Published on *The National Law Review* https://natlawreview.com

A New Decade of HIPAA – What Can We Expect?

Article By:

Sarah Beth S. Kuyers

Dianne J. Bourque

Ellen L. Janos

As the decade winds down, it's hard to believe that the HIPAA Privacy and Security Rules are almost twenty years old. It has been ten years since the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) published the first breach notification rule – the one based on the harm standard. And the Omnibus Rule's "low probability of compromise" standard is almost seven years old! Regulators and regulated entities are heading into the new year and decade with a lot of momentum on some important issues. As we prepare to welcome 2020, we'd like to indulge in a bit of hindsight – as well as speculation – about what the new decade might hold for HIPAA-regulated entities.

OCR Enforcement Will Continue to Be Increasingly Aggressive.

OCR enforcement has been increasingly aggressive over the past decade. We noted last year that 2018 was a record-setter for HIPAA fines, with the largest-ever fine of $16 million. Seven-figure fines are now the norm. The following are some notable examples:

- Sentara Hospitals (Sentara) paid $2.175 million just last month for failing to notify OCR after mailing documents containing about 500 patients' protected health information (PHI) to the wrong address. Sentara had argued and incorrectly concluded that only eight of the incorrect mailings contained PHI and constituted a reportable breach because the others did not contain information specifically about a patient's diagnosis, treatment, or other medical information. As a quick refresher, PHI not only includes information related to an individual's physical or mental health or condition but also information about the provision of health care and the payment of services for the provision of health care to an individual. OCR also found that Sentara did not have a business associate agreement in place with one of its business associates.

- Jackson Health System (JHS) paid $2.15 million for various HIPAA violations. JHS discovered that it had lost paper patient records of 756 patients and reported the breach to OCR; however, it later discovered that it had lost additional paper records and did not report

that breach until 3½ years afterward. JHS also inadvertently disclosed patient PHI in a photograph that was included in a media report and discovered that an employee was selling PHI. OCR found that JHS failed to provide timely and accurate breach notification, conduct an enterprise-wide risk analysis, appropriately manage identified risks, review activity records, and restrict authorization of employees' access to PHI to the minimum necessary.

- Texas Health and Human Services Commission (TX HHSC) paid $1.6 million after a software flaw resulted in the inadvertent exposure of PHI of over 6,000 individuals on the Internet. OCR found that TX HHSC did not conduct an enterprise-wide risk analysis and did not implement access and audit controls on its system, as required by HIPAA.

- Touchstone Medical Imaging paid $3 million after a server error allowed PHI of over 300,000 patients to be available on the Internet. We previously blogged about this settlement here.

There is nothing to suggest that this trend will abate.

Cyber Threats Aren't Going Anywhere.

It became clear over the past decade that covered entities are, and will likely remain, a high value target for cyber criminals. The health care industry is particularly vulnerable to ransomware attacks, or attacks involving malicious software that encrypts the files on a target's computer rendering them inaccessible unless and until a ransom is paid. (Although payment of ransom doesn't guarantee access to encrypted files.) In early 2016, Hollywood Presbyterian Medical Center paid $17,000 in bitcoin in response to a ransomware attack that encrypted its electronic medical records. That same year, OCR issued a Fact Sheet on HIPAA and Ransomware citing a 300% increase in the number of ransomware attacks since 2015. Toward the end of the decade, it seemed as though ransomware attacks were leveling off, but in October of 2019, the Federal Bureau of Investigation (FBI) warned health care organizations regarding the ongoing ransomware threat to the health care industry and other frequently targeted industries. The FBI's Public Service Announcement (PSA) indicated that ransomware attacks have become more targeted, sophisticated, and costly, with health care organizations remaining a high value target. FBI has observed the following techniques as of late:

- Email phishing campaigns in which the attacker sends an email containing a malicious file or link that deploys the malware when clicked by the recipient;

- Remote desktop protocol vulnerabilities, in which criminals use either brute force methods or credentials purchased on the dark web to gain unauthorized remote access to a victim's IT systems for the deployment of malware; and

- Software vulnerabilities or security weakness in widely used software, which cyber criminals can use to gain control of a victim's IT systems and deploy malware.

The PSA reminds healthcare and other organizations that regular, verified data backup is the best way for an organization to protect itself against the ransomware threat. Training is also critical to help employees avoid falling victim to phishing email messages, which will undoubtedly remain a threat into the next decade. The full PSA can be found here. We've continued to see health care organizations be subject to phishing and other hacking attempts.

GDPR/CCPA-Type Laws Are Proliferating. Will HIPAA Be Amended to Keep Up?

In May of 2018, the European Union's General Data Protection Regulation (GDPR) took effect. Shortly thereafter, in August of 2018, California passed its own sweeping data protection law, the California Consumer Privacy Act (CCPA). CCPA protects a very broad scope of "personal information" or "PI" beyond what is protected under GDPR and far beyond what is protected under HIPAA. CCPA grants GDPR-like rights to consumers, including the right to request disclosures of the types of personal information collected and the purpose of collection, the right to request deletion, and the right of access and to obtain copies of PI in a readily usable format for transfer to another entity. As the compliance date for the California Consumer Privacy Act (CCPA) looms near – the law is set to take effect on January 1, 2020 – several states have introduced similar consumer privacy laws, such as New York and Massachusetts. We've previously blogged about the complicated applicability of the CCPA to health care organizations. Importantly, health information that does not fall within HIPAA's definition of PHI and is not afforded the same protections as PHI is not exempt from the law, regardless of whether the organization is a covered entity under HIPAA.

As other states follow suit with their own consumer privacy laws, consumers and businesses will continue to struggle with an increasingly complex patchwork of laws regulating consumers' health and personal data. Now that it's been two decades after HIPAA was enacted, Congress may be ready to address the collection, use, and disclosure of health information that is not covered by HIPAA. Two bills, the Consumer Online Privacy Rights Act (COPRA) and the United States Consumer Data Privacy Act of 2019 (CDAP) are currently being considered by the Senate Commerce Committee. While they differ on preemption and individual private right of action, they both address in a comprehensive way how companies collect, share, and sell data, as well as the consumers' rights to access, delete, and move their data.

Health Information Is Everywhere and Often Held by Non-Covered Entities. Will HIPAA Be Extended?

Throughout the past decade, the multi-billion dollar mobile health industry has accumulated staggering amounts of consumer health and personal information through mobile health apps and devices, wearable fitness trackers, symptom-checker platforms, and web-based diet, exercise, sleep, medication management. Health information is everywhere, and HIPAA only applies to certain holders of health information that qualify as covered entities under the law. Will 2020 finally be the year when Congress enacts a comprehensive law that will take up where HIPAA left off? Given that mobile apps and wearables barely existed when HIPAA was enacted in 1996, it is no wonder that HIPAA was drafted to regulate entities like hospitals and physician practices and their vendors that hold health information, rather than the information itself.

In addition to the two bills detailed above, the Stop Marketing And Revealing The Wearables And Trackers Consumer Health (Smartwatch) Data Act, which specifically targets health information not covered by HIPAA, was introduced in the Senate in November. Unlike HIPAA, the Smartwatch Data Act applies to the information itself rather than the holder of the information. Under the Smartwatch Data Act, all health data collected through apps and wearable devices would be treated as PHI and violations would be enforced by OCR and the penalties for violation of the law would be keyed into the HIPAA penalties.

Whether a bill like the Smartwatch Data Act, COPRA, or CDAP moves forward in the coming year, Congress must ensure that the rules around the creation, storage, and use of health information are

clear to both consumers and businesses and that the rules dovetail seamlessly with HIPAA.

Business Associates Continue to Cause Some Significant Data Breaches. Will the Law Change to Shift More Burden to Them?

The end of the decade saw some significant data breaches caused by business associates (BAs). At the beginning of this year, Centerstone Insurance and Financial Services, operating as BenefitMall, announced that it had been hacked in October 2018 through a phishing attack resulting in over 111,000 consumers' data being potentially compromised. (BenefitMall offers HR, employee benefits, and employer services and acts as a business associate for many covered entities.) Over the summer, LabCorp announced that it received notice from American Medical Collection Agency (AMCA), a collection firm working on its behalf, regarding unauthorized access of 7.7 million patients' PHI stored by AMCA. You can read more about this breach here.

OCR released a guidance document on direct liability of BAs in May, which lists 10 HIPAA violations for which OCR can hold BAs directly liable. (See our prior blog post here for more information.) However, as BAs become more and more of the root cause of large data breaches, it is yet to be seen if the law will shift more burden onto BAs.

We're Still Waiting to See What OCR Is Going to Do with Its December 2018 RFI.

Last December, OCR released a Request for Information (RFI) in which it sought information from stakeholders on how HIPAA could be modified so that it does not impede the latest efforts for better coordinated care among health care providers. Specifically, the RFI requested comments on the following issues:

- Patients' right to access and obtain copies of their PHI and the timeframe for responding to those requests (which is currently 30 days);
- Removing the requirement to obtain written confirmation of receipt of an organization's notice of privacy practices;
- Promotion of parent and caregiver roles in care;
- Easing of restrictions on disclosures of PHI without authorization;
- Possible exceptions to the minimum necessary standard for disclosures of PHI;
- Changes to HITECH Act requirements for the accounting of disclosures of PHI for treatment, payment and healthcare operations;
- Encouragement of information sharing for treatment and care coordination;
- Changing the Privacy Rule to make sharing PHI with other providers mandatory rather than permissible;
- Expansion of healthcare clearinghouses' access to PHI; and
- Addressing the opioid crisis and serious mental illness.

While health care organizations provided comments to the RFI this year, it is yet to be seen what, if anything, OCR will do with them in the coming year.

As we look at the year (and decade!) ahead, there may be a lot of unknowns related to the future of HIPAA, but we have no doubt that the privacy and security of health information will continue to be a top priority for patients, consumers, businesses, and regulators.

National Law Review, Volumess IX, Number 357