Bloomberg BNA

BNA's Health Law Reporter™

Privacy and Security Enforcement—Trends, Lessons Learned in 2017 and Forecast for 2018



By George B. Breen, Adam C. Solander, and Wenxi Li

George B. Breen is Chair of Epstein Becker & Green PC's National Health Care and Life Sciences Practice Steering Committee and is a Member of the Firm in the Health Care and Life Sciences and Litigation practices in the firm's Washington office. He can be reached at gbreen@ebglaw.com or (202) 861-1823.

Adam C. Solander is a Member of the Firm in the Health Care and Life Sciences practice in the firm's Washington office. He can be reached at asolander@ebglaw.com or (202) 861-1884.

Wenxi Li is an Associate in the Health Care and Life Sciences practice in the firm's Washington office. She can be reached at wli@ebglaw.com or (202) 861-1831.

Introduction

Data and privacy breach issues continued to be in the national spotlight in 2017. For example, in May 2017, eClinicalWorks, an electronic health records (EHR) vendor, agreed to pay a $155 million to resolve a False Claims Act case alleging fraud and kickback charges associated with the accuracy and truthfulness of its EHR certifications. In September 2017, more than 145 million Americans potentially had their Social Security and driver's license numbers exposed in connection with a data breach suffered by Equifax, a major consumer credit-reporting agency. Uber revealed in November 2017 that hackers stole 57 million driver and rider accounts; Uber paid the hackers a $100,000 ransom to keep the breach a secret from government authorities and affected individuals for over a year.

Moreover, the Department of Health and Human Services Office for Civil Rights (OCR) remained vigilant in enforcing the Health Insurance Portability and Accountability Act (HIPAA). Roger Severino, the newly appointed OCR Director under President Trump, oversaw the collection of just under $20 million in HIPAA settlements and penalties in 2017. While 2017's fines fell short of the more than $23 million the OCR collected in 2016, covered entities and business associates under HIPAA should not think the OCR will halt its enforcement efforts in 2018 and must not be lulled into complacency.

The number of high-profile information security and enforcement actions in 2017, as well as lessons learned from how federal and state agencies handled breach and enforcement activities last year should inform the regulated community as to what it can expect in 2018.

Trends in 2017

The OCR's Renewed Focus on Data Breach Enforcement

The OCR's enforcement agenda has reflected its belief that the lack of timely action, whether in notifying individuals about the breach of their protected health information (PHI) or the failure to address and implement risk management plans, can expose entities to large civil monetary penalties. In January 2017, Presence Health settled with the OCR for $475,000 due to alleged untimely reporting of a breach of unsecured PHI. Significantly, this was the first time that the OCR fined a health-care entity for failing to report a breach to the OCR, affected individuals, or state media outlets without unreasonable delay and within sixty days of discovering the breach. In February 2017, the OCR issued a $3.2 million civil monetary penalty to Children's Medical Center of Dallas for failing, against recommendations provided by a third party, to implement risk management plans and deploy encryption on portable devices after the loss of an unencrypted, non-password protected Blackberry phone.

In March 2017, OCR Director Severino made the enforcement of data breaches one of his top goals. In fact, he listed data breaches as a top enforcement priority and a way to teach companies how to handle potential incidents, reporting that "the big, juicy [data breach] case is going to be my priority and the methods for [OCR] finding it." He has stayed true to his word. Not only did the OCR's settled cases number approach 2016 levels, the OCR settlements soared into the millions for HIPAA violations, even when no data was lost. Memorial Healthcare System (MHS), for example, settled and paid the OCR $5.5 million when the PHI of 115,143 individuals was accessed and distributed without authorization by MHS's employees through the unauthorized use of a former employee's login credentials. While MHS had an information security program in place and workforce members were trained on these policies, the nonprofit hospital allegedly failed to maintain audit controls, such as regularly reviewing and monitoring access, termination, or modification logs, as required under 45 C.F.R. § 164.308(a)(1)-(4).

We also learned in 2017 that filing for bankruptcy does not shield an entity from the OCR's enforcement reach. On December 18, 2017, 21st Century Oncology, Inc. (21CO), settled with the OCR for $2.3 million in lieu of potential civil monetary penalties as a result of a third-party attacker's unauthorized access to the patient information of 2,213,597 individuals. In May 2017, the OCR mandated and 21CO, despite filing for bankruptcy protection, agreed to a Corrective Action Plan that included creating a risk analysis and risk mitigation plan, revising and adding to 21CO's existing policies and procedures, training its workforce on HIPAA matters, maintaining business associate agreements with all vendors, and submitting an internal monitoring plan conducted by a third-party assessor on a scheduled basis.

New Guidance from the OCR

2017 also saw the OCR issue guidance to help companies understand and report breaches. The OCR's Fact Sheet explains that the OCR views any encryption of electronic protected health information (ePHI) by a third party as a result of a ransomware attack as a breach. Due to the increase of ransomware cases involving health information , the OCR issued a checklist for companies to follow regarding how to respond to ransomware attacks. In the checklist, the OCR requires entities to execute a mitigation and contingency plan, report the incident to other law enforcement agencies, and report the breach to the OCR no later than sixty days after discovery if more than 500 individuals are affected. While ransomware reporting obligations remain the same as other HIPAA breaches, this is the first time that the OCR has equated accessing but not acquiring personal information with HIPAA breach reporting obligations.

Increase in State-Initiated Breach Enforcement

States such as New York increased their focus on data privacy protection, consent, and notification requirements. For example, after Uber announced that it had concealed its 2016 data breach, the New York State Office of the Attorney General (NY-OAG) opened an investigation to further review the incident. The NY-OAG also reached several settlements with health and fitness application developers, such as Cardiio and Runtastic, which promote their ability to collect a person's heart rate data. The NY-OAG contended that these applications did not properly disclose that the personal health information collected and stored may not be protected by HIPAA, and that the aggregated data sent to third parties might be used to re-identify specific users. With more than 150,000 mobile applications on smartphone devices related to health, NY-OAG's interest may show a shift away from traditional Federal Trade Commission (FTC) regulation in favor of state actions in this ever-developing arena.

The Equifax and Uber breaches also resulted in some states beginning to vigilantly enforce state breach notification and reporting requirements for their residents. The California Office of the Attorney General (CA-OAG), for example, investigated and settled with Cottage Health, a hospital chain, in November 2017 for $2 million when patients' medical information was leaked online in two separate data breaches from 2011 to 2015. The two data breaches, which affected approximately 55,000 patients, allegedly revealed patients' sensitive information online when Cottage's information storage depository was connected to the Internet without encryption, passwords, firewall protections, and access control permission. CA-OAG found that Cottage's failure to have basic security safeguards, such as keeping software patched and up to date and maintaining sufficient perimeter security, needed to be corrected via mitigation plans.

Similarly, the Massachusetts Attorney General announced a consent judgment with Multi-State Billing Services, involving a $100,000 fine for losing a laptop containing unencrypted information of more than 2,600 Massachusetts children, including names, birth dates, Social Security numbers, and Medicaid identification numbers, for Medicaid claim and eligibility determination processing. Under the settlement, Multi-State must upgrade its security practice to include a formalized compliance plan, privacy and security training, and encryption across all portable devices.

Predications for 2018

Three major trends in federal and state enforcement efforts are anticipated in 2018.

Increased State Scrutiny for Litigation, Data Privacy Regulations, and Breach Reporting

State attorneys general are increasingly focused on data privacy regulations and litigation. This means entities should expect states to broadly read and apply their unfair and deceptive trade practice laws to address data privacy and breaches. Attorneys general are focused on protecting consumers from the risks associated with new technologies, and data privacy remains a central topic during attorney general conferences.

Entities should also continue to keep an eye out for stricter data security laws and new legislation. After the Equifax breach, in late October 2017, New York Attorney General Eric Schneiderman proposed tighter state data security laws through the Stop Hacks and Improve Electronic Data Security Act. This proposed legislation would require all companies that handle New Yorkers' information to adopt "reasonable administrative, technical, and physical protections for data," regardless of where the company is headquartered. Companies must report to the New York Attorney General any unauthorized disclosures of PHI. Failure to notify individuals or the state would result in a penalty of $5,000 per violation, or up to $20 per instance of failed notification, with an aggregate cap of $250,000. North Carolina has also proposed breach notification legislation entitled the Act to Strengthen Identity Theft Practices (ASITP) to help combat the 1,022 data breaches that North Carolina experienced in 2017. If ASITP passes, North Carolina companies would have to make all breach notifications within fifteen days following discovery of the data security incident, which would be the shortest deadline for breach notifications in the United States.

Whistleblowers and Privacy and Security

eClinicalWorks' multimillion-dollar settlement this year showed the industry what devastating effects a whistleblower can cause in monetary damages and individual officer and employee liability. For the first time, the federal government held an EHR vendor responsible for failing to meet federal patient data handling quality standards, such as failing to satisfy data portability and audit log requirements within their systems. This enforcement effort extended to company founders and even lower-level programmers. Since the Health Information Technology for Economic and Clinical Health Act provides for the establishment of a mechanism to distribute a percentage of any civil monetary penalty or monetary settlement collected to the "individual who is harmed by an act that constitutes an offense" under HIPAA, whistleblowers can bring any company within the healthcare delivery system into the jurisdiction of the FTC and False Claims Act. Entities and responsible employees should expect continuing scrutiny in 2018.

The Necessity for Operational Information Security Programs, Risk Assessments, and Encryption

With more than twenty years of experience enforcing HIPAA through settlements, penalties, and HIPAA audits, health-care entities should be aware that the OCR will not be satisfied with unimplemented, off-the-shelf policies when a breach or security incident occurs. Key takeaways that entities should focus on and implement in 2018 in an effort to try to avoid the OCR enforcement include:

- Information security systems must have formalized, written policies and procedures with designated privacy officers and security officers overseeing the compliance program. The OCR will still investigate and levy settlements against companies with unimplemented draft policies and procedures in place. In connection with its $2.5 million settlement with CardioNet in April 2017, the OCR contended that the company had security policies and procedures drafted, but the compliance documentation was not formalized and employees were not trained on them upon hire.

- All devices, and especially portable media such as laptops and mobile phones, must be encrypted when used for storing sensitive data. CardioNet's settlement was due to a lost, unencrypted laptop containing the ePHI of 1,291 individuals. All systems must be patched with updates, and systems that cannot be patched are not secure and should be retired.

- A regular risk assessment should be conducted on all sensitive data-containing systems so that an entity can understand what risks are acceptable and which ones must be addressed immediately.

An entity should understand the breach notification and reporting requirements for federal and state reporting if a data breach or security incident occurs. Depending on the state, these requirements could affect the entity in the state in which it operates as well as in the states where its consumers or patients reside.

Conclusion

As healthcare entities navigate the regulatory environment in 2018, OCR and state attorneys general will continue to focus on HIPAA compliance, breach notification, and portable device security. Organizations who undergo annual HIPAA audits, as well as regular risk assessments, will likely stay ahead of potential OCR penalties and enforcement actions.