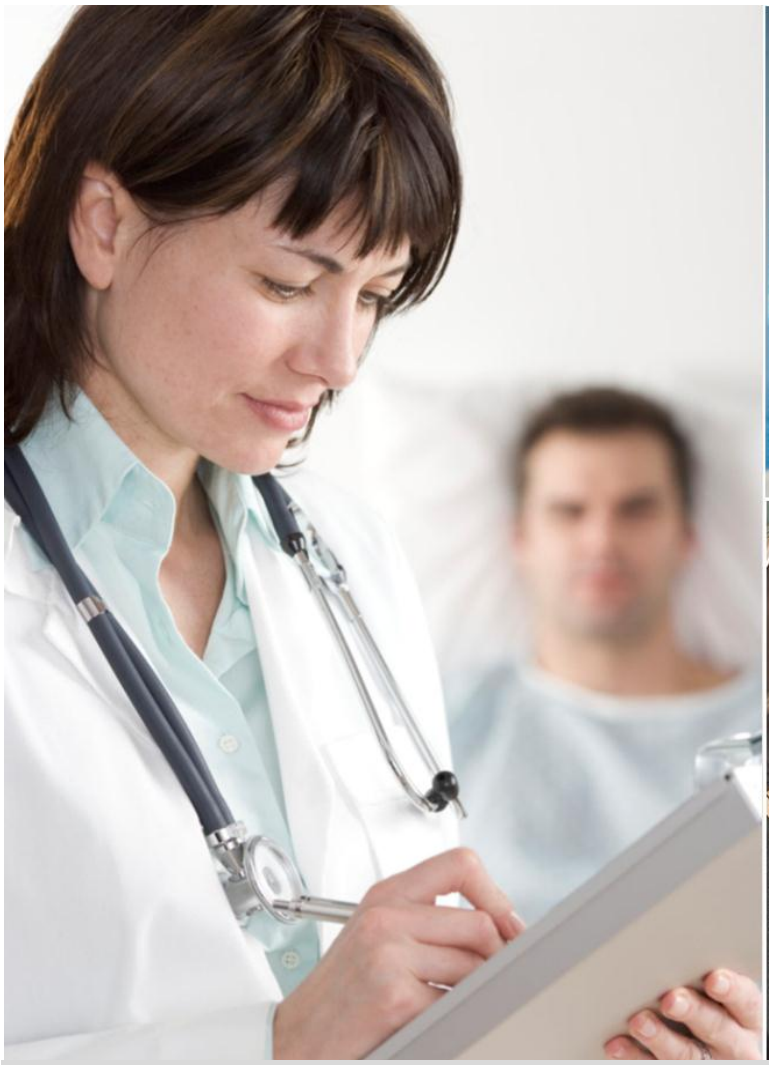
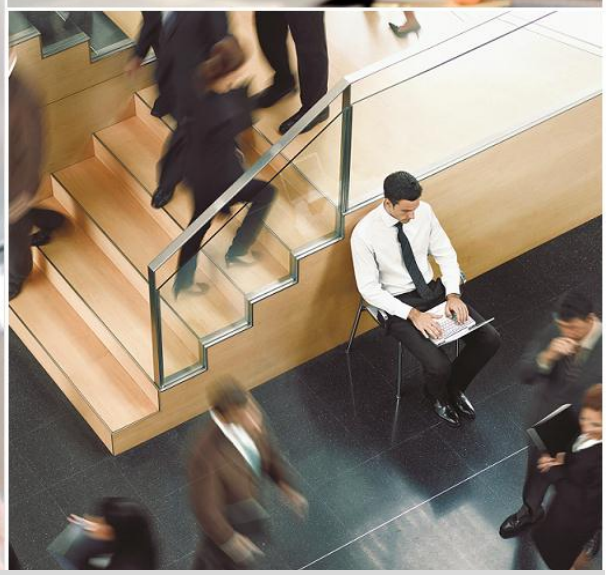
Making Mobility Matter in Healthcare Data Security

Four Critical Tactics





Security in Transition

Executive Summary

Mobile device usage in healthcare facilities has increased significantly in recent years, with more than 2 out of 5 physicians already using a smartphone or tablet during patient consultations. The potential benefits to adoption of these devices are compelling, including facilitation of patient involvement in the care process, as well as increased efficiencies and cost savings for the organization.

However, mobile device usage is also fraught with risks that must be carefully managed to avoid penalties and damaged reputation from breaches of Protected Health Information (PHI).

With a strong demand from clinicians to use personal devices in the workplace, concerns around how to track, encrypt, and manage these devices must be balanced with processes for how they are governed, and ensure that the balance is justified by enhanced productivity of clinicians and the organization as a whole.

Introduction: How We Got Here

Simultaneous with the expected growth of electronic health records (EHR) is the fierce emergence of mobile devices such as smart phones and tablet PCs. The proliferation of such tools indicates that many of the "test flights" for EMRs will be driven by these devices, which combine potential improvements with new risks.

Overall, the healthcare computing environment has grown by leaps and bounds since the advent of paper medical records. And although electronic medical records have been in existence for quite a while, these technologies still haven't been widely adopted. This is partly because the core goal of healthcare is patient care, in terms of outcomes, and not about accessibility of data, although it is becoming apparent that these two realities are converging and rapidly changing and refining the guidelines around adoption of these technologies.

The healthcare industry is now seeing increasing adoption of electronic records. However, the widespread use of portable media, smartphones, and tablet computers creates an urgent need for attention to how and where sensitive data is sent within (and outside of) the provider's networks. A changing relationship with how and where physicians, clinicians, insurers, and billers access information is complicating the list of vulnerabilities that providers face. Handheld devices are particularly notable because these devices put more power in the palm of the hand today than an entire rack of servers had just two decades ago. And clinicians have taken notice: 72 percent of U.S. physicians now use smartphones, up from just 30 percent of physicians in 2001.[1] In addition, some 39 percent of Chief Medical Information Officers have rolled out mobile computers or handhelds at their facilities,[2] and 86 percent of physicians express that their top interest in mobile technology is for accessing electronic medical records.[3]

In the future, Health Information Exchanges and Accountable Care Organizations will require even more open data and connectivity between existing and incumbent systems, creating additional complications for authenticating, encrypting, and protecting sensitive electronic Protected Health Information (ePHI). The big evolution here is that information formerly existed in silos and single locations. But when viewed across the trajectory of what's happened in healthcare in recent years (Figure 1), it is clear that not only is information consumption increasing in complexity as healthcare organizations become more mobile, but the desire and requirements to share information across

[1] Manhattan Research, "Taking the Pulse" Research Report 2011.
[2] http://mobihealthnews.com/7985/cmios-39-percent-have-installed-mobile-devices/
[3] PricewaterhouseCoopers Health Research Institute report: "Healthcare Unwired," September 2010.

enterprises make it imperative to balance security and privacy with aggregation, collaboration, and interoperability to improve quality and reduce costs.

Figure 1: The Evolution of Patient Data

A Speeding Train toward Adoption of Mobile Devices

If anything, data usage, storage, and transfer will become more complex in the years ahead. Total healthcare providers' expenditure on IT solutions is expected to increase by almost 45 percent in the next three years (reaching almost $7 billion in 2014),[4] while at the same time, the mobile device market is projected to increase *1600* percent, to $1.7 billion by 2014.[5] There is therefore a coming explosion of mobile device usage – in 2011 total US hospital IT spending was 47 times greater than the mobile market in healthcare, whereas in 2014 (a three-year projection), it is expected to be only four times the mobile market. This indicates that mobile devices are catching up rapidly with, and even potentially crowding out the usage of many traditional modalities of hospital data usage. This trend highlights the inevitable conclusion that mobile devices are taking over in the healthcare field as a driving force in data exchange.

Already in the U.S., more than one-third of physicians use their mobile devices to input data into the EHR during patient encounters, while the information is still active.[6] And with these mobile devices, there are clear preferences around platforms.

But most of the providers and even physicians using this technology recognize the risks. In a 2010 PricewaterhouseCoopers survey, when asked about barriers to adopting mobile health solutions, "worry about privacy and security" was the top answer, with one-third of primary care providers and 41 percent of specialists.[7]

Boot the Box

Healthcare facilities today support hundreds, or even thousands of desktop computers. Most of these are large, stationary form factor devices. These systems are regularly accessed by multiple practitioners in a day and are frequently left unattended with patients and visitors, creating a significant risk. With mobile devices assigned to each user, the total number of devices required to provide patient care decreases. So, while the use of mobile devices may not be the replacement for all aspects of our healthcare applications and systems today, many applications and uses can be accommodated on these devices.

From a cost perspective, there are also clear benefits to mobile computing. With mobile computing, healthcare organizations can reduce the number of devices needed and thus bring down costs, as well as reduce maintenance and training costs through potential familiarity with the device if it is one that the clinician has brought from home.

Therefore, despite all the prominent "doom and gloom" in the media, the benefits of enabling a secure mobile device platform are clear. For the patient, several obvious benefits exist. The mobile device has become the interface to many different types of equipment, such as radiology stations,

[4] http://www.ihealthbeat.org/articles/2009/6/5/hospital-health-it-spending-ehr-market-to-grow-reports-say.aspx
[5] http://mobihealthnews.com/9581/by-2014-1-7b-market-for-mobile-apps-in-healthcare-enterprise/
[6] http://www.mdnews.com/news/2011_07/mobile-devices-pose-new-security
[7] PricewaterhouseCoopers Health Research Institute report: "Healthcare Unwired," September 2010.

paper charting, nursing desktop computers, biotelemetry monitors, dictation stations, and prescription pads. Mobile devices create more free space, less clutter and lower costs, while delivering more services more efficiently, with a lower error rate, and efficiencies through linking with electronic health systems. They can also enable real-time visibility into the patient's condition, and potentially increase a patient's participation in their own healthcare by increasing the possibilities for more interactive patient-physician encounters.

Under Attack

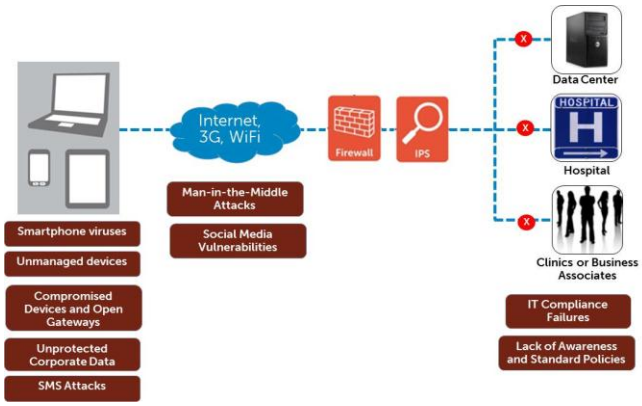
Healthcare organizations are under attack. Nearly one out of every seven data breaches that occurred in 2009 was targeted at the healthcare industry, according to the Open Security Foundation.[8] In a survey conducted by PricewaterhouseCoopers of healthcare institutions in 2011, 54 percent of the respondents reported at least one security issue in the last two years, while the other 46 percent couldn't determine whether they had been breached.[9] For the period from August 2009 through December 2010, the records of more than six million patients were compromised. As of September 2011, that number has risen to eleven million already (since 2008).[10] This dramatic increase is mirrored by the number of people affected per incident – according to HHS as recently as of June 2011, 48,000 people are now affected on average per breach; which could indicate that more data is being stored and transferred onto individual devices, which makes encryption and a security strategy more imperative.

In reality, the actual number of records breached is likely far higher than six million in the 2009-2010 period, since only those incidents affecting greater than 500 people are required to report their incidents to HHS. It is therefore not surprising that all the combined causes of breach create an annual economic burden to US hospitals of $6 billion.[11]

65 percent of these breaches occurred on laptops and mobile devices, with approximately 57 percent of the incidents due to theft. Storing data on mobile devices rather than on a centralized repository, and allowing data transfer to those disparate devices, sets up the organization for difficulty in tracking usage of and access to these devices, who has what kind of information where, and ultimately leaves these endpoints vulnerable to a HIPAA Security Rule violation. Providers need to have a solid and clear strategy for role-based logins, and store data in a central location (instead of the endpoints) in order to mitigate this risk effectively, as well as have a clear assessment of the risk and a mitigation plan in place.

"Mal-Content"

Smartphones and tablets can be the easiest and most efficient ways for a hacker to gain control of a network. According to McAfee security, the number of total pieces of mobile malware grew by 46 percent in 2010, much of it on the Nokia Symbian and Google's Android operating systems. Compared to operating systems such as Windows and Linux, smartphones currently lack as robust an operating system; so protecting these devices is more difficult since they have fewer APIs and functionality – which makes it much easier for attackers to get what they want from them.



[8] http://www.healthcaretechnologyonline.com/article.mvc/PHI-5-Important-Guidelines-For-Avoiding-0002

[9] PwC Health Research Institute, "Old Data Learns New Tricks" September 2011

[10] http://www.redspin.com/blog/2011/07/01/preventing-a-healthcare-data-breach-epidemic/

[11] http://www.experian.com/data-breach/healthcare-data-breach.html

Figure 2: Security Issues Prevalent on Mobile Device Networks

Risky Business

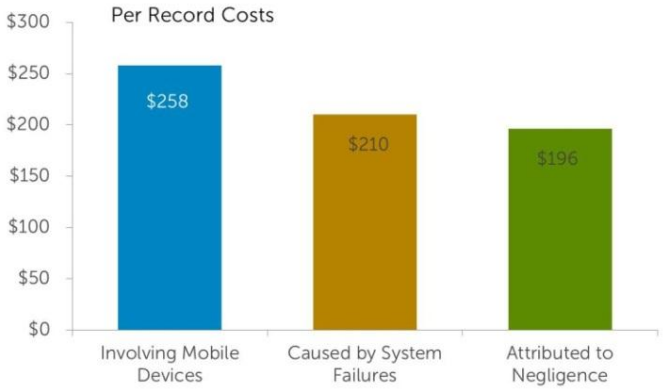
In a well-publicized example, the loss of a BlackBerry containing unencrypted patient data occurred in 2010 at SunBridge Health Corporation, involving eight nursing centers, and included current and former residents' names, dates of birth, medical record numbers, dates of service and clinical data. The breach affected around 1,000 individuals, and lasted for six months before all the damage was rectified. In this instance, the devices were not encrypted.[12]

Today, many of the well-publicized data breach headlines relate to laptops. However, usage of smartphones and tablets are set to far advance laptops in usage for healthcare purposes, since advances in mobile technology has led to the wider adoption of those devices. And as they replace the laptop as the device of choice for many mobile workers, we are likely to see many more headlines of data breaches.

In many cases, both employees and patients can use unsecured personal devices to carry or access health information (the so-called "bring-your-own-device," or BYOD movement), which brings into question the ability to consistently maintain encryption, and track access to appropriate data. The unforeseen consequences from this can be significant. In recent months for instance, a US health insurance firm lost 1.5 million clients' medical records on an unencrypted portable drive. This decision to save money on encryption expenses resulted in $250,000 fielding lawsuits, more than $319,000 in letters to the affected clients, and $1 million for ID theft monitoring services to the victims.[13]

According to a recent PricewaterhouseCoopers report, US federal and state regulators are aggressively inspecting and pursuing privacy breaches and the absence or failure of data safeguards.[14] For the federal government, the revenue gained from the penalties levied on these breaches is an opportunity to help fund the stimulus money for its EHR adoption program and meeting the Meaningful Use guidelines. In this same study, more than 70 percent of executives polled said that recent breach enforcement has prompted them to place more focus on privacy. In all, almost 290 breaches have been reported to the Office of Civil Rights in the last two years.

The damage from breaches due to mobile devices also costs the most to repair. A standard USB drive can store more than 25,000 medical records, and losing just one such device can cost an organization more than $5.7 million in breach mitigation costs, with the national average for a breach standing at almost $7 million.[15] On average, each record breached involving a mobile device can amount to $258 in mitigation costs, which is higher than the costs associated with other breach causes (Figure 3).[16] When considered in the context that hard drives can carry and manage more data with each passing year, there is a clear imperative to implement a strategy for each and every device that touches the organization's network.



[12] http://www.phiprivacy.net/?p=3690
[13] http://www.forbes.com/sites/dell/2011/09/22/mobile-devices-in-healthcare/

[14] PwC Health Research Institute, "Old Data Learns New Tricks" September 2011
[15] http://www.forbes.com/sites/dell/2011/09/22/mobile-devices-in-healthcare/; SecureWorks research.
[16] HITRUST Alliance: "An Analysis of Breaches Affecting 500 or More Individuals in Healthcare"

Figure 3: Breach Costs

Mitigating the Risk

There are a number of steps that need to be taken to guard against all the major types of attacks, but it can be done with the right visibility of your risk across the key areas of usage, and the system state of your network connectivity. Limiting employees' exposure to social networking sites, performing DLP storage assessments to understand where key data resides; reviewing the organization's governance requirements for data; securing mobile device development tools; and creating and enforcing portable media and device access policies are all going to be important measures as part of the overall strategy.

To fully manage security in a mobile environment, your organization will need to ask itself several key questions to gain insight into who is accessing your data, what types of controls are in place; and consider information security best practices as a part of the overall mobile technology and security strategy. For instance, both enterprise-integrated mobile devices and employee- or patient-owned mobile devices need to be as secure as possible with identity authentication, encryption, tracking and trace software, anti-malware, backup and extensive monitoring.

Access controls are critical to keeping data safe in the mobile environment. The original HIPAA rule called for granting role-based access procedures. But as mobile device usage has required identities and privileges to be stored in multiple applications and repositories across the enterprise, many current systems may have deficiencies in this area. What's needed is a centralized and comprehensive view of people, views, roles, and privileges to fully enable more accurate and efficient auditing and reporting. There are several key areas that deserve focus, including:

- How do you protect data as it moves further outside the network perimeter?
- What are the best practices for handling the growing diversity of mobile platforms and applications that are being introduced?
- How do you strike the best balance of allowing healthcare executives to access critical data on-demand on their tablet or smartphone, yet still maintain minimal risk?

Four key tactics that Dell SecureWorks advocates addressing as part of a comprehensive mobile device security program to reduce the risks include:

1. Mobile Security Strategy and Roadmap

Organizations need to comprehensively assess their approach to security on mobile devices, and leverage well-tested methodologies to examine how they plan to move forward, how mobility will be a part of that strategic direction and how security should be considered and integrated to support the business. The output of this exercise should be a strategic plan and roadmap to help drive organizational decisions about mobility and security.

The focus here should be on the areas most important for your environment and needs, and should result in an understanding of anticipated investment, areas of opportunity, and cost.

2. Mobile Device Use Risk Assessment

Organizations that need a more granular analysis of a particular mobile solution should examine mobile device use cases, correlate these to data and system access, and assess the security and compliance risk to the organization. This exercise is especially useful for organizations that want to determine the full costs and risks of using mobile devices.

Regulations such as HIPAA, HITECH, and Meaningful Use impose security and privacy controls and objectives. For this reason, understanding the risks posed by the use of mobile devices and applications is key to understanding an organization's compliance posture. In fact, a risk assessment is a primary requirement to meet the

Meaningful Use guidelines and gain the associated incentive payouts while avoiding penalties.

Another common scenario for a mobile device use risk assessment is when moving from one smartphone platform or ownership model to another: e.g., moving from corporate-provided Blackberry devices to a "bring your own" approach which will require supporting Android, Windows, Apple and Blackberry platforms. This is increasingly common as more individuals own smart phones and want to use their device (BYOD) to access corporate resources, rather than carrying two separate devices. Many organizations are exploring BYOD as a means of reducing telephony costs, and those organizations in regulated industries are willing to spend upfront to ensure this approach does not introduce greater liability under their compliance mandates.

3. Mobile Application Security Assessment

Application testing should combine both automated and manual methods to probe for known vulnerabilities and undiscovered exposures. Specific techniques will vary based on mobile platform, purpose of the application(s), coding practices and quality of the application(s), and the unique deployment environment.

This assessment is typically a holistic and prioritized approach to testing mobile applications which reduces your overall risks and associated remediation costs. A sound methodology is to examine the security and compliance risks of the entire mobile application, its associated systems and the interactions and data flows between them.

4. Data Protection and Encryption

Insider threats are one of the primary concerns for healthcare institutions. End-to-end encryption processes, products and services, rather than a piecemeal approach, are essential to address issues such as celebrity and neighbor snooping.

Enabling encryption for PHI stored on laptops, USB thumb drives, external storage devices, and other mobile devices helps the organization to minimize downtime, and further mitigate the risk of breaches. A robust solution should protect PHI on multi-user devices without impacting ease of access; prevent users from storing data in unencrypted locations; and maintain confidentiality, privacy and auditing of data on any endpoint, as well as easily allow generation of HIPAA and HITECH reports.

A policy-driven protection solution that can be supported seamlessly in any environment can help limit access to non-authorized users. Comprehensive encryption solutions can also lead to fewer system errors across the infrastructure, and lower the risk of losing data during transfer.

Conclusion

Mobile devices are clearly making an impact on the exchange of healthcare data exchange as they continue to be adopted in various form factors at a rapid pace. However, breaches on these devices have increased, and they pose special risks to PHI. In order to remain compliant and maintain a scalable security posture, healthcare organizations need to assess their unique risks and ensure that encryption procedures, policies, and controls are in place to reduce these risks.

For more information about Dell SecureWorks, visit www.secureworks.com