Healthcare Data Security: Part II
Embracing change to manage cost and risk in the extended healthcare ecosystem

The healthcare industry—including all partners, suppliers and advisors—is being inundated with new challenges. Meeting the expectations of digitally aware consumers, improving patient care, adopting new medical devices and technologies, and complying with evolving requirements all demand the protection of patient privacy. This paper explores the security challenges that come with these new demands, and the need for new and creative ways to address health cybersecurity and privacy, both inside and outside of the data center.

This is the second paper in a series. The first paper, Healthcare Data Security: Part I, The Problem with the Future is the Past, offers a prescription for improving healthcare data security based on inventorying “protected” data items, conducting a business-oriented risk assessment and developing an iterative action plan.
EXPANDING CYBERSECURITY DEMANDS IN HEALTH

Cybersecurity used to be a computer issue in the data center. Healthcare management was a computer-intensive recordkeeping activity. There was a time when passwords, access controls and encryption pretty much covered the needs of a responsive healthcare cybersecurity program.

Things have changed. Healthcare compliance requirements have extended the concept of maintaining patient privacy to partners and service providers. Electronic medical record creation, storage and transfer have extended the need for security and privacy controls outside the healthcare enterprise, demanding a new set of standards and procedures to protect patient privacy among providers, payers and specialty services. For the most part, such issues can be addressed by continually improving cybersecurity policies and procedures; however, other challenges such as the Internet of Health Things, are not being addressed.

Growing connectivity beyond health system walls

Today’s medical professional is rapidly adopting advanced technology that is expected to both treat patients and maintain data. This technology is designed with built-in Internet connectivity that often is embedded in or placed near patients, not always in a medical facility, creating additional challenges.

Hospitals, clinics and medical facilities are being extended beyond their walls with home diagnostic and treatment capabilities using devices that can be interrogated and programmed remotely for specific purposes. Unfortunately, along with this enhanced connected capability come advanced challenges. Access to these devices and technologies could be gained in a number of ways by unauthorized individuals desiring to disrupt proper operation. Such bad actors could cause device failures or shutdowns. Even more threatening is the potential for introducing program code that purposefully compromises patient privacy, and could even cause physiological harm.

The U.S. Food and Drug Administration (FDA) has been observing that this new medical technology has the option of programmable operation and has published draft guidance for the security of these devices. Their publication, “Postmarket Management of Cybersecurity in Medical Devices,”¹ is an introduction to some guidelines for addressing security in this new area of the healthcare industry.

MEDICAL DEVICE SECURITY REQUIRES A NEW APPROACH

These advancements in medical services can only be successful by addressing cybersecurity concerns in functions that generally are outside the typical focus of data center operations. Device manufacturers will need to apply cybersecurity defense methods in the design and engineering of their components. Purchasers must be able to include an evaluation of how well those providers can protect their equipment from illicit modifications and data privacy loss.

A new cybersecurity awareness discipline is required in the acquisition and deployment of this equipment. Purchasing cannot be based solely on cost or even an investigation of medical performance references. Device security defense and the flexibility to add and enhance protection software and methods must be added to the evaluation criteria.

Operationally, these remote devices do share a common experience with their data center counterparts. There is a need to monitor software and firmware revision levels in the devices and create a program for effective, safe and timely upgrade and patch management. Manufacturers are being called on to incorporate these methods in their product support. Additionally, some of these devices may be “bring your own devices” with fundamental operating systems that cannot be locked down.

Security testing centers offering services along the lines of the National Information Assurance Partnership Common Criteria Evaluation and Validation Scheme are expected to play an important role in validating the cybersecurity performance of these devices.

**SOME SOLUTIONS ARE FREE**

The lessons to be learned from this new industry development are not new. Technology has been and will continue to be important, but so are responsive security procedures. Frequently, the challenge to effective security is not in developing a security defense program, but in making sure it is known and is being used throughout the organization.

Starting with an awareness training program, all staff members should be empowered to recognize security and privacy and make decisions accordingly. This must now include patient care professionals and diagnosticians in new ways.

Purchasing departments can create processes to assign security responsibility to suppliers, who should be expected to demonstrate operations that addresses cyber risk and use industry-approved cybersecurity defense techniques.

Security traditionally includes the attributes of “Confidentiality, Integrity and Availability” but recently has been focused on “Auditability” to demonstrate to regulators that patient safety and privacy is maintained throughout the entire organization, including these new devices. Compliance and regulatory expectations demand that data access and transfer be well defined and documented.

Manufacturers must embed security techniques that are directed to maintain privacy while enhancing patient-to-professional communication. That includes adopting enhanced authentication methods that strengthen the identity of device users and administrators.

**THE BAD GUYS DON’T SLEEP**

What we have learned from the secure data center operation is that operational security monitoring is expected at all times. Threats do not happen only during business hours. With equipment located outside a controlled office or data center environment, the protection of device operations must be built-in, because it cannot be explicitly observed by people.

Some methods that can be used to increase security defense include:

- Advance warning of security attacks: Many attacks start in predictable ways. Being able to observe these activities can raise an alert that an attack is more likely to occur in the near future.

- Monitoring for deviations. Viewing transactions, deviations from typical locations, transaction types, volumes and content can cause an investigation of the potential for rogue devices, altered operation or a malfunction.

New technology asserts that secure healthcare services are not just local issues—they must match the expectation of the medical profession itself connected to everything, everywhere.

**CONCLUSION**

Healthcare enterprises must address cybersecurity both in and out of the data center. Redeveloping policies and procedures to be security and privacy focused, redefining supplier agreements, and creating an environment where everyone is focused on looking out for protecting private patient information is a good start. Within the data center and in applications, the future will require creating an environment that facilitates dependable and efficient authentication, safe and secure information transfer supporting privacy preservation, provides for collaboration and communication between providers and patients, and expands the core data center services with effective privacy and security monitoring services that widen both the covered geography and the schedule of vigilance.