Newest Trends in Health Data Breaches: FTC, OCR, and AG Enforcement

May 26, 2021

D. Reed Freeman
Partner | T +1 202.344.4606 | rfreeman@Venable.com

Thora A. Johnson
Partner | T +1 410.244.7747 | tajohnson@Venable.com

Erik Jones
Partner | T +1 312.820.3411 | ecjones@Venable.com

James E. Nelson
Partner | T +1 415.653.3730 | jnelson@Venable.com

VENABLE LLP

Electronic Medical Records and Patient Access

- Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009
  - Billions invested by the federal government in health IT—a majority in the form of CMS incentive payments for the use of EHRs
  - Goal of improving healthcare quality, safety, and efficiency through the promotion of EHRs
- 21st Century Cures Act
  - Meant to improve the flow and exchange of EHI
  - Advancing interoperability and prohibiting information blocking
- Increasing patient access to medical records, plus the quantified self
- Combined with the COVID-19 Pandemic
- Has led to…

VENABLE LLP

Breach Landscape

- In 2020
  - Healthcare data breaches of 500 or more records were reported at a rate of more than 1.76 per day.
  - 642 large breaches reported by HIPAA-governed entities—a 25% increase from 2019.
  - Hacking/IT incidents accounted for 67% of data breaches

    * Healthcare Data Breach Report: 25% Increase in Breaches in 2020, *available at* https://www.hipaajournal.com/2020-healthcare-data-breach-report-us/ (last accessed May 23, 2021).

- Large uptick in ransomware and phishing
  - Blackbaud ransomware
  - Phishing emails "from" government regulators
  - Scams to gain access to stimulus checks

VENABLE LLP

The HIPAA Basics

- **Covered Entities**: (1) a health plan; (2) healthcare clearing house; or (3) healthcare provider that transmits health information in electronic form to another party to carry out financial or administrative activities related to healthcare.

- **Privacy Rule**: Most uses and disclosures of protected health information (PHI)—other than those for treatment, payment of treatment, and health care operations—must be authorized by the patient/Enrollee.

- **Security Rule**: Covered entities must "protect against reasonably anticipated threats and vulnerabilities" that compromise ePHI in ways that are not permitted by the Privacy Rule.

- **Breach Notification**: Obligation to assess incidents of unauthorized uses and disclosures of unsecured PHI to determine probability of compromise to the data and make notifications to individuals, government, or the media within 60 days when a breach has been discovered.

VENABLE LLP

HIPAA Penalties

Civil Penalties – Four-Tier System		
Level of Culpability	Penalty per Violation	Maximum Penalty Per Calendar Year for Identical Violations
Did Not Know and By Exercising Reasonable Diligence Would Not Have Known of Violation	$119—$59,522	$25,000
Reasonable Cause	$1,191—$59,522	$100,000
Willful Neglect and Corrected Within 30 Days	$11,904—$59,522	$250,000
Willful Neglect and Not Corrected Within 30 days	$59,522—$1,785,651(no maximum penalty)	$1,500,000

VENABLE LLP

2021 HIPAA Enforcement Actions

- Excellus Health Plan agreed to a $5.1 million CMP and CAP with OCR due to a malware attack that lasted from December 2013 to May 2015.
  - The names, addresses, birth dates, email addresses, social security numbers, bank account information, and claims information of 9.3 million individuals were exposed.
  - OCR stated that the health plan failed, among other things, to complete an enterprise-wide HIPAA security risk assessment.

- Enforcement actions this year have been under OCR's Right of Access Initiative
  - Focused on enforcing patients' rights of access to their own PHI and medical records in a timely, reasonable manner.
  - As of March 26, 2021, OCR settled its 18th enforcement action resulting from the Right of Access Initiative.

VENABLE LLP

New Days Ahead in HIPAA Enforcement?

- Litigation to watch
  - The University of Texas M.D. Anderson Cancer Center lawsuit.
  - Rejected resolution agreement with corrective action plan.
  - Instead, litigated the $4,348,000 CMP levied by OCR.
  - The Fifth Circuit Court of Appeals ruled in M.D. Anderson's favor, partially due to the government's arbitrary and capricious enforcement of the CMP rules against some but not other HIPAA-governed entities.*

* *Univ. of Tex. M.D. Anderson Cancer Center v. U.S. Dep't of Health and Human Serv.*, No. 19-60226, (5th Cir. Jan. 14, 2021).

- Legislation to watch
  - On January 5, 2021, Congress enacted Public Law 116–321 (the Act)
  - Under the Act, as part of its enforcement of the HIPAA Security Rule, OCR must now consider whether the entity under investigation has "recognized security practices" in place for at least the last 12 months.

VENABLE LLP

FTC: Overview of Authority

- The Federal Trade Commission ("FTC") has authority over businesses that collect health information under the FTC Act. This authority extends to some businesses that are *not* covered by HIPAA.
- The FTC Act prohibits unfair and deceptive acts and practices. As applied to health data, the FTC may bring enforcement actions against companies that make deceptive claims about the use or disclosure of health data, or engage in unfair practices, such as a failure to take reasonable security measures to protect health data.
- The FTC considers health data to be sensitive data.
  - "[Health] apps often ask for some of your most sensitive personal information, like your health history or medication list." – *Does your Health App Protect Your Sensitive Information?* (Jan. 2021 Blog Post)
  - "Commission staff believes that consumers should have transparency and choices over their sensitive health information, regardless of who collects it." *Internet of Things Report (2015)*
  - The "Commission agrees that [health information is] sensitive." *Privacy Report (2012)*

FTC: Health Breach Notification Rule

- **Scope:** The Rule applies to certain companies that handle personal health records ("PHRs").
  - **PHRs** are electronic records of individually identifiable health information on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual.
  - The Rule applies to **PHR-related entities**, which are non-traditional handlers of health information, such as mobile health apps, telehealth apps, and virtual health assistants.
    - The Rule *does not* apply to HIPAA-covered entities or entities that engage as business associates for HIPAA-covered entities.
- **Notification**: PHR-related entities must notify consumers in the event of an unauthorized acquisition of unsecured PHR information.
  - For breaches involving more than 500 individuals, the Rule requires notice to the FTC and, in some cases, the media.
- **Enforcement:** The FTC may enforce violations of the Rule as unfair or deceptive acts or practices in violation of the FTC Act.
  - The FTC can assess civil penalties of up to $43,792 per violation.

VENABLE LLP

FTC: Enforcement of the Health Breach Notification Rule

- Since 2009, only two companies have notified the FTC of a breach involving more than 500 individuals.
- To date, the FTC has not filed an enforcement action related to the Rule.
  - In March 2021, several members of Congress sent a letter to the FTC urging it to use the Rule to crack down on mobile health apps that share health information with third parties without user consent.
- In May 2020, the FTC sought comment on the Rule, including additional information about whether the Rule should be amended in light of technological advances, including the rise of health-related consumer technologies and services such as mobile health apps, virtual assistants, and platforms' health tools.
- While the FTC has not cited to the Rule in an enforcement action, the protection and use of health data is under increasing scrutiny by the FTC.
  - *Flo Health, Inc.* – Allegedly misrepresented the disclosure of consumer health data (Feb. 2021)
  - *SkyMed International, Inc.* – Alleged failure to take reasonable steps to secure sensitive information, including health records. (Feb. 2021)

VENABLE LLP

Enforcement in the States

Data Security and Data Breach Notification

VENABLE LLP

State Attorneys General: Overview of Authority

- State AGs have very ***broad consumer protection authority***.
- Enforcement authority is derived from Unfair and Deceptive Acts and Practices (UDAP), ***"reasonable" data security requirements***, and breach notification statutes.
- 22 state data breach notification statutes define personal information to ***include health or medical data***, combined with a first name/initial and last name of the individual:

State Breach Notification Laws that Include Health Information in PI Definition		
Alabama	Illinois	South Dakota
Arizona	Maryland	Texas
Arkansas	Missouri	Vermont
California	Montana	Virginia
Colorado	Nevada	Washington
Delaware	North Dakota	Wyoming
D.C.	Oregon	
Florida	Rhode Island	

VENABLE LLP

Data Breach Notification at the State Level

- **Different Definitions of a Breach Under State Laws**
  - **“Access” States**
  - **“Acquisition” States**

- **Timing for Notification to Individuals**

- **Notification to State Agencies**
  - Thresholds for Notifications
  - Process for Notifications
  - Publication of Notifications

VENABLE LLP

Recent State Attorney General Settlements

State Attorneys General Secure Settlement in First-Ever Multistate HIPAA Data Breach Lawsuit

Anthem Settles with 44 States for $40M Over 2014 Breach of 78.8M

The multi-state coalition of 44 states and Washington, DC reached a settlement of nearly $40 million with Anthem to resolve the 2014 healthcare data breach impacting 78.8 million patients.

The California Attorney General's Settlement with Glow: A Wake-Up Call for Consumer Health App Developers

States Reach $5M Settlement With CHS/Community Health Systems Over Data Breach

VENABLE LLP

Additional State Agencies

- **New York Department of Financial Services (NYDFS)**
  - NYDFS Cybersecurity Regulation adopted in 2017
  - Places cybersecurity requirements on “covered entities”
  - Must notify no later than 72 hours from a determination that a reportable “cybersecurity event” has occurred
  - Has recently settled two enforcement actions

- **Departments of Insurance**
  - NAIC Insurance Data Security Model Law

VENABLE LLP

Upcoming Health Tech Webinar Series Dates

Health Tech: The Marriage of Patient Apps, Price Transparency, and Payment Options

July 27, 1-2 p.m. ET

Health Information and the FTC and State Law Regimes

September 16, 1-2 p.m. ET

Use and Disclosure of Medical Data under HIPAA, Part 2, and the Interoperability Rules

October 26, 1-2 p.m. ET

VENABLE LLP

VENABLE LLP