INCREASING RISK OF THEFT OF HEALTH CARE INFORMATION

Diane Felix

The 2014 “blockbuster” health care data breach of the year was without a doubt the Community Health Systems (“CHS”) breach, in which hackers gained access to personal information for approximately four and a half million patients. CHS reported as follows in an August 18, 2014 Form 8-K filing with the United States Securities and Exchange Commission:

In July 2014, Community Health Systems, Inc. (the “Company”) confirmed that its computer network was the target of an external, criminal cyber attack that the Company believes occurred in April and June, 2014. The Company and its forensic expert, Mandiant (a FireEye Company), believe the attacker was an “Advanced Persistent Threat” group originating from China who used highly sophisticated malware and technology to attack the Company’s systems. The attacker was able to bypass the Company’s security measures and successfully copy and transfer certain data outside the Company. Since first learning of this attack, the Company has worked closely with federal law enforcement authorities in connection with their investigation and possible prosecution of those determined to be responsible for this attack. The Company also engaged Mandiant, who has conducted a thorough investigation of this incident and is advising the Company regarding remediation efforts. Immediately prior to the filing of this Report, the Company completed eradication of the malware from its systems and finalized the implementation of other remediation efforts that are designed to protect against future intrusions of this type. The Company has been informed by federal authorities and Mandiant that this intruder has typically sought valuable intellectual property, such as medical device and equipment development data. However, in this instance the data transferred was non-medical patient identification data related to the Company’s physician practice operations and affected approximately 4.5 million individuals who, in the last five years, were referred for or received services from physicians affiliated with the Company. The Company has confirmed that this data did not include patient credit card, medical or clinical
information; the data is, however, considered protected under the Health Insurance Portability and Accountability Act (“HIPAA”) because it includes patient names, addresses, birthdates, telephone numbers and social security numbers. The Company is providing appropriate notification to affected patients and regulatory agencies as required by federal and state law. The Company will also be offering identity theft protection services to individuals affected by this attack. The Company carries cyber/privacy liability insurance to protect it against certain losses related to matters of this nature. While this matter may result in remediation expenses, regulatory inquiries, litigation and other liabilities, at this time, the Company does not believe this incident will have a material adverse effect on its business or financial results. (emphasis added) ¹

The DHHS/OCR online list of breaches of unsecured protected health information (a/k/a the “Wall of Shame”) shows that CHS reported its breach as a “theft.” ²

CHS’s cost of dealing with the security breach, which involves patients in 29 states, has been estimated at somewhere between $75 million and $150 million. ³ Those costs could include remediation, HHS/OCR fines, identity theft protection or credit monitoring for patients, and defending against both patient and shareholder lawsuits and

settlements. The first class-action lawsuit related to the breach was reportedly filed “within hours after the breach was announced.”

Shortly after public announcement of the CHS breach, the Federal Bureau of Investigation issued a “Flash Alert,” which warned that "The FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)." The FBI had released a similar warning in April, 2014, saying that healthcare organizations’ IT systems and medical devices were at risk for increased attacks from hackers due to lax cybersecurity standards and practices.

While many long-term care provider organizations may believe that they are unlikely to be targets of the kind of hacking attack that caused the CHS breach, they should not assume that their information is of little interest to sophisticated hackers, nor should they assume that only a sophisticated hacker can cause significant damage.

________________________

4 Id.
5 Id.
Another healthcare organization that made it into the “top ten” on the DHHS/OCR “Wall of Shame” in 2014 – NRAD Medical Associates, PC, in Garden City, New York – determined that its breach (identified as “Hacking/IT Incident, Unauthorized Access/Disclosure”) had been caused by an employee. NRAD posted an online notice (dated July 18, 2014), in which it said that NRAD had discovered in April, 2014 that an employee radiologist had “accessed and acquired protected health information from NRAD's billing systems without authorization,” including “some personal information, including patient names and addresses, dates of birth, social security numbers and health insurance, diagnosis codes and procedure codes,” but that there was no indication that any patient financial information was accessed. Reportedly, NRAD sent written notification to 97,000 affected patients, and the radiologist, who was no longer employed by NRAD, was being investigated by the Nassau County District Attorney’s Office. In December, 2014, the Nassau County District Attorney announced that Richard Kessler, MD had been arrested and would be charged with three misdemeanors – unauthorized use of a computer, unlawful duplication of computer-related material, and petty

8 DHHS/OCR Breach Portal, infra.


larceny. According to a news release from the Nassau County DA’s Office, an investigation revealed that:

Kessler connected an external hard drive to his assigned NRAD computer and copied onto it patient information from the NRAD network. A search warrant uncovered Kessler’s hard drive containing approximately 97,000 NRAD patient records, as well as NRAD patient billing system dates, NRAD corporate credit card information, corporate marketing materials, and NRAD IT information.

Even small organizations are at risk of security breaches. An 18-bed county hospital in Flora, IL, reported on December 15, 2014, that it had received an anonymous email, which included some information about some clinic patients and threatened to publicly disclose the information unless the sender received a “substantial payment” from the hospital. The hospital’s press release stated that the information “was limited to name, address, Social Security number and date of birth” and that “no medical information was accessed or disclosed.” The hospital’s press release also stated that “extensive reviews from outside forensic experts concluded that Clay County Hospital

servers have not been hacked and remain secure due to the rigorous security program that meets the standards set by the HIPAA HITECH Act.”

At this point the available information doesn’t indicate what the motivation may have been for the Nassau County radiology breach. One can speculate that the breach was motivated ultimately by the prospect of financial gain, as seems to be case with the Illinois hospital breach. It is unclear whether the individuals or groups behind the two breaches obtained any financial benefit.

It may be tempting to think that most long-term care organizations, particularly smaller ones, won’t have information that will be financially tempting enough to attract potential wrong-doers. Such an assumption would be incorrect.

Georgia newspaper The Telegraph reported that in December, 2014, a former Certified Nursing Assistant for a Macon, Georgia skilled nursing facility was sentenced to five years on probation after pleading guilty in an identity theft scheme involving stolen patient information. In her guilty plea, the CNA admitted that she provided the information to another woman who used the information to file fraudulent tax returns.

__________________________

14 Id.

The second woman was sentenced last year to twenty-seven years in prison. According to The Telegraph article:

Hogan admitted in her plea agreement that she met Blount in the Macon nursing home’s parking lot and gave her a handwritten list of patient names, birth dates and Social Security numbers. Authorities later found the list when they searched Blount’s New Clinton Road home.

Several false tax returns were filed using the nursing home residents’ names, and bank documents showed tax refunds issued based on the returns were deposited onto prepaid debit cards, according to the plea agreement.

Hogan’s conduct contributed to $17,577 in refunds, although only $6,500 was paid out by the U.S. Treasury.

During Thursday’s hearing, defense attorney Catherine Williams asked the judge to allow her client to serve her sentence on probation, saying Hogan was only responsible for disclosing information for 13 people.

“That is it,” Williams said. “She received no money for that.” 16

Medical information, even if it lacks credit card numbers and specific financial information, is still valuable information to an unscrupulous employee, sophisticated hackers, or even outsiders with relatively limited sophistication. An October, 2014, Forbes article regarding the causes of increased medical identity theft noted “Personal medical information is useful to many different types of criminals, which is why it fetches a higher price on the black market than financial information.” The article quoted Larry Ponemon, chairman and founder of the Ponemon Institute, a cybersecurity research firm: “The crime itself can be very valuable to a cyber criminal or any criminal, even a

16 Id.
low-tech criminal, and the reason is that the information contained in a medical record includes just about everything about you.” 17 The *Forbes* article also quotes an attorney with the Federal Trade Commission (Steven Toporoff), who explained that a thief could steal the file for non-medical information such as the Social Security number, but that medical information could also be sold, perhaps to data brokers who sell it to marketers that want to target those with a particular medical condition. 18

Experian’s 2015 *Data Breach Industry Forecast* warns that healthcare is “a vulnerable and attractive target for cybercriminals, and also notes that employees remain the leading causes of compromises. 19 Security rating firm BitSight Technology warns that “massive data breaches at Target and eBay could be a taste of what's in store for the healthcare industry.” 20

Whether the motivation for breaches of health care records is financial gain, intent to hurt an organization’s reputation, or even a bizarre type of entertainment, it’s clear that the risk is real. Health IT security has become one more challenge facing the long-term

18 *Id.*
care world. As with the most serious of those challenges, failure to be prepared can lead to bad publicity and catastrophic expenses.

Diane E. Felix (dfelix@armstrongteasdale.com) is a partner in the St. Louis, Missouri office of Armstrong Teasdale LLP, focusing on representation of health care providers, with a significant portion of her practice involving post-acute services and senior care organizations. She advises clients on matters relating to Medicaid and Medicare reimbursement, licensure and certification, Certificate of Need, business agreements (including network arrangements and leases and purchase agreements) and operational issues such as HIPAA and HITECH compliance and OCR investigations. Before joining entering private practice, Diane had nine years of experience as an attorney with Missouri State government, during which she handled Medicaid-reimbursement and health care-related matters.