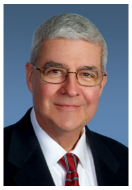
Ransomware Threatens Healthcare

April 2016 • Lockton® Companies

BEN BEESON
Senior Vice President
Cyber Risk Practice Leader
202.414.2653
bbeeson@lockton.com

STEVE D. GRAVELY
Partner
Troutman Sanders, LLP
804.697.1308
steven.gravely@
troutmansanders.com



Hospital pays to unlock electronic medical record from ransomware, the headline says it all. Healthcare providers are facing unprecedented numbers of "ransomware" attacks in which their operating systems and electronic medical records (EMRs) are held hostage in exchange for extortion payments. The Healthcare Information and Management Systems Society (HIMSS) reported that one-half of US hospitals have been targeted by ransomware attacks. In April, the Washington, DC-based health system, MedStar, suffered a ransomware attack that resulted in its entire computer system housing patient electronic medical records, being shut down. MedStar scrambled to implement backup systems, but patient records were left vulnerable, and patient care was disrupted for nearly a week.

Hospitals are being targeted by cyber criminals, in part because medical records are so rich in personal information and, thus, extremely valuable on the black market. The personal information included in a typical medical record easily supports the creation of false identities to commit insurance fraud. Healthcare is also a "target rich" environment.

THE HEALTHCARE INFORMATION AND MANAGEMENT SYSTEMS SOCIETY (HIMSS) REPORTED THAT ONE-HALF OF US HOSPITALS HAVE BEEN TARGETED BY RANSOMWARE ATTACKS.

> IT'S REALLY A NUMBERS GAME; THE MORE EMPLOYEES A HOSPITAL HAS THE MORE POINTS OF ENTRY THERE ARE.

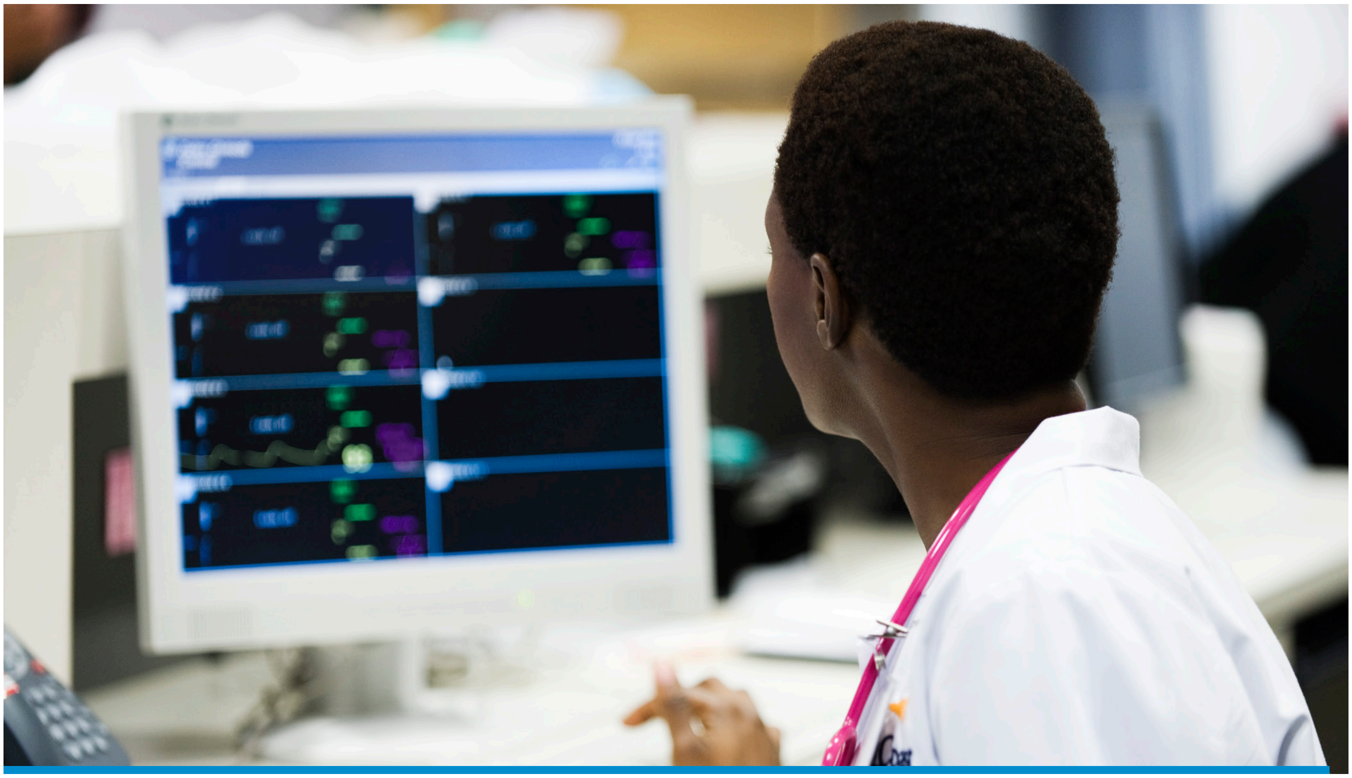
In 2016, The American Hospital Association reported that there were 5,627 hospitals in the US with an astounding 34,878,887 hospital admissions in a single year! The amount of electronic health information that is being created for patients every single day is staggering.

This begs the question of why, in 2016, are healthcare providers so vulnerable to data breach and cyber attacks? The easy answer is to blame healthcare providers for not investing enough money in cybersecurity measures. But, the easy answer is seldom the correct answer, and that is true here. The truth is more complex and reveals why achieving true cybersecurity in the healthcare industry is so challenging.

Multiple Health IT Systems

Hospitals and health systems are extremely complex, multifaceted organizations in which critical, personal patient information can be distributed across multiple IT systems. Computerized financial systems, which contain HIPAA Protected Health Information and other valuable financial records, have been in use by organizations throughout the industry since the 1960s. The first computerized clinical systems appeared in hospital labs and radiology departments in the 1970s, followed by first-generation Computer-based Physician Order Entry (CPOE) systems implemented in the early 1980s in large teaching hospitals. While the HITECH provisions of the American Recovery Reinvestment Act and the Meaningful Use program have led almost every hospital and physician group to implement electronic medical records since 2009, many legacy computer systems, which were implemented before cybersecurity threats to the medical community were understood, remain in use. Valuable patient information can be stored on these outdated systems. Moreover, once legacy systems, which often lack state-of-the-art cybersecurity features, are networked together with more current technology, these older systems become easy backdoors for cyber criminals.

The rapid consolidation of health networks, systems, and physician practices is compounding the already explosive number of different health IT systems. As hospitals merge or acquire physician practices, they inherit whatever operating system storing electronic medical records that was in place before the merger or acquisition. The result is a dizzying array of overlapping health IT infrastructure from different vendors with varying system and cybersecurity requirements. Health systems are required to make major investments to interconnect these disparate systems to support basic patient care, let alone to support meaningful use and value-based care programs. With interconnectivity comes vulnerability since the security of an entire system depends on the weakest link. The effort required to govern so many different health IT systems puts a strain on CIOs, CISOs, and CPOs.

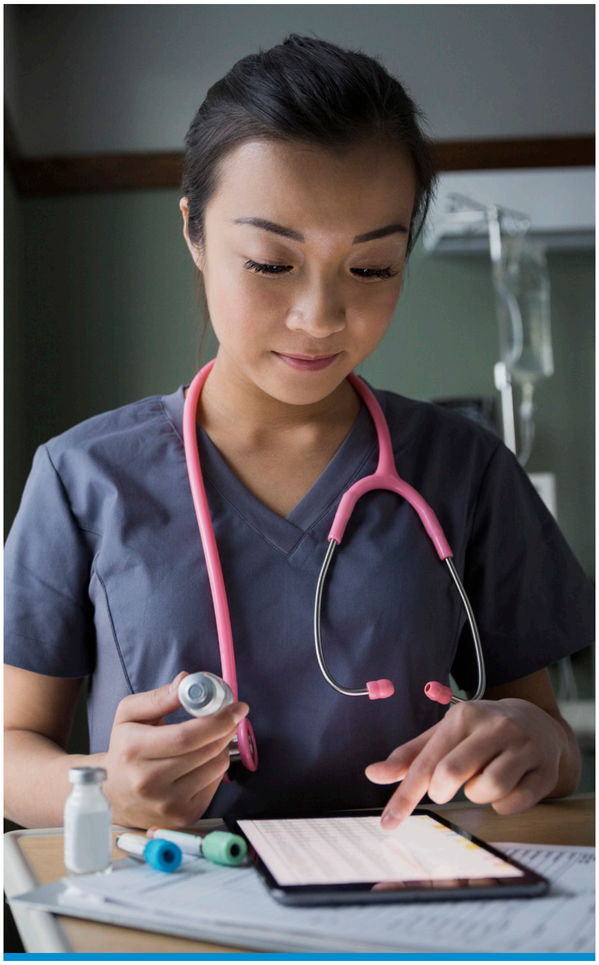


Large Number of Users

Employees are the most common vector for ransomware to gain access to a computer system. The healthcare industry is very staff-intensive. Staffing costs represent the single largest cost component for all US hospitals, averaging over 50 percent of total revenue! An "average-sized" hospital will employ hundreds of personnel with access to electronic health records; larger hospitals employ thousands. Every staff member who requires access to electronic health information must be issued "digital credentials" to permit them to access those operating systems that contain the information. Keeping track of these credentials—and making sure that the credentials are revoked when an employee ceases employment—are massive responsibilities. Real-time monitoring of user access is simply not feasible for most health systems today, given limited resources and the limits of technology. Cyber-criminals are becoming increasingly sophisticated with their phishing attacks, making them harder to detect. It's really a numbers game; the more employees a hospital has, the more points of entry there are.

It is not unusual in healthcare for one care provider to work for multiple health systems in the same community. Flexible staffing helps control costs but can also result in employees having multiple part-time jobs. These staff members will have digital credentials to operating systems and EMRs for every health system employing them, exponentially increasing the opportunity for credentials to be lost or stolen. It is also common for employees to use the same password for access to multiple systems, because it is easier to remember, which means cyber criminals can access multiple operating systems and different EMRs through a single person.

> TECHNOLOGY HAS ALLOWED FOR FEWER HIGHLY TRAINED CLINICAL STAFF MEMBERS TO EFFECTIVELY TREAT A LARGER NUMBER OF PATIENTS.



Healthcare also has large numbers of nonemployed persons who may need access to a hospital's EMRs in order to deliver care. Physicians, care managers, intake nurses for post-hospital care providers and many others must be able to access EMRs in order to do their jobs. Far more than in other industries, health IT systems are open to a large number of people. Not only does this vastly increase the risk of lost or stolen credentials, but it also creates a large pool of people who are vulnerable to blackmail. An employee with an addiction, vulnerable family member, or any other skeleton in the closet that may threaten his or her livelihood, can easily be blackmailed by criminals to provide access to an employer's EMRs and operating system. This kind of access can go undetected for a long time. The sheer number of people who have legitimate access to a hospital's EMRs complicates security training and monitoring of the appropriate system usage.

Connected Medical Devices

The Internet of Things (IoT), the system in which everyday objects have network connectivity, allowing them to send and receive data, has become a dominant feature of everyday life. Today, there are over 6 billion devices connected to the IoT, and reliable projections predict by 2020, there will be 20 billion! The pace and scale of growth are unprecedented in human history. The speed with which the IoT has become embedded into everything that we do and the explosion in connected devices has come at substantial cost: the privacy and security of personal information that the IoT touches are very much at risk. Nowhere is this problem more immediate than in the healthcare sector worldwide.

The delivery of healthcare in all developed countries is extremely technology-dependent. The reasons for this are very clear: cost and quality. Technology has allowed for fewer highly trained clinical staff members to effectively treat a larger number of patients. An automated blood pressure cuff, for example, that checks the blood pressure of a patient every 15 minutes and sounds an alarm if the reading is outside of the acceptable range, eliminates the need for a nurse or technician to manually take the patient's blood pressure. Not only does this allow trained caregivers to focus their efforts elsewhere, but it also enhances consistency of quality through automation. An automated blood pressure device will not get too busy to take a patient's blood pressure. An automated intravenous pump will consistently administer the exact dosage of IV fluid and IV medication entered into the control panel and will sound an alert instantly when something is awry. While these devices are far from perfect, and the device-human interaction has created a whole new set of issues, it is indisputable that medical devices are an integral part of modern healthcare, and their role will only continue to grow.

The US Food and Drug Administration issued an urgent industry alert to hospitals, and others, in 2015, urging them to stop using the Symbiq IV infusion pump because it could be easily hacked. This unprecedented measure highlighted the extreme vulnerability of connected medical devices and how they can be used as easy points of entry by cyber criminals. In early 2016, the US Federal Trade Commission issued guidance for medical device manufacturers, urging them to begin building cybersecurity measures into their devices. Hospitals, in particular, are in a conundrum because connected medical devices have become so ubiquitous that it is becoming impossible to deliver quality care without them. The lack of security in these devices, however, makes them easy portals into the hospital's operating system and EMRs by cyber criminals. Further, if a hospital modifies the device software to add cybersecurity protections, they run the risk of voiding a manufacturer's warranties. It is easy to see that the industry is on a collision course with a cyber disaster. The question is, "What can be done to avoid it?"

The US Food and Drug Administration issued an urgent industry alert to hospitals, and others, in 2015, urging them to stop using the Symbiq IV infusion pump because it could be easily hacked.

This unprecedented measure highlighted the extreme vulnerability of connected medical devices and how they can be used as easy points of entry by cyber criminals.

In early 2016, the US Federal Trade Commission issued guidance for medical device manufacturers, urging them to begin building cybersecurity measures into their devices.

Take the following specific steps immediately to address the threat:

1 Elevate the threat awareness.

Health systems must recognize that ransomware and other cyber threats are not only financial issues. The ability of ransomware to shut down a hospital's EMR and compromise its ability to deliver care makes this a patient safety issue. Even more concerning is the ability of hackers to manipulate medication doses or interfere with life-sustaining equipment, which could disable or kill a patient. Cybersecurity must be considered as major of a threat to patient safety as fires, hospital-acquired infections, or natural disasters.

2 Owning cybersecurity.

During World War II, the government put up posters to remind everyone that "loose lips sink ships." This was a national campaign that made every US citizen feel engaged in the war effort while also recognizing a real national security concern. Everyone who works in a healthcare system, regardless of his or her job title or seniority, should be taught that cybersecurity is a critical responsibility. The notion of sharing one's system password with a coworker should be considered as much of a nonstarter as giving one patient another patient's medicine or treatment. Reporting suspicious activity should be as normal as reporting a broken instrument or device. Performance reviews should include cybersecurity as a core competency for everyone.

3 Think like a hacker.

Every industry has things that are considered so embedded into protocol and procedure that they simply must be done a certain way. When it comes to cybersecurity, it's time to think like a hacker. How would you attack your own system? What is the weakest link or the easiest backdoor? Given that healthcare is so very staff-dependent, the answer should always include people. Tech alone cannot eliminate all of the risk. Changing staff behavior takes time and persistence.

4 To encrypt or not to encrypt?

If heath data was encrypted at rest, it would become much less valuable to cyber criminals. Will that be expensive? Yes. Are there universally accepted encryption standards today? No. Will encryption of data at rest impact the speed and performance of some legacy systems? Perhaps. But, the healthcare industry's vulnerability to cybersecurity threats is a crisis, and we must, as an industry, look in the mirror and recognize that bold action is necessary to reduce this vulnerability.

5 Make your Cyber Incident Response Plan real.

If a healthcare organization does not have a Cyber Incident Response Plan (CIRP) in 2016, it should consider itself behind the times and create one this year. If you have not updated your plan in the last three years, it should be reviewed and updated by a qualified professional.

6 Drill, drill, drill.

Like every plan, a good CIRP is no good if no one knows that it exists or what their roles and responsibilities are. You should be regularly conducting drills, using the plan, and evaluating where you could have done better. The CIRP should become a part of regular in-services with all staff, new employee orientation, and regular hospitalwide exercises.

> THE ABILITY OF RANSOMWARE TO SHUT DOWN A HOSPITAL'S EMR AND COMPROMISE ITS ABILITY TO DELIVER CARE, MAKES THIS A PATIENT SAFETY ISSUE.

7 Make new friends.

Cyber theft is a federal crime and should be treated as such. If someone broke into the hospital pharmacy and stole drugs, you would not think twice about contacting the police as well as the DEA and perhaps even the state licensing authority. If your facility is the victim of a cyber attack, the FBI would like to know. Their door is open, and they are encouraging folks to contact them. This is actually a rather complicated decision that you should make in consultation with competent legal counsel. Don't wait until an attack to meet law enforcement. Reach out and meet your local and regional FBI officials and find out who is the correct contact for cybersecurity issues. Talk to that person, and establish a business relationship.

8 Prepare today for a ransomware attack.

Hospitals should assume that they will be targeted in a ransomware attack and prepare now. This includes developing specific plans on how the hospital will continue to operate without its electronic medical records, or other information systems, for an extended period of time.

9 Review your insurance.

Traditional property insurance policies typically do not cover cyber extortion demands, costs to restore compromised data, or loss of revenue from network downtime. Work with your broker to find specialized cyber insurance that can address these gaps and others such as breaches of protected healthcare information.

The factors that make healthcare systems attractive and vulnerable targets for cyber criminals are not going to change anytime soon. There will continue to be large numbers of overlapping health IT systems for years to come. Hospitals and other providers will continue to employ large numbers of staff, and those employees will continue to work for multiple providers and have access to many different EMRs. The growth of "connected devices" will continue and accelerate with more personal and health information being stored on them. Device manufacturers will respond to regulatory and market forces to imbed more cybersecurity into their devices, but this will take time. In the meantime, cyber criminals are becoming more creative and effective every day. Malware and ransomware constantly evolve in order to be less detectable and more productive. The sheer volume of electronic health data is exploding, making the prize more and more valuable to these criminal elements. By implementing these nine steps, you will be prepared for any cyber threat.

Our Mission

To be the worldwide value and service leader in insurance brokerage, risk management, employee benefits, and retirement services

Our Goal

To be the best place to do business and to work

LOCKTON®

RISK MANAGEMENT | EMPLOYEE BENEFITS | RETIREMENT SERVICES

www.lockton.com