LOCK DOWN mHealth Security

Don't make mobile security more complex than it needs to be. Focus on risk assessment and your overall security architecture to limit your exposure.

By Ken Congdon, Editor in Chief

According to a 2013 HIMSS Leadership Survey, securing health information on mobile devices is the top security concern among healthcare providers. Millions of dollars are being sunk into this endeavor annually, and the sad truth is that many of these efforts will be to no avail. The reality is that no hospital can say its PHI is 100 percent secure (whether the data is on a mobile device or not), and it's likely that no one will ever be able to make this claim. Chasing this goal is the equivalent of Don Quixote charging windmills. This fact isn't unique to healthcare. On the contrary, it's a truth for every industry. If somebody wants something bad enough (PHI is no exception), they'll find a way to get it. After all, this is why banks install sophisticated alarm systems in addition to their safes. A safe can only protect a bank to a point. Once its security is breached, law enforcement needs to be called in.

This brutal honesty is not meant to create an air of futility. Hopefully, it will have the opposite effect and inspire providers to look at the mobile security problem in a different way. Perhaps by accepting this sobering reality, providers will stop trying to find the elusive "magic bullet" to their mobile security issues and place the focus squarely where it needs to be — on security fundamentals, architecture, and effective risk management.

Focus is something many health providers clearly don't have today. "A lot of health providers are currently employing a wide variety of methodologies in an effort to secure PHI on mobile devices," says Mark Kadrich, author of *Endpoint Security* and former principal security architect of a leading health provider organization. "This is introducing more complexity and unknowns into the process. As a result, most of these organizations can't effectively demonstrate how secure their data is."

For Kadrich, being able to demonstrate how your security architecture works is a key step in winning the mobile PHI battle. However, equally important is ensuring you can defend and protect yourself in the event it fails. You need to have a solid plan in place to react to security breaches quickly and limit the associated damage.

Regulatory, Technology Challenges Impede mHealth Security Progress

While no industry can claim that its data is 100 percent secure, the security situation is definitely more dire in healthcare than it is in other markets. The severity of the situation is illustrated by numerous studies, including a 2013 survey by the Ponemon Institute showing that medical identity theft increased 20 percent in 2012, affecting more than 2 million people. This growing problem is perpetuated when PHI falls into the wrong hands, and the prevalence of mobile health technology only makes this scenario more probable.

There are other factors at play in healthcare that make mobile data security such a difficult proposition. For example, after years of sitting idle, healthcare providers have suddenly been thrust into an era of rapid IT adoption and implementation. With initiatives like Meaningful Use (MU) in play, providers feel increasing pressure to install technology in an effort to improve the quality and cost of care. Moreover, they're doing this in an increasingly hostile regulatory environment.

Ed Ricks, VP of information services and CIO at Beaufort Memorial Hospital, is one healthcare leader who is understandably confused by this juxtaposition. "I think

providers are getting mixed signals from programs like MU and regulations like HIPAA," he says. "On one hand, MU incentivizes us to share patient data, but HIPAA places complicated restrictions on exactly how this data can be shared. It's confusing to navigate this environment, particularly from a mobile security perspective. We feel like we're trying to do all the right things security wise, yet I feel our data isn't as secure as it should or could be. This isn't from lack of effort, but rather from a lack of understanding of what the acceptable practices are and how to apply the right technology to help."

Kadrich points out another, more troubling, contradiction playing out in healthcare. "Health providers today are basically trying to plug new innovative mobile technologies and devices into legacy architectures that can't support the effective protection of information in a mobile environment," he says. "Most providers aren't taking all the elements of a mobile infrastructure — the network, the cloud, and mobile technologies — and combining them to create an environment that protects the data. Instead, they are largely relying on vendors to solve this problem for them."

Kadrich also explains how certain regulatory organizations can actually serve to impede progress in the area of mobile security. For example, several state regulatory bodies (e.g., OSHPD [Office of Statewide Health Planning and Development]) require a hospital to go through a lengthy review process before making any configurations to their network. This flies in the face of a mobile technology sector that is ever changing. Providers may need to upgrade their mobile technology every few months in order to stay relevant. The inability of network changes to be made at the pace necessary to accommodate these mobility enhancements can create a huge problem. In short, it may force hospitals to invest in mobile technology that is already obsolete by the time they are given the green light to make the required network adjustments.

How Real Is The Threat?

Several other characteristics make healthcare providers particularly attractive targets for hackers and other cybercriminals. For example, health provider security departments are often under-staffed relative to other industries. Case in point — Ed Ricks also serves as the de facto CSO for Beaufort Memorial Hospital even though he doesn't have the credentials for that role. Furthermore, hospitals and other clinical facilities are difficult to defend because of the complex systems in play (e.g., EHRs, etc.) and the wide array of people (e.g., clinicians, patients, payers, etc.) who need to access the health data contained on the network — access which is often facilitated via third-party portals.

According to Kadrich, the one saving grace for the healthcare industry is that cybercriminals have yet to figure out a way to effectively monetize healthcare records and the PHI they contain. "When and if the criminal industry identifies how to make easy money from healthcare records, many providers will face major disaster," he says. "Today, the main threat to PHI comes from the inside — an employee or contracted worker who accesses the network and uses the resources it contains to benefit an entity other than the provider organization and its patients."

Assess Your Risk

While the challenges in healthcare are daunting, there are several mobile security steps your organization should take to ensure it isn't an easy target for a data breach. The first is to ensure you are assessing and managing risk effectively.

For example, Beaufort Memorial hires an outside vendor to conduct an independent risk assessment and security audit annually. The hospital also conducts its own internal assessments every quarter. During these audits, Ricks and his team review the hospital's security systems and practices from an ISO standards perspective. They also take HIPAA regulations and their own internal policies into account. Through this exercise, Beaufort is able to identify its security vulnerabilities and the severity of each. Every threat identified is assigned a score of 1 to 5 to illustrate the likelihood of an adverse event occurring (5 being most likely to occur), and another score of 1 to 5 to denote how bad the consequences would be if that event did occur (5 being catastrophic). These two numbers are then multiplied together to generate an overall score of 1 to 25. Ricks and his team then prioritize these threats (with those scoring closest to 25 topping the list) and present them to the hospital board. The board and the IT team then work together to determine how to address each threat. Can the biggest threats be addressed with education and policy, or is technology required? Can Beaufort afford to fix this problem immediately, or is it something that requires a long-term plan to correct?

"Truly understanding your risk is the first step to improving security," says Ricks. "We know we have vulnerabilities, but we're not afraid to face this reality. In the end, it gives us the knowledge and power to strengthen our overall security position. Some providers choose not to search for their vulnerabilities. They like to believe they have no weaknesses. These providers are fooling themselves and putting their health data at risk."

Many of Beaufort's most notable mobile security initiatives to date

were a direct result of the risk assessments it conducted. For example, early on, these audits alerted the provider to several unencrypted drives on corporate laptops and other mobile devices. In response, Beaufort invested in mobile encryption technology and reinforced its policies regarding this practice. Similarly, risk assessments made the hospital aware of security issues resulting from clinicians ineffectively managing multiple system passwords. In response, Beaufort implemented a single-sign on solution that allows clinicians to use one intricate password to access all hospital systems — even from mobile devices. A secure texting solution was another investment spurred by a risk assessment that enlightened Beaufort to the dangers of uncontrolled text messaging in a clinical environment. Lastly, the provider is currently evaluating a mobile virtualization solution that allows clinicians to access hospital systems via a virtual desktop on a mobile device. Using this tool will significantly reduce the amount of health data that is stored on mobile devices — a key vulnerability identified by (you guessed it) a risk assessment.

Focus On The PHI, Not The Device

The security steps taken by Beaufort Memorial thus far may seem basic to many healthcare providers. Indeed, many of them are fundamental practices, and there are other "no brainer" security procedures all providers should implement when leveraging mobile devices. These include (but aren't limited to) enforcing password/lock screen protection on all smartphones and tablets used to access PHI, providing IT personnel with the ability to remotely wipe mobile devices in use at a healthcare facility, effective inventory management of the mobile devices accessing a healthcare network, and sound mobile antivirus and malware protection.

As important as these steps are, it's equally important to realize that simply trying to cobble together a bunch of one-off technology solutions to address these needs will not provide you with a secure mobile environment. Moreover, the added element of mobility to the healthcare ecosystem has led many providers to mistakenly focus their mobile security efforts on the devices as opposed to where it actually belongs — the PHI itself. A mobile health security initiative needs to be treated as part of the overall enterprise security strategy and administered in a fashion similar to the rest of the infrastructure. A mobile device should be viewed as just another endpoint on the network.

"Healthcare security departments that are spending so much time worrying about the security of individual mobile devices are actually spending a huge amount of time and money chasing a very small problem," says Kadrich. "The reason I say it's a small problem is because if they have security in depth, the fact that one tablet is trying to access 10,000 records should raise a big red flag. There should be a system of controls in place that works to prevent this activity and protect the data."

Kadrich urges providers not to look at mobility as an individual piece of technology but as part of an architecture or a "system of systems." Moreover, he challenges hospital leaders to demand that their security leaders be able to demonstrate how their organization's security architecture works.

"Your security or IT staff shouldn't defer to vendors when describing your security architecture," says Kadrich. "They need to be able to articulate or diagram how it works. How do you detect threats? How are those threats identified? How are they mitigated? What pieces of technology support these efforts? Security is not some mystic art. It is a very well-grounded engineering discipline that should elicit a factual answer in response to these questions. If your IT department can't prove how your overall architecture is secure, use mobile technology at your own risk."

A final piece of advice from Kadrich is for healthcare providers to stop taking their security cues from the financial industry. "Finance is an industry that believes $5 to $8 billion in loss per year is acceptable," he says. "It incorporates failure and recovery models that don't apply to healthcare. For example, when a credit card is lost or stolen, the user is issued a new card and fraudulent charges are wiped from their account. Healthcare doesn't have this luxury. When a health record is leaked and used for nefarious purposes, it's not like we can issue a patient a new health record and forget about the old one. Health providers need to assess their security architectures from their industry perspective and stop copying the failed approach of the financial industry."