THE
NATIONAL LAW REVIEW

Cybersecurity, Inside Jobs, Outside Jobs, and HIPAA

Thursday, March 14, 2019

Article By Vinay Bhupathy
Kenneth YoodDaniel R. Eliav
Sheppard, Mullin, Richter & Hampton LLP
Healthcare Law Blog

Communications, Media & Internet
Health Law & Managed Care
All Federal

According to a February 12, 2019 Press Release from Protenus, a developer of analytics for patient privacy monitoring and compliance, 15,085,302 patient records were breached in 2018 – a startling number made even more startling by the fact that the number of breached patient records in 2018 is three times greater than the number of records breached in 2017.

As evidenced by the Protenus data and information reported by the U.S. Department of Health and Human Services ("DHHS"), Office of Civil Rights ("OCR"), a growing number of these breaches relate to third-party hacking, ransomware, and related malware incidents (collectively, "Hacking/IT Incidents"). As such, the OCR data shines a bright light on the obvious difficulties that healthcare entities ("Covered Entities") covered by the security and confidentiality requirements applicable to protected health information ("PHI") under the Health Insurance Portability and Accountability Act of 1996 and 45 CFR Parts 160 and 164, as amended by the Health Information Technology for Economic and Clinical Health Act ("HITECH") (collectively referred to hereinafter as "HIPAA").

The following examines representative HIPAA settlements and rulings from 2018, and considers the 2018 breach statistics and the growing security risk associated with Hacking/IT Incidents.

Anthem ($16 million fine)

While the breach actually took place in January of 2015, the settlement agreement was inked in October of 2018. The breach was the result of cyber-attackers infiltrating Anthem's systems through spear phishing emails. Cyber-attackers stole the ePHI of almost 79 million individuals, including names, social security numbers, addresses, and dates of birth. This was the largest breach of information in history. In an October 15, 2018 DHHS Press Release, OCR Director Roger Severino is quoted as saying, "[t]he largest health data breach in U.S. history fully merits the largest HIPAA settlement in history." The $16 million paid by Anthem eclipses the previous high of $5.5 million.

University of Texas MD Anderson Cancer Center ($4.3 million)

As announced in a June 18, 2018 DHHS Press Release, the University of Texas MD Anderson Cancer Center ("MD Anderson") was required to pay $4,348,000 in penalties in what is the second summary judgment victory in OCR's history of HIPAA enforcement and the fifth largest amount ever awarded to OCR by an administrative law judge or secured in a settlement for HIPAA violations.

According to DHHS, the settlement was the result of three separate breach reports in 2012 and 2013 arising out of the theft of an unencrypted laptop and the loss of two unencrypted thumb-drives. The ePHI of more than 35,500 individuals was compromised, but it seems as if the core of the OCR's complaint (and subsequent fines) was that MD Anderson had adopted policies regarding the encryption of all devices as early as 2006, but failed to implement its own policies. Although MD Anderson argued that it was not required to encrypt the "research" data, the administrative law judge sided with the OCR and stated MD Anderson's "dilatory conduct is shocking."

Advanced Care Hospitalists PL ($500,000 fine)

Advanced Care Hospitalists ("ACH"), a Florida-based physicians' hospitalist group, agreed to settle a claim with OCR for $500,000 and the adoption of a "substantial corrective action plan." *See* December 4, 2018 DHHS Press

Release. Although the monetary penalty imposed against ACH is smaller in magnitude than the other incidents we discuss in this blogpost, ACH's missteps and OCR's findings make this a noteworthy enforcement action.

From November 2011 to June 2012, ACH hired an individual who represented himself to be a representative of Doctor's First Choice Billings, Inc. ("First Choice"); the individual provided the billing services using First Choice's name and website but allegedly without the knowledge or permission of the First Choice owner. Finally, as discovered by OCR in its investigation of the incident (*See*, below), ACH never entered into a business associate agreement with the individual providing medical billing services to ACH and ACH failed to adopt any policy requiring business associate agreements until April 2014.

On February 11, 2014, a local hospital notified ACH that patient information was viewable on the First Choice website, including name, date of birth and social security number. ACH immediately instructed First Choice to remove the offending PHI and, on April 11, 2014, ACH filed a breach notification report with OCR on April 11, 2014, stating that 400 individuals were affected; however, after further investigation, ACH filed a supplemental breach report stating that an additional 8,855 patients could have been affected.

OCR concluded that ACH was at fault for not taking steps to protect the information. Specifically, ACH (i) failed to put a Business Associate's Agreement in place; (ii) failed to conduct an enterprise-wide risk analysis; (iii) failed to implement security measures; (iv) failed to implement HIPAA compliant policies and procedures; and (v) failed to monitor or audit the vendor's compliance with HIPAA requirements.

The OCR's findings in this case highlight an important component of HIPAA compliance that is not often discussed in the OCR's breach-related press releases or settlement agreements. It is important for a Covered Entity to conduct due diligence on its business associates to ensure that they are legitimate businesses that have also implemented relevant HIPAA privacy, security and breach notification policies and procedures. Although it goes without saying, this case also highlights the need for a Covered Entity (and a business associate in relation to a downstream vendor) to enter into a written vendor agreement with each of its vendors, as well as written and signed business associate agreement when the vendor is providing services that require the vendor to receive, create, transmit, and/or maintain the Covered Entity's PHI.

Increase in Hacking/IT Incidents

As required by Section 13402(e)(4) of the HITECH Act, DHHS must post a list of breaches of unsecured PHI affecting 500 or more individuals. This list of breaches – which is posted electronically on the OCR Breach Portal – is commonly referred to as the "Wall of Shame."

Looking at the 2018 entries on the Wall of Shame, we see that six of the top ten reported breaches (by number of individuals affected) relate to Hacking/IT Incidents. As reported by the HIPAA Journal on February 13, 2019, the Protenus 2019 Breach Barometer reports that 44% of all 2018 tracked data breaches were caused by Hacking/IT Incidents. This is notable in that OCR data gathered over the last 10 years shows that, on an aggregated basis, 23% of all breaches relate Hacking/IT Incidents. Moreover, although more than half of all data/security breaches reported by the OCR over the last 10 years have been caused by individuals internal to the organizations at issue (i.e., "inside jobs"), there has been a growing number of breaches caused by third parties outside of such organizations (i.e., "outside jobs"). In fact, of these outside jobs, a growing number are now originating overseas. It goes without saying that this increase in Hacking/IT Incidents has been, and continues to be, significant.

2018 Lessons Learned: Best Practices for 2019

The growing number of Hacking/IT Incidents reported on the Wall of Shame makes it clear that Covered Entities need to focus their security and privacy efforts on strengthening their IT systems to withstand foreign and domestic attacks.

In keeping with our above observations, we recommend the following actions as a way to reinforce a Covered Entity's HIPAA compliance efforts in relation to the protection of electronic PHI from Hacking/IT Incidents:

- In light of OCR's findings in the ACH case, a Covered Entity is well advised to undertake significant due diligence on its business associates before entering into a vendor arrangement with a business associate. Moreover, since the activities of a Covered Entity's business associates inure to the betterment and detriment of the Covered Entity, a Covered Entity is well advised to not only have a HIPAA compliance program but to ensure that the compliance program includes policies and procedures that require relevant vendor agreements to include extensive audit rights for the Covered Entity to access and review vendor books and records for compliance with the Covered Entity's HIPAA-related policies and procedures. Moreover, the Covered Entity should make sure to exercise its audit rights on a regular basis.

- In order to ensure that its IT security systems are in compliance with industry best practices, a Covered

Entity should consider undertaking a review and analysis of its IT infrastructure against an existing healthcare industry cybersecurity framework – e.g., the Common Security Framework ("CSF") developed by the Health Information Trust Alliance ("HITRUST"). As noted in a February 2018 GAO report, "CRITICAL INFRASTRUCTURE PROTECTION: Additional Actions Are Essential for Assessing Cybersecurity Framework," DHHS officials have identified compliance with CSF requirements as a strong indication that a Covered Entity's cybersecurity program complies with Federal governmental standards (i.e., the National Institute of Standards and Technology's ("NIST") Framework for Improving Critical Infrastructure Cybersecurity) and meets health care industry best practices.

- Covered Entities should undertake a cybersecurity risk analysis on a regular basis to account for ongoing developments in cybersecurity technologies.
- Any consideration of changes to existing business lines or expansion into new business lines should be accompanied by a review of existing cybersecurity practices as they may apply to the changes and/or developments under consideration.
- Covered Entities are well advised to encrypt and otherwise protect all electronic forms of PHI. Key risk areas – e.g., mobile devices and thumb drives which are easily misplaced, and/or ancillary devices that routinely have minimal security protections (e.g., connected speakers) – should be subject to focused attention as part of any cybersecurity audit.
- Covered Entities should take specific action to ensure that any and all cybersecurity (or other) breaches are treated as opportunities to update policies and procedures relating to the Covered Entity's overall security management process.
- Covered Entities should review all vendor and contractor relationships to ensure that Business Associate Agreements are in place as appropriate and ensure that these agreements address the requirements of HIPAA (e.g., breach, security, and incident reporting obligations).

Source URL: https://www.natlawreview.com/article/cybersecurity-inside-jobs-outside-jobs-and-hipaa