

# The Complexities of Managing Vendor Relationships: Practical Strategies for Navigating Data Breaches in the New Age of Data Privacy

June 30, 2025 3:15 PM

July 1, 2025 1:30 PM

## Kelly Pollock

Vice President Assistant  
General Counsel  
Novant Health

## Maria Salgado

Vice President  
Cornerstone Research

## Shalyn Watkins

Attorney  
Holland & Knight

1



1

## Presenters



### Maria Salgado

Vice President  
Cornerstone  
Research



### Kelly Pollock

Vice President  
Assistant General  
Counsel  
Novant Health



### Shalyn Watkins

Attorney  
Holland & Knight

2



2



## Objectives

- Explore legal requirements for preventing data breaches
- Discuss best practices for negotiating vendor contracts
- Explain pitfalls and lessons learned from vendor breaches


[americanhealthlaw.com](http://americanhealthlaw.com)

 AMERICAN HEALTH LAW ASSOCIATION

3

# Health Information and Data Privacy Summary

□ □ □ □ □

 AMERICAN HEALTH LAW ASSOCIATION

4



“I am convinced there are only two types of companies: those that have been hacked and those that will be.

~ Former FBI Director Robert Mueller in 2012:

5

## Health Insurance Portability and Accountability Act of 1996 (HIPAA)

### Privacy

Sets national standards for the protection of individually identifiable health information (IIHI).

### Security

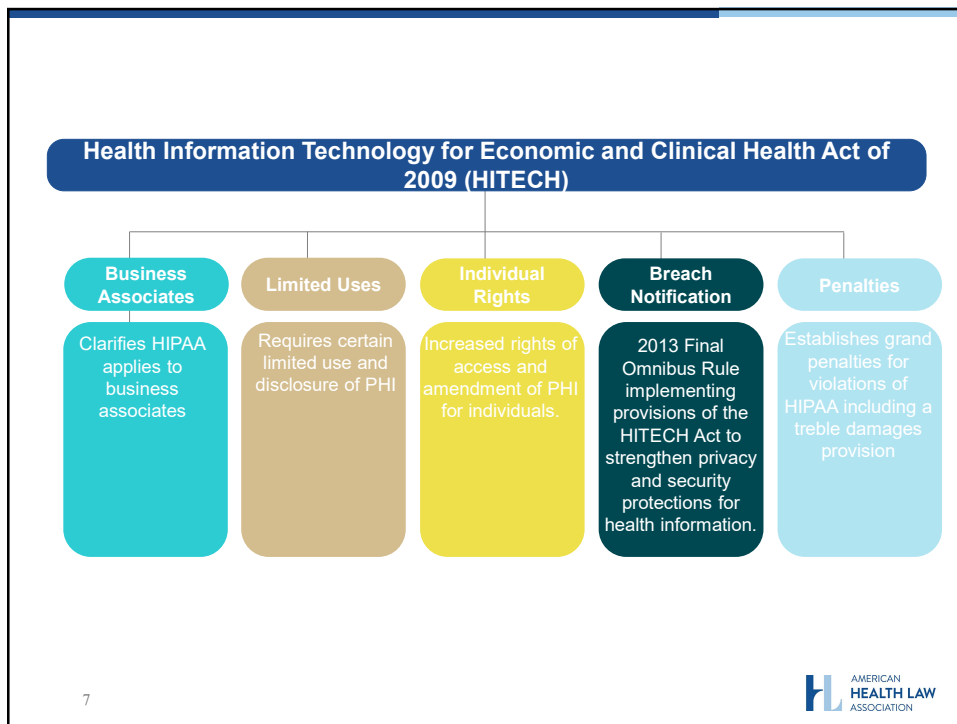
Sets national standards for protecting the confidentiality, integrity, and availability of electronic Protected Health Information (ePHI).

### Enforcement

Standards for the enforcement of all Administrative Simplification Rules.

6

6



7

## HIPAA “Business Associate”

45 CFR § 160.103

“Business Associate” means a person or entity who:

- Creates, receives, maintains, or transmits Protected Health Information (PHI) for the purpose of carrying out certain functions or activities for or on behalf of a Covered Entity; **or**
- Receives PHI from a Covered Entity (or a Business Associate on behalf of the Covered Entity) so that person or entity may provide legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for the Covered Entity.

8

AMERICAN HEALTH LAW ASSOCIATION

8

## HIPAA: IIHI and PHI Definitions

- Individually Identifiable Health Information (IIHI) is information:
  - Created or received by a health care provider, health plan, employer, or health care clearinghouse;
  - That relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
  - That identifies the individual or there is a reasonable basis to believe such information could be used to identify the individual.
- Protected Health Information (PHI) is IIHI that is transmitted by or maintained in electronic media or transmitted or maintained in any other form or medium.

9



9

## FTC Act Health Breach Notification Rule: Personal Health Record (PHR) Identifiable Health Information Definition

- PHR Identifiable Health Information = IIHI Definition + Information that is provided by or on behalf of an individual
- Examples include:
  - Browsing information;
  - Location information; and
  - Purchase information.

10



10

## But Wait... There's More

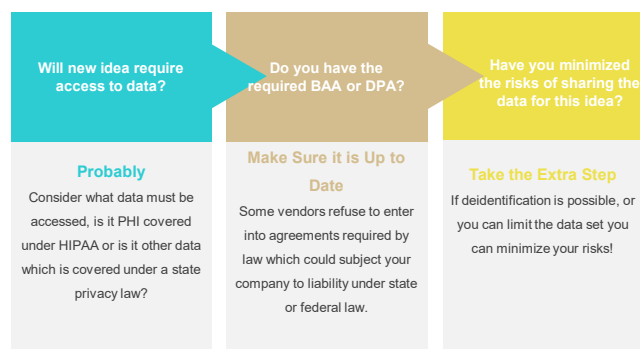
- Washington My Health My Data Act
- California Consumer Privacy Act
- Nevada SB 370
- Connecticut Data Privacy Act
- Maryland Online Data Privacy Act
- New York Health Information Privacy Act
- Colorado Privacy Act
- More to come...

11



11

## Understanding Health Data is Impacted



12



12

## Legal Risks – Unauthorized Use or Disclosure

- HIPAA
  - Breach presumed when there is an acquisition, access, use, or disclosure of PHI not permitted by the Privacy Rule
  - Covered Entity/Business Associate can overcome presumption by demonstrating low probability that the PHI has been compromised through a risk assessment
  - Breach treated as discovered on the first day on which such breach:
    - Is known to ICHI Covered Entity; or
    - By exercising reasonable diligence should have been known to the Covered Entity.

13



13

## Legal Risks – Unauthorized Use or Disclosure

- FTC Act Health Breach Notification Rule
  - Applies to:
    - Each vendor of personal health records, following the discovery of a breach of security of unsecured PHR identifiable health information that is in a personal health record maintained or offered by that vendor; and
    - Each PHR related entity, following the discovery of a breach of security of such information that is obtained through a product or service provided by that entity.

14



14

## Legal Risks – Unauthorized Use or Disclosure

- FTC Act Health Breach Notification Rule
  - “Breach of security” means, with respect to unsecured PHR identifiable health information of an individual in a personal health record, acquisition of such information **without the authorization** of the individual.
  - “Unauthorized acquisition” presumed to include **unauthorized access** to **unsecured** PHR identifiable health information
  - Breach of security includes unauthorized acquisition as a result of a data breach or **unauthorized disclosure**.

15



15

## BAA Requirements

45 CFR 164.504(e), a BAA between a covered entity and a business associate must:

- establish the permitted and required uses and disclosures of protected health information (PHI) by the business associate
- provide that the business associate will not use or further disclose the information other than as permitted or required by the contract or law
- require the business associate to implement appropriate safeguards to prevent unauthorized use or disclosure of the information, including implementing requirements of the HIPAA Security Rule with regard to electronic PHI
- require the business associate to report to the covered entity any use or disclosure of the information not provided for by its contract, including incidents that constitute breaches of unsecured PHI
- require the business associate to disclose PHI as specified in its contract to satisfy a covered entity's obligation with respect to individuals' requests for copies of their PHI, as well as make available PHI for amendments (and incorporate any amendments, if required) and accountings

16



16



## BAA Requirements (cont.)

- to the extent the business associate is to carry out a covered entity's obligation under the Privacy Rule, require the business associate to comply with the requirements applicable to the obligation
- require the business associate to make available to HHS its internal practices, books and records relating to the use and disclosure of PHI received from, or created or received by the business associate on behalf of, the covered entity for purposes of HHS determining the covered entity's compliance with the HIPAA Privacy Rule
- at termination of the contract, if feasible, require the business associate to return or destroy all PHI received from, or created or received by the business associate on behalf of, the covered entity
- require the business associate to ensure that any subcontractors it may engage on its behalf that will have access to PHI agree to the same restrictions and conditions that apply to the business associate with respect to such information
- authorize termination of the contract by the covered entity if the business associate violates a material term of the contract; contracts between business associates and business associates that are subcontractors are subject to these same requirements

17



17

## Vendor Agreements

- Form documents
- Sometimes out of date
- Not always reflective of full scope of relationship between the parties
- Typically drafted to benefit vendor

18



18

## Considerations for Vendor Negotiations

- Breach reporting obligations
- Costs for breach reporting
- Timing and form for reporting security incidents
- Who makes the ultimate decision on whether a breach occurred?
- Limiting uses of information
- Restricting policies for use of data analytics and cookies
- Deidentification protocols

19



19

## Economic Impact of Data Breaches

□ □ □ □ □



20

## Financial Costs of Data Breaches

- The average cost of a data breach in 2024 was \$4.9 million (IBM Security's Data Breach Report 2024).
  - **The healthcare industry faces the highest data breach costs, averaging \$10.93 million.**
- Immediate costs of data breaches include breach notification costs and IT costs to address and prevent future breaches.
- Under HIPAA, fines range from \$50 to \$50,000 per record exposed, with a yearly cap of \$1.5 million.
- Operational disruptions occur when providers shut down systems, delay treatment, or modify patient care.
- Litigation costs can be significant.

21



21

## Plaintiffs Key Theories of Harm in Class Action Lawsuits

- Injury due to fraud or identity theft
- Monetary costs to identity theft monitoring
- Diminished value of breached PHI
- Time spent / loss of productivity to address the breach
- Loss of value of privacy
- Overpayment for Defendants' products and services
- Unjust enrichment

22



22

## Potential Economic Defenses

- Whether fraud or identity theft leads to harm depends on whether exfiltrated data can be used to conduct ID theft or fraud in the first place.
- Financial losses from fraud or identify theft can be small or zero.
- Difficult to establish causal link between any alleged data breach and fraudulent activity or identity theft.
  - There are thousands of data breaches in the U.S. and millions of compromised records.
- Monetary costs of identity theft monitoring may be limited.
- Value of breached PHI is limited as most people do not try to monetize their PHI.
- Value of privacy is often overstated and varies across individuals.
- Payment for Defendant's products and services depends on many factors.
- Assessing injury to putative class members requires individualized inquiry.

23



23

## Examples of Healthcare Data Breach Settlements and Fines

Year	Provider	Type of Settlement	Amount (millions USD)
2015	Anthem	Class Action Settlement	115
2018	Anthem	HIPAA Settlement	16
2020	Premera Blue Cross	HIPAA Settlement	6.85
2016	Advocate Health Care	HIPAA Settlement	5.5
2017	Memorial Healthcare	HIPAA Settlement	5.5
2025	Tampa General Hospital	Class Action Settlement	6.8
2025	Navvis and SSM Health	Class Action Settlement	6.5
2025	Robeson Health Care	Class Action Settlement	0.75
2024	Lehigh Valley Health	Class Action Settlement	65

24



24

# Application



25

## Recent Lessons Learned: Meta Pixel

- Meta Pixel was a piece of code that website embedded to track user activity such as page views, clicks, etc.
- Data sent to Meta who used it for targeted ad campaigns on its social media platforms.
- The Pixel was placed on health system websites (often by vendors/business associates who were engaged by the health system).
- Issues:
  - Lack of transparency
  - Lack of consent

26

## Lessons Learned: Meta Pixel

- **Office of Civil Rights Bulletin (Dec 2022) – Tracking Technologies:**

- Cookies and Pixels collect information from consumers that could be PHI.
- Relates to past, present or future health or healthcare or payment for healthcare.
- Even if not directly related to health care, can still be PHI.
- Disclosure by a vendor is considered a disclosure of PHI.

• **Northern District of Texas ruled for a vacatur (rather than a permanent injunction) against OCR around this guidance. The court left in place that the connection of an IP address activity on an authenticated website constitutes a disclosure.**

27



27

## Lessons Learned: Meta Pixel

- Meta Pixel was installed behind the authentication page of My Chart, as well as other Novant Health websites.
- Class action lawsuit of 158,000 patients who used My Chart portal between May 1, 2020 and August 12, 2022.
- OCR did not take adverse action against any of the health systems who inadvertently used Meta Pixels on websites and portals.
- How to make sure this did not happen again?

28



28

## Lessons Learned: Meta Pixel

### Vendor Contracting:

- Requiring a business associate agreements with marketing vendors
- Closer dialogue between marketing team and legal/privacy
- Definitive statements in agreements



### Data Governance:

- Stricter controls on what data leaves the organization and how
- Information Governance Steering Committee formed
- Third party risk assessments
- IT review of new technologies



29

29

## Lessons Learned: Recent Breaches

### Change Healthcare:

- Exposed data of 190 million people
- Cyberattack- ransomware
- Affected nearly 40% of all medical claims processed in the US
- Hackers are increasingly focusing on healthcare for attacks
- Cost \$2.5 billion

### Particle Health:

- Particle is a data exchange platform
- Epic claims Particle was sharing patient data for unrelated to treatment
- Particle countered that Epic leverages its market power to restrict access to patient data

30

30

## Best Practices



Make sure the clients understand the contract and the deliverable



Empower clients to work with the vendor directly on privacy issues



Consider a demo or meeting with the vendor with Legal and Privacy at the table

31



31

## Questions?

32



32





## Educating and Connecting the Health Law Community

[americanhealthlaw.org](http://americanhealthlaw.org)



33

## We Are AHLA

### Our Vision

A diverse health law community working to advance health care

### Our Mission

To deliver authoritative educational content and serve as a professional home for all who engage with health law

### Diversity and Inclusion

In principle and in practice, the American Health Law Association values and seeks to advance and promote diverse and inclusive participation within the Association regardless of gender, race, ethnicity, religion, age, sexual orientation, gender identity and expression, national origin, or disability. Guided by these values, the Association strongly encourages and embraces participation of diverse individuals as it leads health law to excellence through education, information, and dialogue.



34

© 2025 is published by the American Health Law Association. All rights reserved. No part of this publication may be reproduced in any form except by prior written permission from the publisher. Printed in the United States of America.

Any views or advice offered in this publication are those of its authors and should not be construed as the position of the American Health Law Association.

“This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is provided with the understanding that the publisher is not engaged in rendering legal or other professional services. If legal advice or other expert assistance is required, the services of a competent professional person should be sought”

—from a declaration of the American Bar Association.

