The Strict Demands and Growing Complexity in Keeping Sensitive Healthcare Information Secure Requires a Strong IT Network Partner

By Chris West

There is no more highly regulated industry in the United States than the healthcare industry – and it's easy to see why. Healthcare providers literally hold the lives of their clients in their hands, and any mistake that is made when diagnosing and treating their patients can lead to a series of negative outcomes, up to and including death.

As if being tasked with doing everything possible to guarantee patient wellness isn't enough, healthcare providers must simultaneously protect each and every bit of patient information regarding his or her health history and course of treatment. Doctor-client privilege is not just a hoary old bromide with no teeth; it is the foundation on which the healthcare industry rests and any fracture in the doctor-client privilege relationship can lead to a lack of trust and do irreparable harm to both the provider and the patient.

So, the country's healthcare providers, who, as a group, accounted for $3.3 trillion in patient spending in 2016, or 17.8% of the U.S. gross domestic product (GDP), face a daunting two-pronged task: one, supply, without fail, a level of care that creates the best path forward in the lives of its patients and, two, do so without allowing any confidential and sensitive patient information to become public knowledge or fall into the hands of unscrupulous actors.

This white paper will focus on the second of these charges, the threats to healthcare information security and how to best build an IT infrastructure that ensures that no personal information will ever enter the public domain, either accidentally or via a hacking attempt.

The Challenge

There are six main challenges to confront and overcome when building a healthcare-friendly IT infrastructure:

- **HIPAA Compliance:** Passed in 1996, the Health Insurance Portability and Accountability Act, more commonly known as HIPAA, is a federal law that, according to the Centers for Disease Control and Prevention, mandated "the creation of national standards designed to protect sensitive patient information from being disclosed without the patient's consent or knowledge." The law mandates that every healthcare provider that electronically transmits health information ensure that those transactions are performed over a completely secure system. Specifically, healthcare providers must do four things to satisfy HIPAA's Security Rule: 1) ensure the confidentiality, integrity and availability of all protected health information; 2) detect and safeguard against anticipated security threats to sensitive patient information; 3) protect against any anticipated impermissible uses or disclosures; and 4) certify compliance by their workforce. If any HIPAA Security Rules have been found to be ignored, broken or improperly implemented (whether intentionally or unintentionally), depending on the severity of the transgression, potential outcomes range from internal punishments of employees to criminal charges that can include fines and imprisonment.

- **Data Sharing:** For many decades, all healthcare information for every individual patient was recorded and stored in a library of paper records. It is only in the past 10-15 years that the use of electronic health records (EHR) has come into greater utilization, with many healthcare providers fully committed to transitioning their paper records to an EHR system. Simply put, an EHR is a digital version of a patient's paper medical chart. The obvious advantage of an EHR is that it makes the patient's health record available to the service provider at the touch of a finger in real time. Beyond that, the EHR can use evidence-based tools to suggest the proper course of care for the patient. The challenge in operating an EHR system is that any and all digitized patient information must be stored somewhere electronically, which can make it a target for hackers who wish to steal patient information, from addresses and phone numbers to credit-card data.
- **Data Integration:** While patient data piles up, the IT systems used to compile, store and aggregate that information continue to evolve. This can create a challenge for the healthcare provider, who, while being an expert in the medical field, may know next to nothing about Cloud-based IT services, including how to select the best provider and then keep up with any upgrades and modifications that the IT company may be implementing in its systems. This makes falling hopelessly behind a real concern for healthcare providers, with any procrastination in building the best structure for data integration leading to bigger problems down the road.
- **Network Knowledge:** Hand-in-hand with Data Integration, healthcare providers must make sure that the status of their IT network is always in tip-top shape. Again, this can be hard to do since healthcare providers are always busy doing what they do best – caring for their patients – while not always having the proper knowledge concerning the operation and upkeep of their data-storage network.
- **Staying Ahead of the Curve:** There is no end to the constant churn of technological advancement. The evolution happens so quickly that what was cutting-edge two weeks ago can be hopelessly out-of-date today. The rate and complexity of this churn can be hard to grasp, especially if you do not possess the capability to ferret it out and use it to your advantage. Again, healthcare providers are in business to treat their patients, not to act as sentries who are on the lookout for the latest advance in data-storage technology. That being said, not staying cutting edge can have negative effects on their overall operation.
- **Phishing/Spear Phishing:** According to a recent Verizon Data Breach Investigative Report, system breaches that are caused by so-called "phishing" attacks, or a fraudulent attempt to obtain sensitive information via an electronic communication, are the root cause of more than 80% of all major IT security breaches. Within the realm of phishing, "spear phishing" is a targeted form of phishing attack in which deceitful emails are used to gain access to confidential information within specific organizations. Spear phishing focuses on specific employees within an organization, or the organization's social media accounts, in an attempt to customize seemingly legitimate emails that, when opened, will infect the company's entire electronic-communication system with malware. Knowing this and the sensitivity of the

information that they hold, it is easy to see how healthcare providers can be common targets for phishing/spear phishing campaigns.

The Solution

While going digital has been an unquestioned boon for the healthcare industry due to the improvements offered in time management, diagnostic capabilities and overall streamlined efficiency within the doctor-patient relationship, it has come with plenty of built-in headaches. By now these stumbling blocks should be familiar to all healthcare providers: interoperability and integration, aging equipment and hardware, asset tracking and keeping up with ever-evolving technology trends being among the most notable.

For nearly 20 years, Nexigen, Newport, KY, has been a leading developer of tools and services that can optimize operations and security protections for healthcare providers who have or will be transitioning to a digital data-management system. Specifically, Nexigen offers Secure & Protect data, virus, malware and phishing protections, Managed Services for desktop, network, server and WiFi, and Cloud Solutions platforms.

Specific to the needs of healthcare providers, Nexigen can offer the following services as solutions to common challenges:

- **HIPAA Compliance:** Nexigen is built to meet the requirements of HIPAA, especially as they pertain to the critical data-security rule. Nexigen can custom build a data-protection system that will ensure that all EHRs are fully protected before and after they are backed up and stored. Nexigen's systems and tools will make sure that all IT systems are protected from outside attacks, viruses, malware and phishing attempts. Nexigen can also provide preventive "medicine" for scanning and risk assessment, ensuring that if or when a system does crash, the cause will be identified and remedied immediately, with no adverse effect for the client or any patients. To guarantee this, Nexigen requires all of its employees to be HIPAA-trained and certified.
- **Data Integration and Protection:** This ties together the second through fifth challenges listed above. Nexigen understands all overarching needs and requirements that must be satisfied in order to run a healthcare business. Chief among this is Nexigen's ability to focus on making sure that its client's systems are always running optimally and securely, which enables the healthcare provider to put its attention where it is needed most – on its patients. Nexigen's staff has also worked closely with and built relationships with the leading EHR companies, including Allscripts, MDI, Nextech and Epic, which puts them firmly on the front lines in the battle to protect sensitive patient information. Regarding actual patient information, Nexigen is able to assist companies who are looking to transition from an outdated system to current hardware/software. This switch can be completed without the healthcare provider experiencing any disruption in service or efficiency. In the end, Nexigen treats every network that it builds like one of its own, with a proactive approach to monitoring, servicing and troubleshooting that is guaranteed to deliver the best network coverage available.

- **Phishing/Spear Phishing:** In order to get into the minds of the devious hackers who wish to disrupt, damage or disable your in-house communication network, Nexigen has conducted simulated phishing attacks that are based on threat intelligence gathered from more than 20,000 email accounts. This has allowed Nexigen to construct reports that offer a real-world view of the level of threat that a healthcare provider's system may be under. To eliminate phishing threats, Nexigen offers a self-service phishing platform with more than 20 built-in templates. This allows for unlimited phishing-prevention campaigns per month, while the Phishing Premium service adds one prevention campaign specific to the organization per month that is created by a Nexigen engineer, in addition to the 20 built-in campaigns.

As a way to tie this all of this together, Nexigen is involved with the Health Collaborative in an advisory role, mainly as a source for Security Incident review and Event Management services. The mission of the Health Collaborative is to bring together the healthcare industry's top minds to find ways to ensure that healthcare providers have the right systems in place so that access to the right information is available in the right place, at the right time, all while keeping said information as secure as possible. The ultimate result will be better care, lower costs and healthier people. In this role, Nexigen works closely with many of the larger hospital networks, as well as many private practices, and in some cases, sits on the board of their IT committees.

Conclusion

Even in an industry as important and potentially vulnerable to attacks from outside actors as the healthcare industry, the first line of defense can be the simplest: practice good IT hygiene, from using strong passwords to doggedly protecting all personal information of staff and patients. But when the inevitable attempted system hack or phishing attack occurs, all healthcare providers must have the most up-to-date IT cybersecurity systems in place. As the complexity of any attacks continues to increase, Nexigen stands ready to assist any healthcare company that must – by law and by ethical demand – protect the sensitive personal information and medical history of each and every one of its patients at all times.

About the Author:

Chris West is the Director of Sales and Marketing for Nexigen and can be reached at (859) 491-6601, ext. 257, or cwest@nexigen.com. Founded in 2003, Nexigen, Newport, KY, is a developer and provider of Security, Managed Services and Cloud Solutions tools and systems that have been designed to optimize Internet Technology operations in the Manufacturing, Legal, Financial Services, Healthcare and Retail industries. For more information on Nexigen, please visit nexigen.com.