



# ***Cybersecurity in Medicine***

## ***It All Started with HIPAA***

**By**

**Sheila Mints, Esq.**  
**smints@capehart.com**  
**856.840.4945**

**October 11, 2023**

# *HIPAA PRIMER*

---

# HIPAA Privacy

---

- Enacted in 1996
- Applies to all forms of Protected Health Information (PHI)
- Requires safeguards be in place
  - Administrative
  - Physical
  - Technical



# What is Protected Health Information (PHI)?

---

- Protected Health Information (PHI) is individually identifiable health information that is:
  - Created or received by a health care provider, health plan, employer, or health care clearinghouse and relates to:
    - The past, present, or future physical or mental health or condition of an individual
    - The provision of health care to an individual
    - The past, present or future payment for the provision of health care to an individual

# What are Patient Identifiers?

---

- PHI includes information by which the identity of a patient can be determined with reasonable accuracy and speed either directly or by reference to other publicly available information



# Covered Entities under HIPAA

---

- Physicians
- Hospitals
- Other Health Care Providers
- Health Plans
- Health Care Clearinghouses

# HIPAA IN 2023

---

- HIPAA was enacted in 1996, a time in which the health care industry maintained health records on paper.
- HITECH was enacted in 2009 to extend HIPAA to electronic data storage and communications
- HIPAA serves as the predominant federal law governing use, disclosure, and protection requirements for protected health information (PHI). HIPAA sets a federal floor for data protection.
- More and more health care technology companies are entering the marketplace in a way that does not subject them to HIPAA regulation

# *Expansion of the World of Business Associates*

---



# Business Associates under HIPAA

---

- Who is a Business Associate?
- What Must a Business Associate Do?
- What Happens if it Doesn't?
- Business Associate Contracts

# The New Business Associates

---

- Providers, payers, life science companies, digital health companies, wearable tech companies, telehealth companies, diagnostic companies, laboratories, and a cornucopia of other entities generate an ever-growing pool of data.
- In 2014, estimates indicated that the volume of health care data would grow from approximately 153 exabytes produced in 2013 to an estimated 2,314 exabytes produced in 2020.
- Other experts estimate that in the year 2025 there will be 500 times more health care data than in the year 2012.

# Value Based Care/Meaningful Use

---

- CMS “Meaningful Use Program” (now called the Promoting Interoperability Program) incentivized providers to adopt EHR systems.
- The CMS Meaningful Use Program drove data proliferation further by creating opportunities for providers to utilize EHR data to showcase quality.
- CMS sought to shift payment paradigms from traditional fee-for-service to value-based reimbursement models.
- The goal of interoperability is to promote data access across the entire continuum of care, with the patient as the central focus.
- BUT interoperability further drives the proliferation and commercialization of health data. Third-party app developers collect data and leverage such patient data for various secondary commercial purposes

# Cybersecurity Threats Proliferate

---

- Since September 2023, 7 hospital systems have experienced data breaches involving patient data
- HIPAA data protection standards by which Covered Entities and Business Associates should operate are insufficient as cyber threats and data breach risks continue to rise
- 11 of the 20 largest recent data breaches occurred at the Business Associate level.
- Need for more robust diligence, contracting, and ongoing management of vendors that capture, process and/or host personal information.
- Breach risks multiply exponentially as data proliferates and moves between HIPAA-regulated to largely unregulated entities.

# More Cybersecurity Threats

---

- Three cybersecurity threats have strong potential to disrupt healthcare organizations:
- **Generative AI and large language models:** A growing number of healthcare leaders said they are concerned about the potential for unintentional breaches of patient data by internal teams who utilize large language models to enhance efficiency and scalability
- **Ransomware groups:** According to the FBI, ransomware attacks on the healthcare sector increased more than any other critical infrastructure sector in 2022, with healthcare accounting for 24 percent of all ransomware attacks.

**Software vendors and IoT exposure:** The healthcare industry is heavily reliant upon third-party vendors, and hackers often target these third parties as a way to breach into a company's data.

# Enforcement

---

# How are the HIPAA Regulations Enforced?

---

- **Patients.** Patients are knowledgeable about their privacy rights and will take action. Still no private cause of action for HIPAA breach
- **Office For Civil Rights (OCR).** The federal agency that enforces the privacy regulations providing guidance, monitoring compliance, auditing, investigating
- **Department of Justice (DOJ).** Federal agency involved in criminal privacy violations, assessing fines, penalties and imprisonment to offenders
- **State Attorney General.** Authorized to enforce HIPAA and state privacy rules

# Patchwork of Additional Legal Enforcement

---

- **Federal Trade Commission.** FTC's Breach Notification Rule requires vendors of personal health records and related entities to notify consumers following a breach involving unsecured information.
- The Health Breach Notification Rule requires certain businesses not covered by HIPAA to notify their customers and others if there is a breach of unsecured, individually identifiable electronic health information.
- The FTC Bureau of Consumer Protection enforces claims against companies that misrepresent uses and protections for consumer health data and has settled cases



# FDA Medical Device Regulation

---

- FDA will now require medical device makers to submit information about their cybersecurity efforts alongside applications for regulatory clearance of their devices. Enforcement began On October 1, 2023.
- The [new law](#) updates the Food, Drug and Cosmetic Act to mandate that all regulatory submissions for medical devices include information regarding core cybersecurity requirements.
  - How they plan to track and address any cybersecurity vulnerabilities that may arise once their device is on the market.
  - Must include a “software bill of materials” in each of their FDA submissions, detailing every single software component included in a device.
  - Must “comply with such other requirements mandated by the FDA to ensure cybersecurity

# What Can a Physician Do?

---

# How to Protect Yourself

---


- Familiarize yourself with HIPAA requirements for physician
- Review your practice policies, consents and medical staff rules on data security
- Make sure your practice has data breach insurance to cover costs
- Ensure that contracts with Business Associates enforce HIPAA compliance

# Thank you.

**Sheila M. Mints, Esq.**

**Capehart & Scatchard, P.A.  
8000 Midlantic Dr., Ste 300S  
P.O. Box 5016  
Mt. Laurel, NJ 08054  
Phone - (856) 840-4945  
Fax - (856) 235-2786**



- 
- These materials reflect the views of the authors and not necessarily the views of Capehart Scatchard or the Firm's other attorneys and professionals.
  - These materials are for educational and informational purposes only. They are not intended to be a substitute for detailed research or the exercise of professional judgment. This information should not be construed as legal, tax, accounting or any other professional advice or service.