**: FTC action against fertility tracking app
- **June 2022**: Article on hospitals' use of tracking technologies within calendar apps; Roe v. Wade overturned
- **August 2022**: Data breaches & class action lawsuits filed
- **Dec. 1, 2022**: OCR Bulletin published

# Protected Health Information

- PHI means Individually Identifiable Health Information.
- HIPAA's definition of ***Individually Identifiable Health Information*** –
  - Information that is a subset of health information, *including demographic information collected from an individual*, and:
  - (1) Is created or received by a health care provider…; and
  - (2) Relates to the … (a) physical or mental health or condition; (b) provision of health care; or (c) payment for the provision of health care… to an individual; and
  - (3) That identifies the individual; or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.
- "***All such IIHI collected on a regulated entity's website or mobile app generally is PHI***, even if the individual does not have an existing relationship with the regulated entity and even if the IIHI, such as IP address or geographic location, does not include specific treatment or billing information like dates and types of health care services."



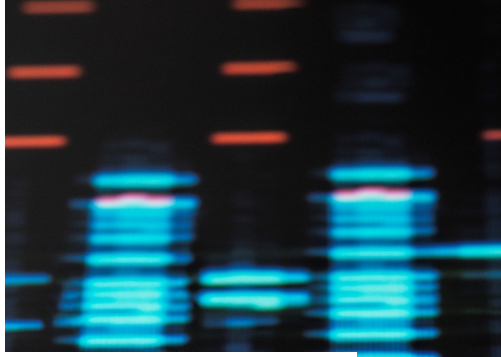
# OCR Bulletin: Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates



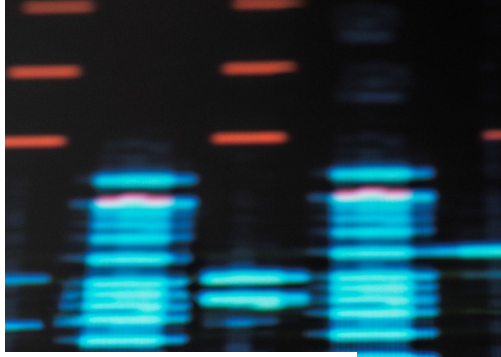
- Guidance:
  - Tracking on ***user-authenticated webpages***
  - Tracking on ***unauthenticated webpages***
  - Tracking within ***mobile apps***
  - HIPAA compliance obligations for regulated entities when using tracking technologies

# HHS/FTC Added Pressure

- **July 2023**: HHS/FTC sent letters to 131 health care organizations notifying the organizations that they “may be” using tracking technologies in violation of HIPAA.
- **September 2023**: HHS/FTC publicized the list of organizations that received the letters.



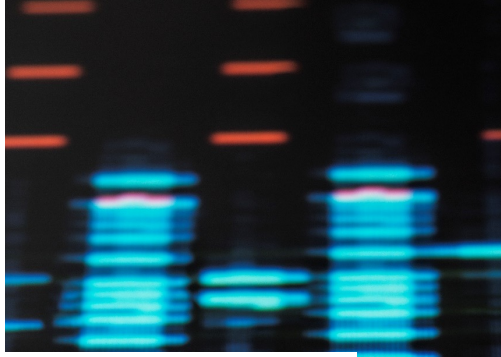
# AHA Lawsuit (Nov 2023)

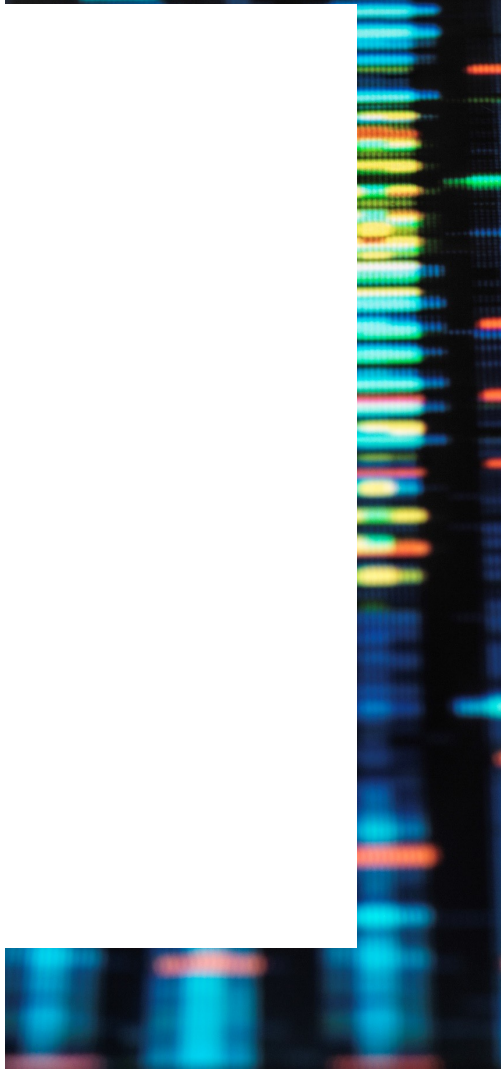


- AHA filed suit against HHS alleging that the bulletin exceeds its statutory authority under HIPAA.
- AHA seeks “to bar enforcement of an unlawful, harmful, and counterproductive rule that has upended hospitals’ and health systems’ ability to share health care information with the communities they serve, analyze their own websites to enhance accessibility, and improve public health.”
- AHA alleges:
  - HHS did not follow required notice-and-comment rulemaking processes.
  - Prior to issuing the bulletin, HHS did not consult with health care organizations about their use of third-party technologies that depend on the collection of IP addresses or the impact on patients.
  - IP address information on public facing webpages cannot reasonably be used to identify an individual whose health care relates to the webpage visit.

# Regulatory Implications & Next Steps

- Are tracking technologies being used?
  - Who, what, when, and where?
- What if not PHI?
- Don’t forget about other federal/state laws

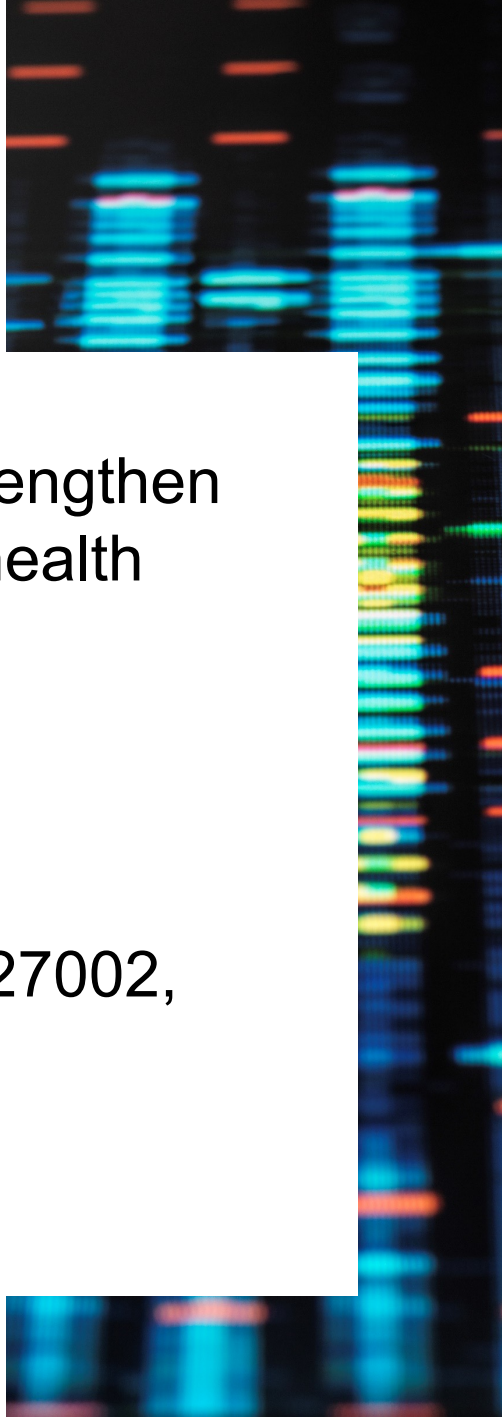





# Cybersecurity

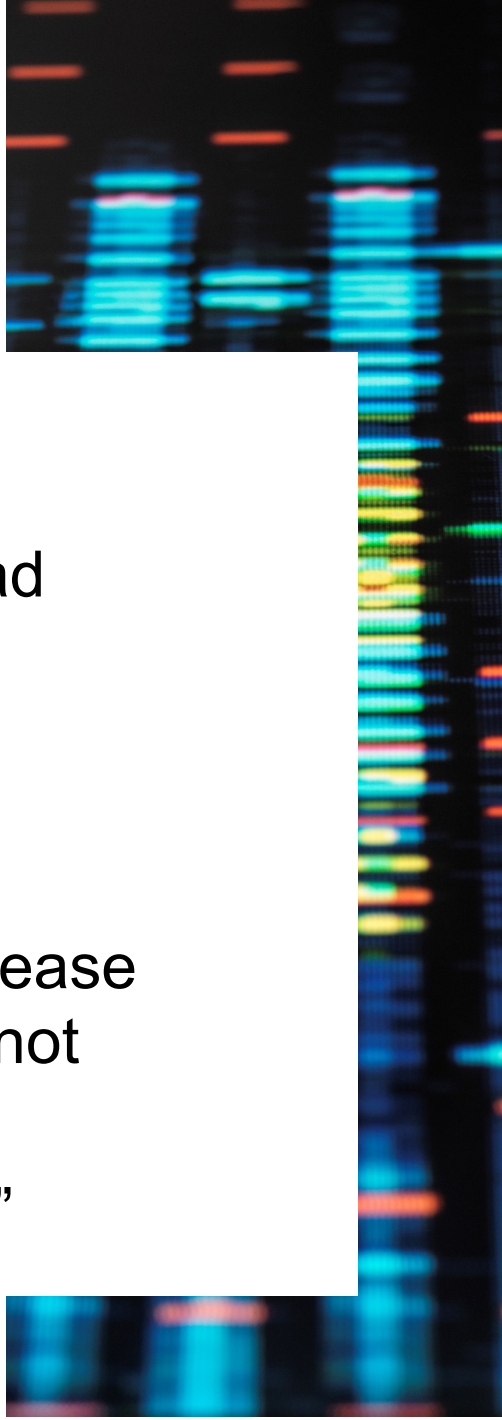
# Proposal to Update HIPAA Security Rule

- HHS is proposing to update the HIPAA Security Rule in 2024 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.
- Health care organizations generally use other more sophisticated frameworks (e.g., the NIST Cybersecurity Framework, ISO 27001/27002, SOC2, etc.) to build out their cybersecurity program.



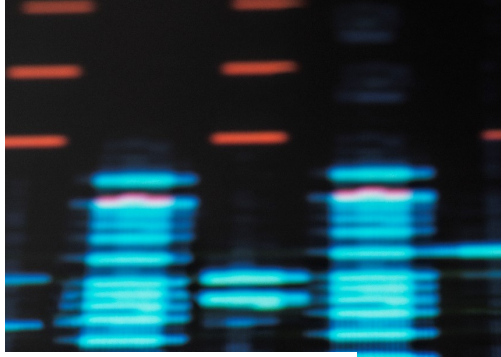
# HIPAA Safe Harbor Law

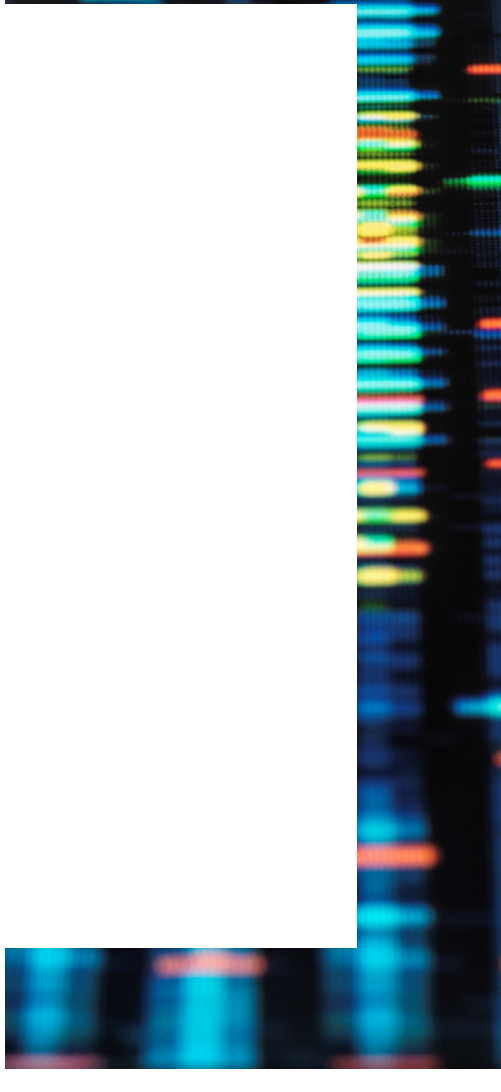
- Enacted January 2021
- Creates a “HIPAA safe harbor” for HIPAA regulated entities that had “recognized security practices” in place for at least 12 months.
  - Mitigate fines
  - Result in the early, favorable termination of an audit
  - Mitigate the remedies in settlement agreements
- The law expressly states it does not give HHS the authority to increase fines or the length, extent, or quantity of audits for entities that do not implement these “recognized security practices.”
- HHS soliciting input from public on “recognized security practices.”



# Dark Web Activity

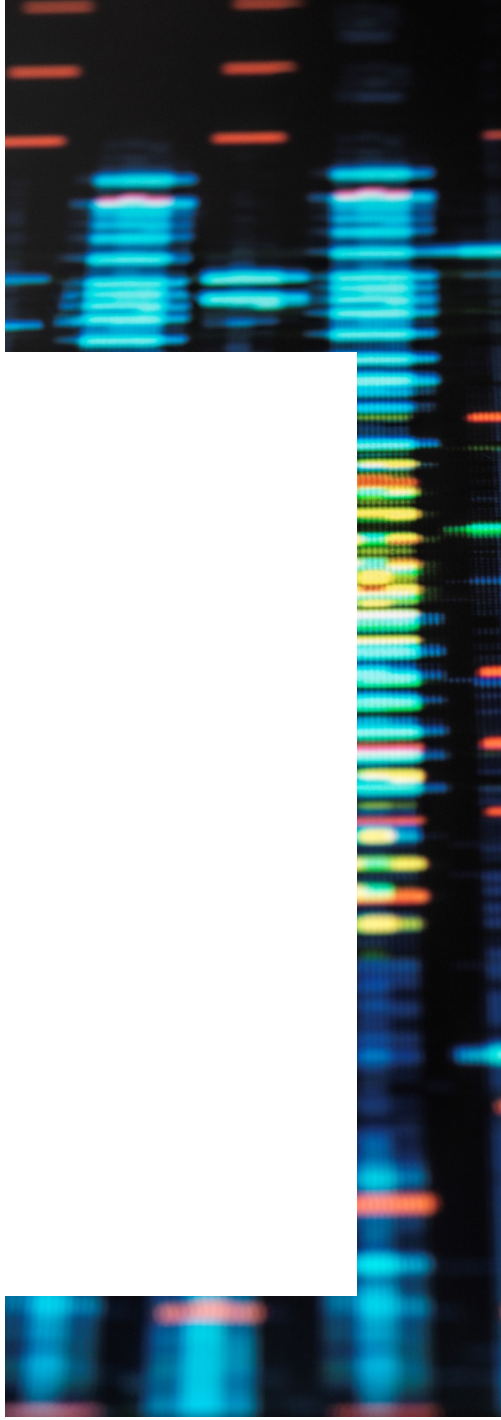
- **WormGPT**, appeared on the dark web on July 13, 2023.
  - Marketed as a ‘blackhat’ alternative to ChatGPT with no ethical boundaries, WormGPT is based on the open-source GPT-J large-language model developed in 2021.
  - Available in yearly $600 subscriptions, WormGPT, is allegedly trained on malware data.
  - Its primary uses are generating sophisticated phishing and business email attacks and writing malicious code.
  - The tool is constantly being updated with new features, which are advertised on a dedicated Telegram channel.





# Dark Web Activity

- **FraudGPT** appeared for sale on the dark web on July 22.
  - The tool—based on GPT-3 technology—is marketed as an advanced bot for offensive purposes.
  - Its uses include writing malicious code, creating undetectable malware and hacking tools, writing phishing pages and scam content, and finding security vulnerabilities.
  - Subscriptions start at US$200 a month through to US$1,700 for an annual license.
  - According to the security firm that discovered it, FraudGPT is likely focused on generating quick, high-volume phishing attacks, while WormGPT is more focused on generating sophisticated malware and ransomware capabilities.



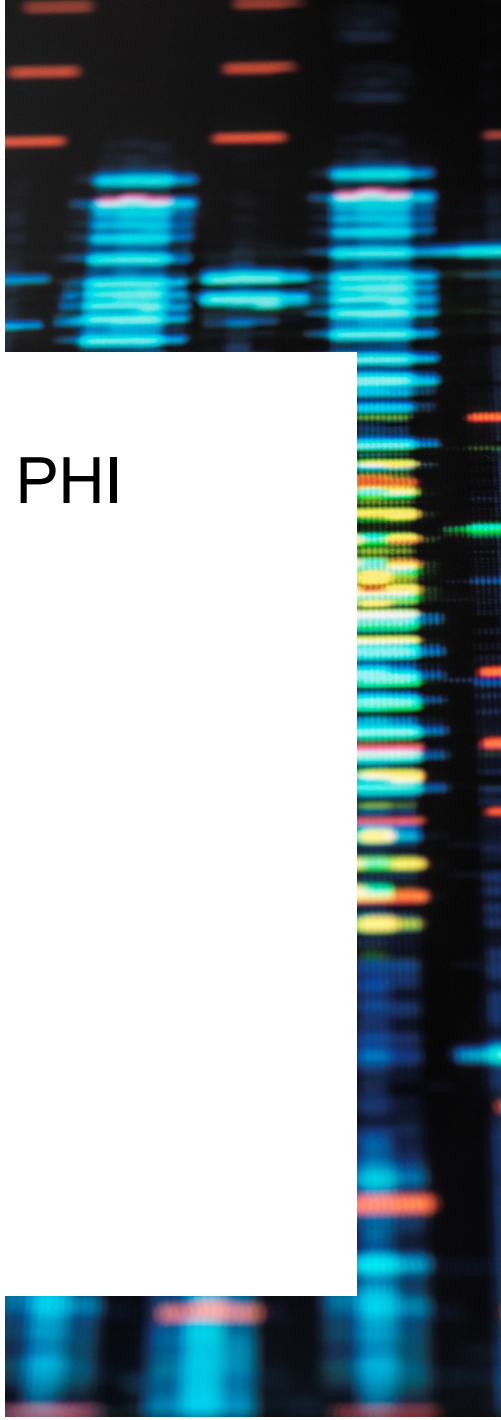
FOLEY & LARDNER LLP

PYA

# HIPAA Right of Access

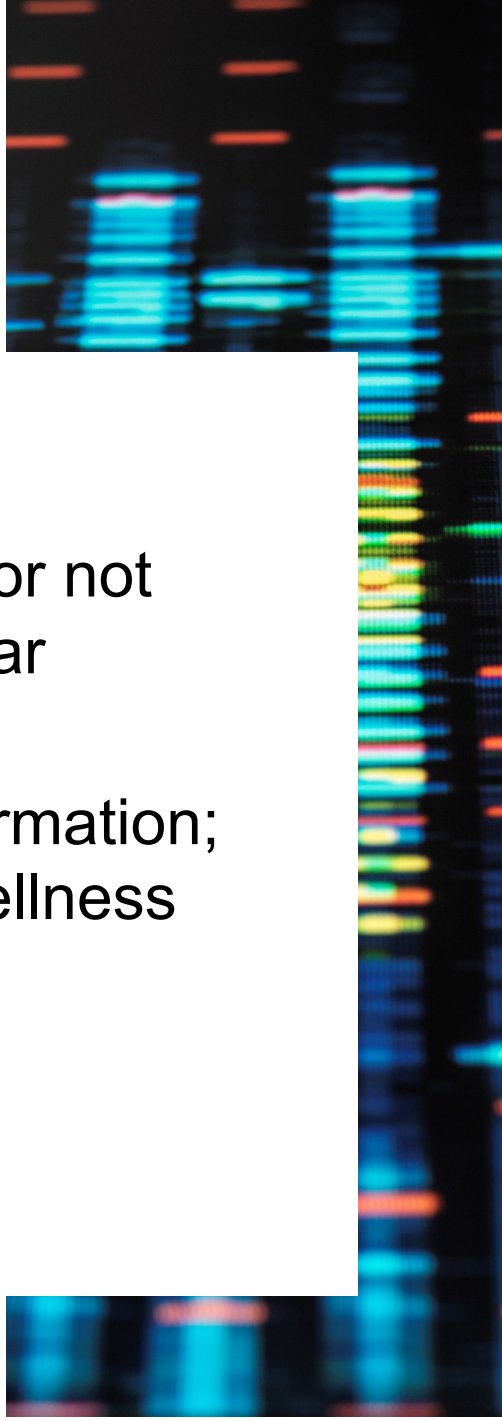
# HIPAA Right of Access

- 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 (HHS *proposing* to amend this to 15 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



# Designated Record Set

- Medical and billing records
- Other records used to make decisions about individuals, whether or not the records have been used to make a decision about the particular individual requesting access
- E.g., medical records; billing and payment records; insurance information; clinical laboratory test results; medical images, such as X-rays; wellness and disease management program files; and clinical case notes



# 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
- Prior to this initiative, this right was not enforced with any regularity
- Since the initiative’s announcement in 2019, HHS has settled 46 “right of access” investigations

# 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 that incudes up to 2 years of monitoring

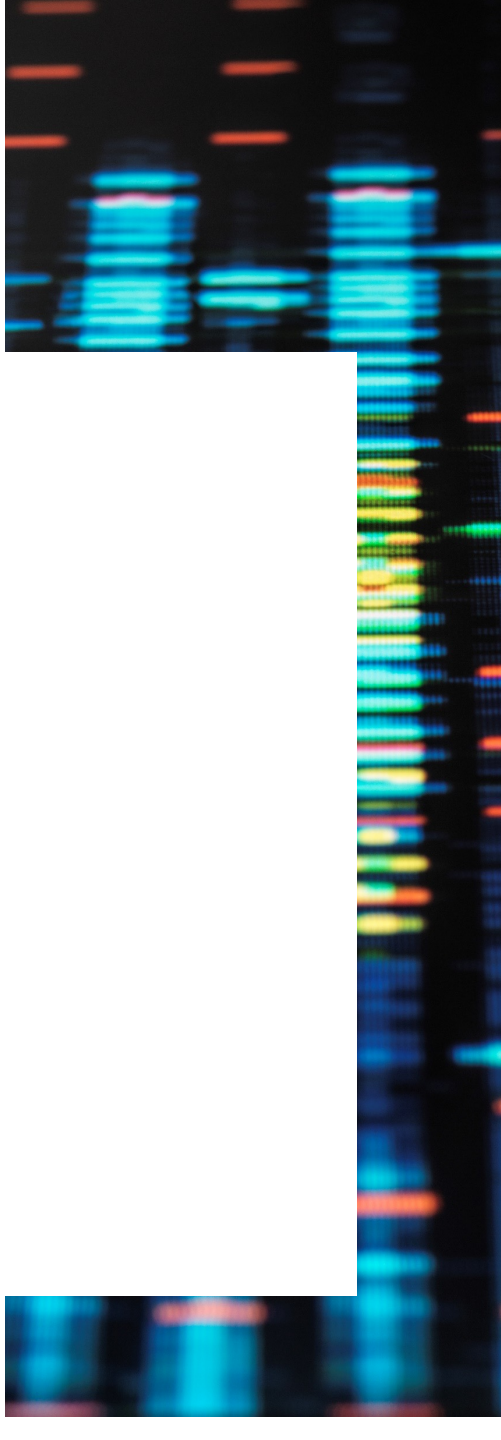
FOLEY & LARDNER LLP

PYA

# Trends in HHS Investigations

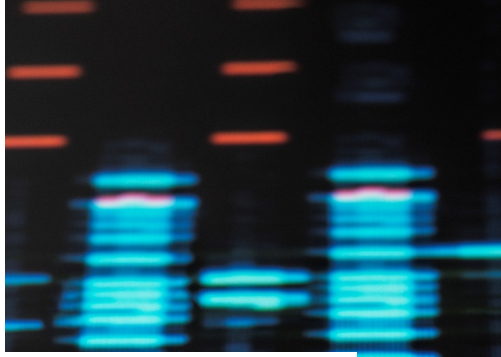
# Incidents Leading to Settlements

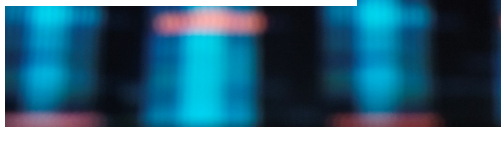
- Cyber issues
- Disclosure to news reporter
- Responding to online reviews
- Snooping



# Takeways

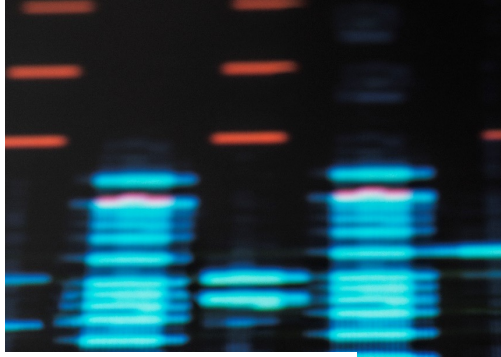
- Conduct a security risk analysis of the potential risks and vulnerabilities to electronic protected health information and update it regularly.
- Ensure privacy and security policies address HIPAA's requirements.
- Implement security procedures to comply with HIPAA Security Rule and other cybersecurity frameworks (e.g., review information system activity).
- Train workforce members on cybersecurity and HIPAA policies and procedures.

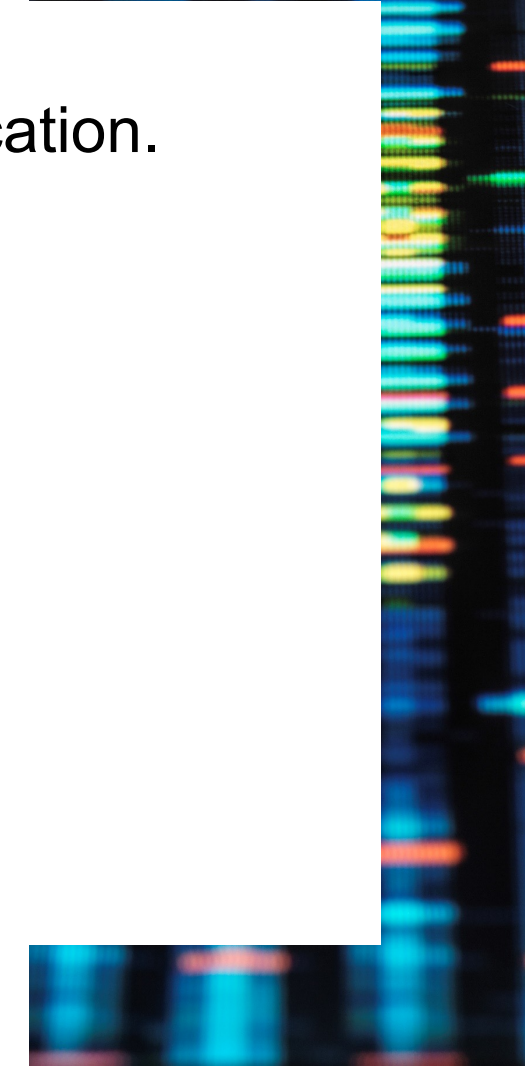




# Additional Recommendations

- Implement strong security controls such as Multi Factor Authentication.
- Keep systems updated.
- Develop and test cyber incident response scenarios.





# Contacts

**Jennifer Hennessy**
Foley & Lardner LLP
Partner | Madison

**T: 608.250.7420**
**E: jhennessy@foley.com**

**Barry Mathis**
PYA, P.C.
Principal | Knoxville

**T: 423-827-7893**
**E:bmathis@pyapc.com**

# About Foley

Foley & Lardner LLP is a preeminent law firm that stands at the nexus of the Energy, Health Care & Life Sciences, Innovative Technology, 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 40 years, PYA, a national professional services firm providing healthcare management consulting and accounting, has helped its clients navigate regulatory compliance. PYA's suite of compliance services includes developing and evaluating compliance programs and performing risk assessments, serving as an Independent Review Organization, supporting providers undergoing investigations/payer audits, advising on reimbursement and revenue management, and providing fair market value compensation opinions. Serving clients in all 50 states from offices in seven cities, PYA is consistently ranked by Modern Healthcare as one of the Top 20 healthcare consulting firms in the U.S. and by INSIDE Public Accounting as one of the nation's “Top 100” Largest Accounting Firms.

**PYAPC.COM**

FOLEY
FOLEY & LARDNER LLP

PYA