CYBERSECURITY

THE NEW PROFESSIONAL RISK

PART 1 OF 4: CYBER CRIME AND THE VULNERABILITY OF THE HEALTHCARE INDUSTRY

Karen Painter Randall and Steven A. Kroll Connell Foley LLP

The cyber-attack on Sony Pictures Entertainment at the end of 2014 has brought cybersecurity to the forefront of mainstream media and pop culture. Although the data stolen from Sony included, among other things, embarrassing emails between Sony's top executives, other industries, including healthcare, took notice as no business is insulated from attacks and the harm that is caused. This includes damage to reputation and millions of dollars estimated to be incurred in first and third party claims as a result of a hacking incident. In the first of a four-part series touching on various professional, business and insurance sectors, this article will discuss cyber and privacy issues facing the healthcare industry in today's evolving technological climate.

CYBER THREATS TO THE HEALTHCARE INDUSTRY

The digitization of the healthcare industry has provided many benefits to both patients and doctors alike. However, the use of this new technology has also seen the development of new levels of risk and privacy issues. According to multiple reports, electronic data in the healthcare sector is among the most vulnerable. In fact, the Federal Bureau of Investigation ("FBI") recently issued a warning to healthcare organizations that their IT systems and medical devices were at risk for increased attacks from hackers due to lax cybersecurity standards and practices. The FBI cited a report from the SANS Institute, a non-profit organization that indicated healthcare security strategies as being deficient in preventing cyber threats that could expose confidential and sensitive patient data. It also referred to the annual Ponemon Institute report, which said that 63% of health organizations surveyed reported a data breach in the past two years at an average loss of $2.4 million per data breach. With digitized healthcare records, the creation of HealthCare.gov and the exchange of electronic protected health information ("ePHI") online, the healthcare industry, from small providers to pharmaceuticals, has become the perfect target for cyber criminals. In fact, health data appears to be much more valuable than credit card information to hackers who operate in the black market because the data can be used to facilitate identity theft, access bank accounts or obtain prescriptions for controlled substances.

WHAT IS HIPAA?

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and its implementing regulations provide federal protections for the privacy and security of PHI held by covered entities and their business associates. The responsibility for HIPAA oversight and enforcement efforts rests with the U.S. Department of Health & Human Services Office for Civil Rights ("HHS-OCR"). To fulfill this requirement, HHS-OCR published what are commonly known as the HIPAA Privacy Rule and the HIPAA Security Rule. The Privacy Rule, or Standards for Privacy of Individually Identifiable Health Information, establishes national standards for the protection of certain health information. The Security Standards for the Protection of Electronic Protected Health Information (the "Security Rule") establish a national set of security standards for protecting certain health information that is held or transferred in electronic form. The Security Rule operationalizes the protections contained in the Privacy Rule by addressing the technical and non-technical safeguards that organizations called "covered entities" must put in place to secure individuals' ePHI.

The Security Rule requires covered entities to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting ePHI. Specifically, covered entities must: (1) ensure the confidentiality, integrity, and availability of all ePHI they create, receive, maintain or transmit; (2) identify and protect against reasonably anticipated threats to the security or integrity of the information; (3) protect against reasonably anticipated, impermissible uses or disclosures; and (4) ensure compliance by their workforce. HHS-OCR recognizes that covered entities range from the smallest provider to the largest, multi-state health plan. Therefore, the Security Rule is flexible and scalable to allow covered entities to analyze their own needs and implement solutions appropriate for their specific environments. What is appropriate for a particular covered entity will depend on the nature of the covered entity's business, as well as the covered entity's size and resources.

HIPAA VIOLATIONS CAN BE SIGNIFICANT

In the wake of data breaches across the country, and with impermissible uses and disclosures of ePHI remaining at the top of HHS-OCR's list of most frequently investigated compliance issues, HIPAA has received a great deal of attention recently. While punitive measures are rare, it appears that HHS-OCR's enforcement activity is designed to send a message to covered entities that safety measures must be taken to protect ePHI.

On May 7, 2014, HHS-OCR announced a record $4.8 million settlement with New York Presbyterian Hospital and Columbia University stemming from a breach involving a data network shared by the two entities. The breach occurred in September 2010, when a Columbia physician attempted to deactivate a personally owned server and, while doing so, inadvertently made the medical information of 6,800 patients accessible via pubic internet search engines. Ultimately, HHS-OCR's investigation revealed that neither organization had conducted an accurate and thorough risk analysis, or developed a satisfactory risk management plan, which lead to the above settlement.

On January 2, 2013, HHS-OCR announced that the Hospice of North Idaho (HONI) agreed to pay $50,000 and enter into a Corrective Action Plan as part of a settlement involving a breach of unsecured ePHI. This was significant in that it was the first settlement by HHS-OCR involving a breach affecting less than 500 individuals. HONI had self-reported in February 2011 that an unencrypted laptop containing ePHI of 441 patients was stolen in June 2010. In response, an investigation into the breach indicated that HONI failed to conduct a risk analysis of the security of ePHI transmitted using portable devices, and failed to adopt or implement sufficient measures to ensure the confidentiality of ePHI transmitted using portable devices "to a reasonable and appropriate level." HIPAA requires that breaches of unsecured PHI affecting 500 or more individuals be reported to the Secretary of HHS and the media within 60 calendar days after discovery of a breach. However, the settlement with HONI sends the message to the healthcare industry that HHS-OCR is investigating even relatively smaller disclosed breaches of unsecured PHI to identify and penalize noncompliance with HIPAA. Moreover, it confirms HHS-OCR's lack of tolerance for the storage of ePHI on unencrypted portable devices.

PREVENTING A BREACH

On March 28, 2014, HHS-OCR released a free security risk assessment ("SRA") tool to help businesses comply with HIPAA. Specifically, the SRA tool is a software application that allows covered entities to conduct and document their risk assessment. Besides this software, healthcare organizations must not only put into place solid security policies, but enforce them. For example, a weak password, unlocked door, or unsecured USB port can all lead to serious security holes. Moreover, physical security at the healthcare data center level is mandatory. This means utilizing biometric scanners, locked racks, delegated sets of administrator duties and good security systems. Although this operational change may be costly, the alternative is the potential loss of hundreds of thousands of patient records. Furthermore, healthcare organizations must deploy proper security for their systems, which includes network scanners, virtual appliances and other technologies placed within the infrastructure to scan for anomalies or irregular behavior. These are just a few of the steps that must be taken in order to avoid being scrutinized by the HHS-OCR. Ultimately, a covered entity under HIPAA must be cognizant of the mandates of the Security Rule, but review and modify their security measures to continue protecting ePHI in a changing environment.

CONCLUSION

Recently, in January 2015, Anthem, the second-largest health insurance company in America, announced that a database containing personal information of approximately 80 million of its customers and employees had been hacked. Investigators were still looking into the extent of the incursion, though Anthem stated it was likely that "tens of millions" of records were stolen. Reportedly, while no credit card information was compromised, the breach exposed names, addresses, birthdates, Social Security numbers, email addresses and employment information of employees and customers of Anthem – including income. Moreover, to date, no medical information such as insurance claims or test results were targeted or obtained, thus, it does not appear that HIPAA will apply. Nevertheless, the Anthem incident has been reported as the largest health care breach to date.

According to industry executives, the data security threats facing the healthcare industry will only intensify in 2015 as cyber criminals believe hospitals and health systems are not taking necessary steps to protect its wealth of data including confidential personal and medical information, credit card information, demographic details and insurance beneficiary data. Last year, 164 PHI data breaches were reported to the HHS-OCR, according to the fifth annual Redspin data breach report. Approximately 9 million patient records were affected resulting in a 25% increase of PHI data breaches in 2013. Thus, the healthcare industry must heed the FBI's warnings and boost security measures or face continued serious consequences.

Karen Painter Randall is a Complex Litigation Partner with Connell Foley LLP in Roseland, NJ, and Co-Chair of the Firm's Cyber Security and Data Privacy and Professional Liability Practice Groups. She provides representation and advocacy services to professionals and businesses in a wide variety of complex litigation matters and is a veteran trial attorney in state and federal courts. Ms. Randall, a former Chair of USLAW's Professional Liability Group, is designated a Certified Civil Trial Attorney by the Supreme Court of New Jersey.

Steven A. Kroll is an Associate with Connell Foley LLP in Roseland, NJ. In addition to representing professionals in various areas, Mr. Kroll concentrates his practice in the areas of professional liability, general insurance litigation and employment law handling matters in both New Jersey and New York. Mr. Kroll received his J.D. from Rutgers-Newark School of Law in 2009, cum laude, and received the distinguished award of Order of the Coif.