



Facing Evolving Cyberthreats and Crippled by Ransomware Attacks, *Can Hospitals Ever Really Be Prepared?*

Prepared by:
Laura E. Jehl
Sheppard, Mullin, Richter & Hampton LLP



January 2017

Facing Evolving Cyberthreats and Crippled by Ransomware Attacks, Can Hospitals Ever Really Be Prepared, ©2017 Lorman Education Services.
All Rights Reserved.

INTRODUCING

Lorman's New Approach to Continuing Education

ALL-ACCESS PASS

The All-Access Pass grants you **UNLIMITED** access to Lorman's ever-growing library of training resources:

- ☑ Unlimited Live Webinars - 120 live webinars added every month
- ☑ Unlimited OnDemand and MP3 Downloads - Over 1,500 courses available
- ☑ Videos - More than 700 available
- ☑ Slide Decks - More than 1700 available
- ☑ White Papers
- ☑ Reports
- ☑ Articles
- ☑ ... and much more!

Join the thousands of other pass-holders that have already trusted us for their professional development by choosing the All-Access Pass.



Get Your All-Access Pass Today!

SAVE 20%

Learn more: www.lorman.com/pass/?s=special20

Use Discount Code Q7014393 and Priority Code 18536 to receive the 20% AAP discount.

*Discount cannot be combined with any other discounts.

Facing Evolving Cyber Threats and Crippled by Ransomware Attacks, Can Hospitals Ever Really Be Prepared?

- Laura E. Jehl

It's happened again. On November 2, an unspecified "major" cyberincident forced three National Health Service (NHS) hospitals in the UK to shut down all planned operations and divert critically ill patients to other facilities for three days until their electronic systems could be restored. The shutdown affected 3,300 patients and came just as the UK detailed a national cyberstrategy designed to shore up security in critical national infrastructure such as hospitals. In response, the NHS placed all hospitals across the UK on high alert and suggested that Russia may have been behind the disruption.

As in previous incidents this year, the hackers' tool of choice was likely ransomware, an increasingly popular form of attack that does not steal data but instead disables files and systems by encrypting them with a virtually unbreakable code. The hackers then demand a ransom payment to re-enable or unlock them. Indeed, 2016 has been called "the year of ransomware," and a recent report by Intel Security finds the healthcare industry in the crosshairs, experiencing a reported 20 ransomware incidents per day, with hospitals having paid nearly \$1,000,000 in ransom to specific Bitcoin accounts so far in 2016.

In February, for instance, Hollywood Presbyterian, a Los Angeles-area hospital, announced that its communications systems had been disabled for more than a week, until the hospital paid a ransom of 40 bitcoins – about \$17,000 – in order to regain access to its systems. And in March, MedStar Health, a 10-hospital system in the Washington, D.C., area, and Prime

Healthcare, an operator of three California hospitals, reportedly suffered similar attacks, as did Methodist Hospital in Kentucky. To date, the ransoms demanded in hospital attacks have not been astronomical – generally in the tens of thousands of dollars – but the potential threat to patient safety as a result of the disruption of communication and lack of access to patient records has been particularly frightening.

This year's epidemic of ransomware attacks follows a tumultuous cybersecurity year in 2015, which experts called "the year of the healthcare data breach." Last year opened with the news that health insurer Anthem, Inc., had suffered a cyberattack resulting in the theft of personal health information (PHI) of nearly 80 million individuals, including Social Security numbers. The magnitude of the attack, and the extremely sensitive nature of the data stolen from Anthem's systems, sent waves of concern through the healthcare industry, which had traditionally lagged behind other industries in cybersecurity preparedness. Just six weeks later, the alarm rang again when Premera, a Pacific Northwest health plan, announced that it, too, had suffered a major breach, this time involving the confidential records of 11 million individuals. Next came breaches at CareFirst Blue Cross Blue Shield affecting 1.1 million records, and Excellus, another Blue Cross Blue Shield (BCBS) plan, which disclosed 9 million records. But the healthcare industry breaches weren't limited to insurers: Hackers broke into UCLA Health System and may have accessed sensitive health information on as many as 4.5 million patients; an attack on Medical Informatics Engineering, a provider of electronic health records, disclosed 3.9 million patient records; and state health agencies in Virginia and Georgia were breached, each disclosing sensitive PHI of hundreds of thousands of individuals. All told, according to the Office for Civil Rights at the Department of Health and Human Services, more than 112 million records protected under the federal Health Insurance Portability and Accountability Act (HIPAA)

were disclosed in 2015, the vast majority accessed and/or stolen as a result of cyberattacks.

The healthcare industry reacted to 2015's mega data breaches with concern. Historically focused on their compliance obligations under HIPAA, insurers, hospitals and other providers had long emphasized preventing breaches of patient privacy through the loss or theft of laptops, unauthorized access to patient files by staff, and other inadvertent lapses; by contrast, cybersecurity efforts were often underfunded and unsophisticated. After last year's wave of huge breaches, however, healthcare industry players opened their wallets, hiring teams of forensic security consultants to comb through their electronic data systems looking for any evidence of compromise, identifying and remediating vulnerabilities, and protecting confidential patient information with encryption. In addition, the Blue Cross and Blue Shield Association announced that all BCBS companies would make identity protection services available to their customers nationwide beginning on or before January 1, 2016, in an effort to provide better safeguards in the event of fraudulent use of customers' personal and financial information.

Healthcare Still Under Fire - Why is healthcare still so easily hacked? Why, even after boards and executives focused on cybersecurity and invested heavily in improving their systems after the wave of major data breaches, is healthcare being crippled by this new scourge, ransomware? First, the cybersecurity safeguards of many healthcare organizations have been aimed at "fighting the last war" rather than anticipating and guarding against new threats. The industry's prior focus on avoiding laptop thefts and unauthorized disclosures of paper files left hospitals and insurers nearly defenseless against last year's sophisticated cyberattacks, which were intended to steal vast troves of electronic data. And now it appears that the emergency – and expensive – remediation efforts undertaken across the

industry in response to the 2015 attacks may be inadequate to safeguard those same hospitals against ransomware, a new type of attack.

Many traditional cybersecurity safeguards are simply not aimed at preventing unauthorized encryption of data and are thus ineffective against ransomware attacks. Although access to systems in both the breach and ransomware scenarios is usually achieved the same way – through “phishing attacks designed to induce employees into sharing passwords and/or downloading malware – ransomware attacks demand different defenses than cyberattacks intended to steal data. For instance, an important security measure has been the implementation of data encryption (and not just during transmission), which renders data unreadable, unusable and unmarketable in the event it is stolen. Such encryption became more widespread, including among many healthcare companies, following last year’s massive breaches. But encryption will not prevent a ransomware attack, since the intent of ransomware is not to steal data in a meaningfully readable form. Instead, it encrypts the data itself, making it unreadable and unusable by its rightful owner.

Second, despite the advances made in the last year, healthcare has historically lagged behind other industry sectors in spending on IT security, and it still may not have caught up. Third, attacks on the healthcare industry are financially profitable for hackers. Stolen healthcare data is often more valuable than stolen credit card data; unlike a credit card, which can be canceled, healthcare data contains permanent elements such as Social Security numbers that can be used indefinitely to commit identity theft or healthcare fraud. Ransomware is a low-cost, low-risk cash-generating business for hackers.

Finally, electronic records have been aggressively pushed by the federal and state governments and, as such, embraced by the vast majority of the healthcare industry as a way to enhance patient care. As a result, hospital staff is more dependent on electronic health records than ever before. If a treating physician can't access critical information such as patient drug dosages, medical history, complex treatment plans or diagnostic tests due to a ransomware attack, treatment can be compromised. Some hospitals that have been attacked – including those in the UK attack in November – have been forced to move temporarily to paper records or to shut down their entire systems for fear of the malware spreading to core servers and functionality.

The impact of a ransomware attack can also extend beyond immediate patient care. Consider, for instance, medical records coders who can't access the records necessary to code for inpatient or outpatient services rendered, thereby preventing the hospital from billing, which interrupts the revenue cycle. Or the finance department that can't pull up crucial reports, memos and financial data needed to run the hospital's day-to-day business. Although no ransomware attack to date has been publicly reported as having compromised electronic dosing or treatment systems, these systems, like all computers, can and will eventually be hacked.

Because a ransomware attack has potentially crippling adverse consequences, hospitals are often in an untenable position when facing a ransom demand, and, as a result, have been willing to pay the ransom, despite concerns that the money may end up in the hands of organized crime, terrorist groups or foreign governments. Experts believe that the dollar amount of these demands is likely to rise as hackers become more sophisticated about the value of the systems they disrupt, as the attacks themselves become increasingly focused on high value (and high patient-

risk) systems, and – importantly – as healthcare providers become more accustomed to paying ransoms.

Anticipate the Attack and Prepare Now - Many hospitals have developed sophisticated enterprise risk-management programs that are designed to address a wide range of institutional risks, from HIPAA privacy and security to fraud and abuse compliance and disaster preparedness. At the very least, the risk of ransomware attacks should be part of such a program. That includes taking steps to prevent or minimize the occurrence of such attacks and establishing a clear plan about how to respond to an attack, without panic, while protecting patient safety and the integrity of hospital operations. A copy of this emergency response plan – including phone numbers of key contacts – should be kept somewhere other than on the company's systems.

The best protection against a ransomware attack is to frequently and thoroughly back up all critical applications and data in a secure file, so that they can be restored and work properly if an attack cripples the main systems. The backups should be tested to verify their integrity, and they should never be connected to the networks they are backing up. If a hospital or other victim of a ransomware attack can use its own backups to conduct operations, it won't be necessary to pay the ransom. In addition, hospital systems must include robust firewalls, ensure that their intrusion detection/prevention systems are up to date and able to receive updates and patches, and consider adopting ransomware-specific detection and prevention systems.

Further, healthcare providers can benefit from programs to train employees about how to recognize phishing attacks. The most effective training sends a series of mock phishing emails to employees who have been told to be on

the lookout for attacks. But even the best training is not foolproof; one recent study found that, on average, 13 percent of recipients who received mock emails in training scenarios clicked on a link or opened an attachment associated with a fake phishing email. Administrators should also restrict access to sensitive files and ensure that personnel can only access the data necessary to perform their jobs.

Rather than becoming mired in day-to-day demands, or devoting too many scarce resources to “fighting the last war,” the healthcare industry needs to focus on anticipating the next risks on the horizon. Ransomware attacks are likely to become more sophisticated and the attackers savvier about the value of the data they have encrypted, making the potential business impact more devastating. Worse, if hackers choose to devote their efforts to disabling medical devices and treatment technologies, rather than merely communications systems, the potential risks to patients will skyrocket. Healthcare’s best defense against potentially disastrous future attacks – whether through data breaches, ransomware, or the next variant on the horizon – is to be forward-looking, nimble and vigilant.

