FOLEY HOAG

Robotics and Health Information:

Navigating Clinical Deployments in Light of Current Trends in Health Information Privacy and Security

MassRobotics Healthcare Catalyst Program

March 5, 2026

The information provided in this document is not intended to be legal advice, but is provided for general information purposes only.

Depending on when and where you are reading it, it may not constitute the most up-to-date legal or other information and it may not be applicable to your particular situation.

Colin Zick

Partner and Co-Chair, Health Care Compliance and Privacy & Data Security Practice Groups

BOSTON

+1.617.832.1275

czick@foleyhoag.com

- Counsels clients ranging from the Fortune 1000 to start-ups on issues involving information privacy and security, including state, federal and international data privacy and security laws and government enforcement actions.
- Advises on issues involving the transfer of data between jurisdictions, including HIPAA, GDPR, CCPA, CPRA, and other data privacy and security laws, data breach response, cloud security, and cyber insurance.
- Co-founded the firm's Privacy and Data Security Group (which he currently co-chairs) and regularly contributes to its "Security, Privacy and the Law" blog, www.securityprivacyandthelaw.com.
- Selected by his peers for inclusion in THE BEST LAWYERS IN AMERICA in the fields of Privacy and Data Security (2018-present) and Healthcare Law (2015-present)
- Ranked by CHAMBERS USA: AMERICA'S LEADING LAWYERS FOR BUSINESS as one of Massachusetts' leading Healthcare attorneys (2010-present)

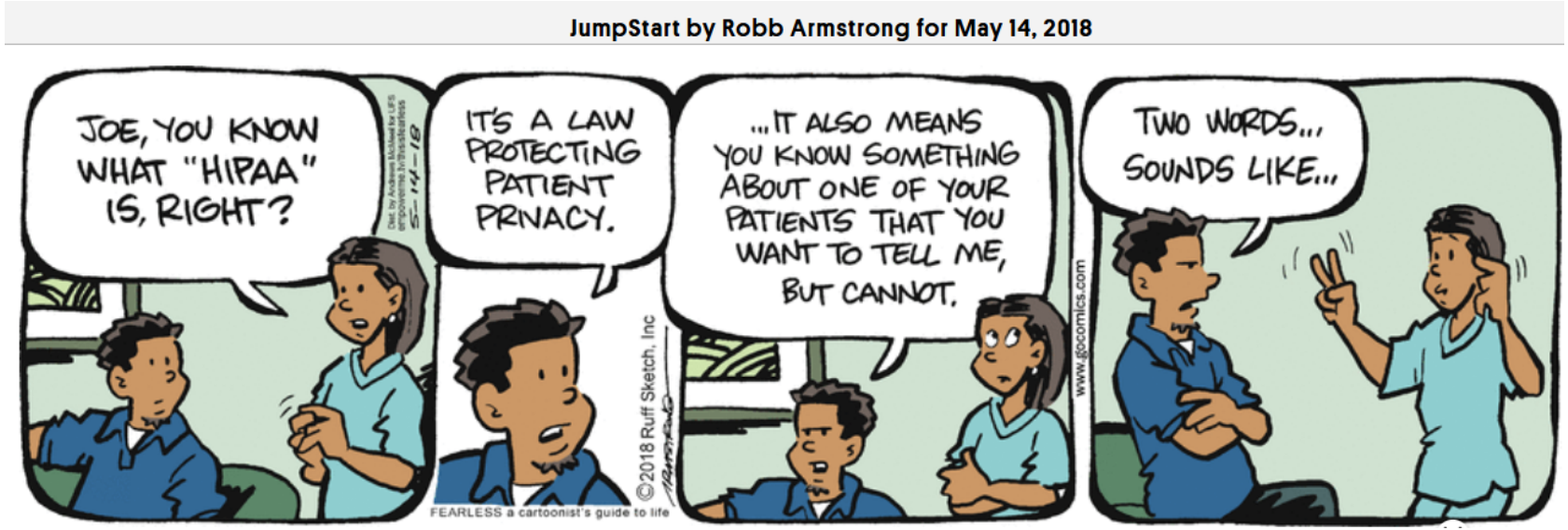
Privacy and Data Security Overview

- The overall regulatory environment is an overlay of federal, state, local and ex-U.S. laws
  - Enforced by governmental agencies and individuals exercising private rights of action
  - Privacy and security laws increasingly touch on AI, and vice versa
- Privacy
  - Laws around obligations concerning personal information
  - Legal definitions around personal information are broad and categorize data based on risk
  - Increasing concerns in privacy laws around biometric information
- Security
  - Laws and practices concerning technical, physical, and other means of securing data
  - Relevant to protecting personal information
  - Not exclusive to personal information

Health Information Risks Relating to Robotics

- Data collection
  - Collecting large volumes of health information can create legal and security risks
  - Automatic and inadvertent captures of sensitive health information and create tension with laws concerning biometrics and consent
- Methods of collection
  - Intentional
  - Unintentional or incidental
- Security against compromises and breaches
  - Large data sets have great value and therefore are a target for hackers
  - Non-PHI but commercially sensitive data also an attractive target
- Cross-border/international transfers
  - Complex rules around data transfers, especially with EU

“You Know What ‘HIPAA’ Is, Right?”



What is HIPAA?

- The Health Insurance Portability and Accountability Act of 1996 –HIPAA
- It is designed to protect and insure the privacy of sensitive medical information
- HHS's Office for Civil Rights ("OCR") has responsibility for implementing and enforcing the Privacy Rule with respect to voluntary compliance activities and civil money penalties.
- A major goal of the Privacy Rule is to assure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well being.

HIPAA History

- HIPAA was an attempt by Congress to improve efficiency in healthcare, eliminate wastage, combat fraud, and ensure that health information that can be tied to an individual and would allow them to be identified is protected and kept private and confidential.
- HIPAA introduced a set of new standards for healthcare organizations to follow to ensure everyone was singing from the same hymn sheet. Standard codes and identifiers were created to make it easier for health information exchange and healthcare providers, health insurers, and their business associates were required to use the same codes for electronic transactions to ensure data could be exchanged efficiently. This saved a great deal of time, effort, and resulted in substantial cost savings.

HIPAA Considerations for AI Software Use and Development

- In the context of HIPAA, healthcare data, and AI technologies, AI developers and vendors should consider that HIPAA only provides a federal floor of privacy and security standards.
- Often, other state and federal laws can apply that pre-empt HIPAA – particularly with regard to healthcare adjacent data – or apply to more organizations than Covered Entities and Business Associates.
- Check the FTC guidance.
- Review the Government Accountability Office's report entitled "Artificial Intelligence in Healthcare" which discusses the benefits and challenges of AI technologies for medical diagnoses and provides some pointers for future federal legislation.
- NIST AI Standards are a useful reference.
- State health privacy laws also impact the use of health information for AI.

What are HIPAA Business Associates?

- A HIPAA “business associate” is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.
- A member of the covered entity’s workforce is not a business associate.
- A covered health care provider, health plan, or health care clearinghouse can be a business associate of another covered entity.
- Business associate functions and activities include: claims processing or administration; data analysis, processing or administration; utilization review; quality assurance; billing; benefit management; practice management; and repricing.
- Business associate services are: legal; actuarial; accounting; consulting; data aggregation; management; administrative; accreditation; and financial.

Health Information and the Post-COVID World

HIPAA has not changed:

- Telehealth was allowed to prosper because HIPAA was *not* enforced
- Self-testing is not necessarily covered by HIPAA
- Personal device data is not necessarily covered by HIPAA
- De-identified data feeding AI is not covered by HIPAA
- Preventative and collaborative care tests the boundaries of HIPAA concepts of “treatment, payment, and health care operations”

Examples of Non-HIPAA Legal Frameworks

- California (CCPA/CPRA)
  - Most restrictive comprehensive privacy law
  - Broad definition of personal information
  - Notice, consent, and contract
- Illinois (BIPA)
  - Most restrictive law concerning biometric collection
  - High potential for liability
- Europe/EU (GDPR, EU AI Act)
  - GDPR - Gold standard privacy law, comprehensive regulatory scheme and well enforced
  - EU AI Act – Categorizes AI uses based on risk for multiple players in the market
- Consumer Protection Laws
  - Enforced by FTC and AG's offices
  - Focuses on representations, unfair/deceptive acts and practices
- Ordinary tort laws

The iRobot Bankruptcy: Lessons in Consumer Information Privacy

Background

- iRobot filed Chapter 11 bankruptcy in December 2025 in the U.S. Bankruptcy Court for the District of Delaware
- Shenzhen Picea Robotics (Chinese manufacturer and creditor) will acquire 100% of iRobot's equity
- Bankruptcy plan approved by court in January 2026, but transaction still requires CFIUS clearance

The iRobot Bankruptcy: Types of Sensitive Data Collected by Roomba Devices

Data Category	Details
Home Mapping Data	Detailed floor plans, room layouts, dimensions, and spatial data
Visual/Camera Data	Onboard cameras capture obstacle images; some models record video
Usage Patterns	Cleaning schedules, occupancy indicators (when users are away)
Wi-Fi/Network Info	Network credentials, signal strength, connected devices
Account Information	Name, email, billing, and device registration data

Data Security Issues in the iRobot Bankruptcy

National Security & Regulatory Concerns

- **CFIUS Review Triggered**: DOJ filed notice that transaction may pose national security risks
- **Bipartisan Congressional Scrutiny**: Reps. Torres (D-NY) and Nunn (R-IA) demanded immediate CFIUS review, citing risk of sensitive U.S. data flowing to a PRC-linked entity
- **Chinese Data Access Laws**: Under PRC law, government can demand unlimited access to corporate databases—privacy pledges could be nullified
- **Bankruptcy Does Not Immunize Data Transfers**: CFIUS authority extends to technologies collecting sensitive personal or geospatial data at scale

Data Protection Measures Announced

- iRobot created "**iRobot Safe**"—a U.S.-governed spin-off entity to serve as data custodian
- U.S. and European customer data stored in U.S.-based servers
- CEO assurances: "No data will leave the U.S."
- FTC has signaled it will hold companies accountable for privacy promises made during bankruptcy (citing 23andMe precedent)

Specific Compliance Requirements to Incorporate into Robotics

- Lawful processing
- Data minimization
- Notice and consent
- Individual privacy rights
- Internal governance
- Third party contracting and risk management
- Industry standard security

Ways to Meet Data Compliance Obligations

- Privacy by design (and default)
  - Integrate privacy into the design stage; create features the prioritize privacy
- Encryption and secure storage
  - Basic cyber hygiene
- Transparent data policies
  - Clearly articulate **what** you collect, **why**, **when**, and **how;** tell users **where** the information goes; and with **whom** it is shared
- Regular security audits
  - At least annual third-party auditing of cybersecurity
- Monitor changes to privacy laws
- Consider AI a regulated space
  - Law enforcement will use consumer protection, privacy laws, and tort laws to regulate AI even without specific statutes

FOLEY HOAG

QUESTIONS?

Colin J. Zick, Esq.
Chair, Healthcare Compliance Practice Group
Co-Chair, Privacy and Data Security Practice Group
Foley Hoag LLP
155 Seaport Boulevard
Boston, MA 02210

(617) 832-1275
czick@foleyhoag.com
https://foleyhoag.com/people/zick-colin/
https://www.linkedin.com/in/colinzick/