Health Law Daily

Wolters Kluwer

SEPTEMBER 18, 2014

STRATEGIC PERSPECTIVES: Data breaches: Unsecured health information in the digital age

By Sarah E. Baumann, JD

Data breaches make good news. Headlines across the internet include figures involving hundreds of thousands, and in some cases, millions, of individuals whose protected health information (PHI) has suddenly been compromised and potentially made available to perfect strangers. Patients and providers and other data handlers are understandably concerned. What is causing the seeming increase in breaches and what can be done to avoid them? This Strategic Perspective will examine recent trends in data breaches and offer advice as to how providers can work to prevent them.

Breach Notification Requirements

Since 2009, as mandated by the Health Insurance Portability and Accountability Act (HIPAA) (P.L. 104-191), covered entities (CEs)—health plans, health care clearinghouses, and health care providers who transmit health information electronically in connection with certain transactions—have been required to notify individuals when their unsecured PHI has been breached. PHI is defined as individually identifiable health information that is transmitted or maintained in any form by a CE. Until 2013, however, CEs were not required to notify individuals of breaches unless they determined there was a significant risk of financial, reputational, or other harm to the individual.

The breach notification rules changed in 2013 with the publication of the HIPAA Omnibus final rule (78 FR 5566) in January 2013, which implemented provisions of statutory amendments contained in the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009 (ARRA) (P.L. 111-5). The rule made both CEs and their business associates (BAs) responsible for breach notification. Previously, CEs were not required to notify individuals of breaches when there was a low probability that PHI had been compromised. Once the Omnibus final rule breach notification provisions became effective on September 26, 2013, reporting became mandatory unless CEs and BAs could demonstrate a low probability that PHI was compromised (see *HIPAA privacy and security issues facing covered entities in 2014*, January 17, 2014). CEs and BAs must perform a risk assessment to determine the probability of compromise, including the nature and extent of the PHI involved, the unauthorized person or person who used the PHI or to whom the disclosure was made, whether the PHI actually was acquired or viewed, and the extent to which the risk to the PHI has been mitigated. CEs and BAs must also notify the HHS Secretary of the breach. For breaches involving fewer than 500 individuals, they may notify HHS on an annual basis; for breaches involving 500 individuals or more, they

must notify HHS at the same time that they make individual notification. In addition, they must notify the media of breaches involving 500 individuals or more.

Alisa Chestler, a shareholder at Baker Donelson, told Wolters Kluwer that the Omnibus final rule has changed the way that CEs prepare for potential breaches. "I think the real change is to actually have a breach notification plan in place." She notes, "Prior to HITECH we saw either no security plan in place or an off the shelf plan that had very little relevance to the operations. We are encountering that problem less and less."

Breaches

Although data breaches are occurring less, they remain a part of the health care landscape. Breaches result from a variety of actions ranging from mere negligence to criminal behavior and are the target of increased enforcement actions. The consequences for unprepared CEs and BAs and patients can be severe.

Types of breaches. The HHS Office of Civil Rights (OCR) tracks all reported data breaches and lists breaches affecting 500 or more individuals on its website. The OCR divides breaches into six types, including one catchall "other" category. The remaining categories are theft, unauthorized access/disclosure, loss, hacking/information technology (IT) incident, and improper disposal. Although most breaches are attributed to a single category, some involve more than one. Between September 26, 2013, the effective date of the Omnibus final rule, and September 13, 2014, there were 177 reported data breaches affecting at least 500 individuals. The leading cause of data breaches, by far, was theft. At 78 reports, the theft category included exactly twice as many reports as the next biggest category, unauthorized access/disclosure. The other, loss, and hacking/IT incident categories hovered together at a level of reports in the twenties, while only five breaches were attributed to improper disposal. Two particularly large breaches, both involving data for more than 700,000 individuals, involved thefts of information from laptops. The largest breach, which involved data for an astounding 4.5 million individuals, resulted from theft of data from a network server.

Trends. In June 2014, the OCR submitted its Annual Report to Congress on Breaches of Unsecured Health Information for calendar years 2011 and 2012. The report included, among other scenarios, incidents of theft of both desktop and laptop computers, loss of backup files, and the hacking of an unencrypted network server. In one notable instance, a CE discovered its files were corrupt and inaccessible and then received a ransom note asking for money in exchange for access to the files.

The Identity Theft Resource Center (ITRC) began tracking data breaches in various industries in 2005. In 2013, for the first time, the health care sector accounted for more breaches than the business sector, with 43.8 percent of all breaches attributed to health care. The ITRC suggests this increase in data breaches could be attributed to the mandatory reporting requirements. According to ITRC President and CEO Eva Velasquez, "This is significant because it demonstrates that regulations in this area have a powerful impact."

A Washington Post analysis notes that 944 breaches affecting 500 or more individuals have been reported since reporting requirements were first put in place, involving PHI from about 30.1 million people. A Ponemon Institute report based on interviews with personnel from 91 health organizations revealed that data breaches resulting from criminal attacks have risen by 100 percent since 2010. The report also indicates that employee negligence is the

biggest threat to security and notes that employees are increasingly using personal mobile devices. It suggests that unsecured laptops, smartphones, and other devices are contributing to the risk (see *Report indicates criminal attacks on health care systems rose 100 percent since 2010*, March 13, 2014).

In her practice, Chestler sees "the whole gamut – human error, snooping employees, malicious hackers, viruses . . . improper firewall management and the theft and loss of electronic media." She notes that her firm is increasingly faced with "bring your own device" queries to stave off potential threats. "For a while all we ever heard about were lost laptops, and while such losses are still occurring, they are not as disproportionate as other kinds of issues."

Newsworthy breaches. The largest post-Omnibus rule breach reported as of September 13, 2014, occurred at Community Health Systems (Community Health), a health system based in Franklin, Tennessee that operates 206 hospitals in 29 states. From April through June, a group of Chinese hackers known as APT 18 are believed to have used the Heartbleed bug to access the names, addresses, birth dates, telephone numbers, and Social Security numbers of patients who had been referred to or received services from affiliated physicians in the last five years. Theories abound as to why the hackers, who typically target valuable intellectual property, would seek personal records information. The health system announced the breach on August 18th. Noting that the breach was "the second largest health information breach in history and the largest hacking-related health information breach ever reported," Ranking Member of the House Committee on Oversight and Government Reform Elijah Cummings (D-MD) is requesting that the committee engage in a formal investigation of Community Health. (A slightly larger data breach involving the theft of information regarding TRICARE enrollees occurred in September 2011.) The OCR, however, classified this breach as theft of data from a network server, rather than a hacking/IT incident.

In December 2013, Horizon Healthcare Services, Inc., doing business as Horizon Blue Cross Blue Shield of New Jersey (Horizon) reported that two password-protected, unencrypted laptops were stolen from its headquarters. The laptops were believed to contain names, addresses, and dates of birth of 839,711 subscribers and, in some cases, Social Security numbers and "limited clinical information." In October 2013, two password-protected laptops were stolen from the administrative offices of AHMC Healthcare in California, which included patient names, Medicare/insurance identification numbers, diagnosis/procedure codes, insurance/patient payments, and, in some cases, Social Security numbers, related to 729,000 Medicare patients treated at six different hospitals.

Enforcement

The OCR reported that it entered into seven resolution agreements and corrective action plans (CAPs) with CEs by the end of 2013 for data breaches that occurred through 2012. These agreements were the first settlements resulting from OCR investigations into reported breaches. Four of the breaches involved the theft of electronic devices containing unencrypted patient information. In the first enforcement action resulting from a breach report, the OCR determined that Blue Cross Blue Shield of Tennessee (BCBST) failed to perform a required security evaluation in response to operational changes and failed to implement required physical safeguards, compromising the PHI of more than 1 million individuals when a number of hard drives were stolen. After agreeing to pay $1.5 million, BCBST also entered into a CAP in which it agreed to review, revise, and maintain its HIPAA Privacy and Security policies; conduct regular, in-depth HIPAA trainings for employees, and engage a monitor to ensure compliance with the CAP. Other CAPS were similar, but some included additional items requiring entities to conduct risk analyses, develop risk management plans, name a security official to be responsible for HIPAA security

rule implementation, submit documentation of plans, and, in one instance, attempt to retrieve photocopier hard drives containing unencrypted information that were sent to the photocopier leasing company.

In addition, the OCR completed a pilot HIPAA audit program at the end of 2012, in which it audited 115 entities to assess compliance with privacy and security requirements. The OCR audited 101 entities for breach notification requirements; 31 had at least one finding or observation related to the breach notification rule. The largest issue was method of individual notification, followed by burden of proof, timeliness of notification, and notification of individuals. In its 2014 work plan, the HHS Office of Inspector General (OIG) expressed its intention to review the OCR's oversight of the breach notification requirement. In addition, the OIG plans to assess the security of portable devices containing PHI utilized at hospitals, certified EHR technology, and networked medical devices, such as dialysis machines.

The federal government is not alone in its investigation into data breaches. State attorneys general also are becoming involved. In July 2014, for example, the Massachusetts Attorney General settled with Women & Infants Hospital (WIH) of Rhode Island for $150,000 for the hospital's failure to comply with breach notification requirements. In the summer of 2011, 19 unencrypted backup tapes from two prenatal diagnostic centers that included 12,127 Massachusetts residents' patients' names, dates of birth, Social Security numbers, dates of exams, physicians' names, and ultrasound images went missing. WIH failed to realize the data were missing until the spring of 2012 and failed notify the Massachusetts Attorney General until November 2012.

Lawsuits. Data breach victims also have begun bringing lawsuits against CEs and BAs in civil court. Although courts tend to dismiss those cases for lack of standing, the threat of lawsuits is very real. In 2011, an employee of a firm contracting with TRICARE was the victim of an automotive burglary, during which data tapes containing the names, Social Security numbers, addresses, dates of birth, phone numbers, and medical information of 4.7 million military TRICARE enrollees were stolen. Many plaintiffs filed lawsuits, but a federal district court hearing eight consolidated cases determined that only two individual plaintiffs had standing to bring the suits because they were able to demonstrate a relationship between the stolen data and identify theft or targeted medical advertising. The remaining plaintiffs did not have standing because an increased likelihood of identity theft, without evidence that data was actually accessed or misused, did not establish a sufficient injury. In the court's opinion, "wide-scale disclosure and misuse" of all data was not "certainly impending." To drive the point home, the court referred to a study suggesting that 3.3 percent of Americans will experience identify theft and noted that 155,000 TRICARE beneficiaries could expect to "experience identity fraud simply by virtue of living in America and engaging in commerce, even if the tapes had not been lost," (see *4.7 million TRICARE enrollees' protected health information stolen*, May 13, 2014).

In July 2013, Advocate Medical Group's suburban Chicago administrative office was burglarized and four unencrypted computers including demographic and limited clinical information for more than four million patients were stolen. Two lawsuits filed in circuit courts in separate counties have been dismissed because the plaintiffs were unable to demonstrate actual harm. A federal lawsuit alleging that Advocate violated the Fair Credit Reporting Act (FCRA) also was dismissed for lack of standing because the judge determined that hospitals are not CEs for purposes of the FCRA. A consolidation of 12 class action lawsuits filed in Cook County Circuit Court remains pending. Five Alabama plaintiffs also have brought suit against Community Health stemming from the data breach announced it in August.

Conclusion

What lessons can CEs and BAs learn from recent breaches and enforcement actions? The OCR advises ensuring that the security risk analysis has been thoroughly conducted and that a comprehensive risk management plan is in place. In addition to being required by law, Chestler points out that the security risk analysis can help a provider know where its "particular weakness lies," given "very complex and intertwined systems and access." The OCR also recommends performing security evaluations when operational changes occur, such as facility moves and conducting technical evaluations when technical upgrades or changes take place. It emphasizes the security of portable electronic devices, advocating clear policies and procedures for protecting PHI on and off-site. It also urges the implementation of policies and procedures governing the proper disposal of PHI, safeguards limiting physical access to facilities and workstations, and training regarding the proper use and disclosure of PHI, as well as the sanctions for failure to comply.

Chestler is frank in her advice to CEs, BAs, and their representatives. "While the regulatory landscape has not changed, HIPAA is no longer just a law on the books." Counsel, she contends, must "understand the enforcement is much more vigorous." Providers should know that "their program must be more than just words on a page."

Attorneys: Alisa Chestler (Baker Donelson)

MainStory: StrategicPerspectives ConfidentialityNews EHRNews EnforcementNews HITNews HIPAANews

HRWE ELEMENTS
- Kicker for HRWE:
- Tags for HRWE: