# Managing Information Security and Compliance in a Healthcare Environment

## White Paper

By: Kevin Beaver, CISSP

August 2012

WINMAGIC® DATA SECURITY

HIMSS® Gold CORPORATE Member

## Contents

## Summary

This whitepaper discusses the current state of information security and compliance in the healthcare industry along with the cultural and political challenges associated with mobile computing.

The reality you face in healthcare is that sensitive electronic information is everywhere – especially on your laptops and mobile storage devices. When these systems are lost, stolen or otherwise mishandled the tangible and intangible costs to your healthcare business can be enormous. According to the *2012 HIMSS Analytics Report: Security of Patient Data* (*http://www.krollcybersecurity.com/media/Kroll-HIMSS_2012_-_Security_of_Patient_Data_040912.pdf*), 27 percent of respondents had a security breach in the past 12 months with 69 percent reporting more than one breach. Whether you work for a healthcare provider or nay of the numerous other entities and business associates working in and around the healthcare industry, one seemingly small mishap can create big problems with the business.

It's critical to understand what there is to lose *before* a mobile security breach occurs. The ultimate goal is not about completely eliminating mobile security risks but rather having the proper systems in place to minimize the impact when breaches occur. Well thought out controls involving proven security technologies combined with the proper documentation and business processes are essential. Not only are these requirements of the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH) Act, they're simply smart ways to approach mobile computing in business today.

Be it for healthcare industry compliance or overall information risk management, read on for some practical and proven ways to gain control of your laptops and mobile storage devices once and for all.

## Introduction

The healthcare industry is currently undergoing many changes. Not only is medicine advancing but so is the information technology that serves as the underpinning of healthcare delivery. In the United States alone, the Department of Health and Human Services Medicare and Medicaid EHR Incentive Program is providing massive taxpayer funding to bring 21st century technologies to the healthcare industry – up to $27 billion dollars over 10 years. Such growth in social programs around the world combined with the advancement in IT and electronic health records (EHRs) is leading to numerous complexities especially when it comes to the mobile workforce.

From remote access to professional collaboration to telemedicine, the case for mobility in and around healthcare delivery is obvious. What's not so obvious – and continues to not get the attention it deserves – are the information security issues associated with mobile computing in healthcare. In fact, the desire for mobility often outweighs the potential security consequences. This approach leads to laptops and other mobile devices getting lost, stolen or otherwise mishandled. Subsequently data breaches occur.

Electronic information is everywhere – often in more than one place at the same time – and the mobility factor has made it increasingly difficult to keep sensitive healthcare information under wraps. Furthermore, consumerization – the issue of computing devices becoming ubiquitous with users calling the shots coming and going as they please – is here to stay. What started with basic Internet access evolved into technologies such as instant messaging and wireless networks has now become the era of mobile computing. We're now two decades into educating users what they can and cannot do with their computers but we haven't been all that successful. Whether network managers like it or not this battle is far from being over.

> If we aren't able gain some semblance of control and set everyone up for success, mobile systems and the sensitive information they house could be the greatest IT challenge ever for businesses operating in the healthcare industry.

We have to embrace the reality that users are extending the security perimeter beyond its traditional boundaries – way beyond. We must assume that sensitive information will be put at risk. We must also ensure the proper controls are in place to minimize the impact when a mobile security breach does occur.

## Current State of Compliance and Security in Healthcare

In any given part of the world – the U.S., Canada and other developed countries – one of the greatest challenges for businesses in the healthcare industry is ensuring compliance with privacy and security regulations. From HIPAA and the HITECH Act in the U.S. to PIPEDA in Canada and beyond, healthcare providers have an enormous government compliance burden. The 2012 updates to HIPAA/HITECH dubbed "Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules" (http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/nprmhitech.pdf) bring even tighter privacy and security controls to the healthcare industry in the U.S. Whether or not you're in support of such governance, the reality is these laws exist and will continue to evolve with new federal, state and provincial regulations. There's simply too much at stake when it comes to the protection of personal health information.

Even with broad regulation, many organizations in the healthcare are still struggling with tightening down their security controls and are thus experiencing breaches in great numbers. The numbers say it all. As per the HITECH Act, the U.S. Department of Health and Human Services maintains a database of breaches affecting 500 or more individuals (www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html). Theft and loss of laptops and mobile devices comprise the majority of the breaches listed. According to the Identity Theft Resource Center *2012 Data Breach Stats Report* (http://www.idtheftcenter.org/ITRC%20Breach%20Stats%20Report%202012.pdf), medical/healthcare breaches accounted for 28% of all breaches – up from 20.5% in 2011. The findings of the Privacy Rights Clearinghouse *Chronology of Data Breaches* (http://www.privacyrights.org/data-breach) underscore this problem: over 6 million compromised records due to mobile security breaches since 2011.

Based on what I see in my work, the headlines and data breach statistics only paint part of the picture. There are untold numbers of hack attacks, employee breaches and similar incidents that require forensic analysis and information security expertise that we don't hear about. Imagine what's *really* taking place behind the scenes.

We've already seen 435 breaches of personal health information impacting more than million individual records since 2009. Clearly the message needs to be conveyed that we are at a critical crossroads in the protection of medical data.

The importance of mobile security is directly related to compliance and successful information risk management overall. In fact, mobile devices pose one of the greatest information risks in any given healthcare organization today. Figure 1 outlines mobile data breach scenarios that can impact your organization regardless of its size.


*Figure 1 – Mobile data breaches can occur through various scenarios*

Such breaches can be intentional or unintentional and brought about by an insider or external attacker. Regardless of how it occurs, it's still a breach that your organization doesn't need. Exacerbating the problem is the fact that so much sensitive healthcare information is stored on laptops and mobile storage devices (external hard drives, thumb drives, etc.) making it difficult to

know what's where at any given time. Your mobile devices represent literally hundreds, often thousands, of islands of information scattered about. Understanding how this information is protected – or at risk – can be very difficult if you don't have the proper operational and technical controls in place.

Not surprisingly, the consequences of lax security and non-compliance are much greater than the actual costs of keeping things in check. In fact, the 2011 Ponemon Institute study *The True Cost of Compliance* (www.tripwire.com/ponemon-cost-of-compliance/pressKit/True_Cost_of_Compliance_Report.pdf) found that the cost of non-compliance is, on average, 2.65 times greater than the cost of compliance. For example, if security and privacy compliance costs for a hospital are, say, $2 million per year, the cost of non-compliance could reach $5.3 million in the same organization. Interestingly, the compliance cost per capita for organizations with between 1,000 and 5,000 employees is $459. The cost per capita for *non-compliance*: $2,151.

The Ponemon Institute study also found that the smaller the gap between compliance and non-compliance costs resulted in a lower occurrence of data breaches over a given 12 month period. Furthermore, organizations that do not perform compliance audits experience the highest compliance costs. That's no surprise but it is interesting to note the number of organizations that choose to forgo compliance audits altogether – a full 28 percent of respondents. Furthermore, this study found that businesses in the healthcare industry ranked among the worst in security effectiveness.

The math speaks for itself: get on board with compliance and keep things in check or your organization can end up paying that much more several times over.

## IT Challenges in Healthcare Environments

Even with compliance requirements, enormous losses and the associated fines, mobile security in healthcare settings is often ignored in the name of culture, politics and budget. This largely stems from the heterogeneous nature of IT environments in healthcare settings. In any given scenario, there are numerous organizations (hospitals, physician's offices, insurance companies, etc.) working together to get things done. An unintended consequence is the complexity of the associated business processes and computer networks.

> Complexity is the enemy of security and compliance. The more complex the environment - especially when it involves mobile computing - the greater the chances of things going awry.

Hospitals have a highly-mobile workforce combined with physical security weaknesses and a general lack of accountability given how many people are involved with delivering services. This section of the healthcare workforce being on the move – often without a main home base – further undermines security-related accountability. Related factors include physicians' practices having minimal IT knowledge and support and business associates and third-party service providers who many not have the same buy-in and understanding of what's at risk and the associated consequences of a breach. Insurance companies have application, systems and business process complexities – many of which are brought on by antiquated systems – which create further challenges to security and compliance. Combine all of these issues together into the industry as a whole and it's easy to see why healthcare-centric businesses have a long road ahead of them.

Not only is there an overarching problem with mobile security and compliance, the basic foundation that's needed to build a set of reasonable defenses is often missing. Common issues include those shown in Figure 2:


*Figure 2 – Underlying business issues create mobile security and compliance gaffes in healthcare*

A primary contributor to mobile security issues in healthcare is that many in management understand the concept and the need for security and compliance but they often don't understand the true impact of mobile breaches. This leads to budget constraints, lack of awareness and user buy-in and so on. The cycle of mobile risks continues.

One final issue that's somewhat unique to the healthcare industry is that it's easy to get caught up in the compliance hype and miss the big picture of what these regulations are trying to accomplish. This can be bad for business especially given the investment of time, effort and money that's required long term. Mobile security and, more importantly,

**What is there to lose?**

When a laptop is lost or stolen, the cost to the business is more than just replacement value and the hassle of cleaning things up. There are numerous costs including:

- Legal fees
- Forensic investigation fees
- Fines
- System outages and lost opportunities
- Damage to brand and reputation (i.e. the Sony Online Entertainment and PlayStation Network security breach in 2011) and subsequent loss of trust

These costs can be enormous given what's at stake. For instance, the Ponemon Institute documented in its benchmark study *The Cost of a Lost Laptop* that the average value of a single lost laptop is $49,246.

In the Ponemon Institute's *The Billion Dollar Lost Laptop* study, it was determined that the total economic impact of lost laptops was an average of $6.4 million per organization. It was also determined in this study that healthcare and pharmaceuticals had the second highest number of laptop losses among all industries surveyed.

information risk management are more than just "compliance" as we know it. Furthermore, compliance is technically a one-time snapshot or status of where things stand – or *should* stand. Given the fluidity of IT and the continually emerging threats and vulnerabilities, simply focusing on compliance alone is short-sighted and can end up creating a false sense of security that your mobile systems and information are truly secure.

## The Way Ahead

The mobile computing aspect of information security and compliance can seem overwhelming. Where do you even start? First, it's imperative that all of the key players possess the ability to think long term. Rather than ignoring the glaring issue of mobile security and promising to address it down the road, why not do something now? You cannot change what you tolerate. The mark of true business leaders is to be able to think about the consequences of the choices being made (or *not* being made) today when it comes to mobile security.

> Many people believe that further government control in the name of "cybersecurity" is the solution to our world's information security woes. Continued regulation is not the answer. Instead, we must have personal accountability among all the players involved.

Gaining control of the problem is a three step process. The first step involves getting the right people on board. Without management and user support, information security and compliance will be a continual uphill battle. This will require establishing a security or IT governance committee that oversees all such initiatives and helps establish a culture of security and privacy throughout the organization. At a minimum, the roles on this committee should include IT, information security, corporate security, HR, legal and operations.

The next step involves truly understanding what you're up against. You cannot secure what you don't acknowledge so you need to understand how mobile weaknesses are impacting your business. In order to have information risk you must have a threat and vulnerability. With mobile computing, you have both so the opportunity for exposure is ripe. Some common information systems impacted by mobile security exposures in healthcare include:

- EHR systems
- Email, Web applications and backend databases
- Unstructured files (spreadsheets, word processing documents, PDFs, log files, etc.)
- VPN and remote desktop access

In any given healthcare organization, these systems all process or store electronic protected health information, personally-identifiable information, intellectually property and other sensitive business information. Be it through a careless employee, rogue contractor or malicious outsider, all it takes for an exposure in any of these areas is a simple loss, theft or improper disposal of a laptop or mobile storage device.

Once you have a clear baseline of what you're up against, a good exercise for your committee to work through is something called zero-based thinking. In this process the committee needs to answer the following four questions:

1. If our information security and compliance programs were perfect in every way how would they be different from the way they exist right now?
2. What would we be doing more of?
3. What would we be doing less of?
4. Knowing what we know now, what should we do or *not do* moving forward?

It's important to prioritize your efforts and focus on your highest payoff tasks. That is the *urgent* issues on the most *important* systems. This will likely be the fact that full disk encryption and related security controls are missing from your laptops and your mobile storage devices.

Finally, you'll want to pull together a set of reasonable operational and technical controls to ensure the risks you uncover are minimized. Operational controls will include security policies for passwords, travel, remote access and so on as well as a formal security incident response plan that outlines how you'll respond when a security breach occurs. Technical controls will include full disk encryption, centralized logging and monitoring and remote system disablement.

Many regulations have exemptions for businesses that experience a breach if they can demonstrate that the sensitive data was encrypted when the incident occurred.

Just be careful with the false sense of security that full disk encryption can bring about if it's not implemented properly. Issues that can negate most benefits of full disk encryption include:

- Blank or weak passwords
- Users not locking screens when leaving their systems unattended
- No re-authentication required when the system resumes from standby and hibernate

Another technical control that helps supplement full disk encryption is pre-boot authentication. Pre-boot authentication addresses the long-standing problem of network administrators having limited access to administer encrypted laptops and endpoint systems. When administrators cannot fully manage encrypted devices it can introduce weaknesses into the environment which can lead to unintended consequences including data breaches. The benefits of pre-boot authentication include those shown in Figure 3:

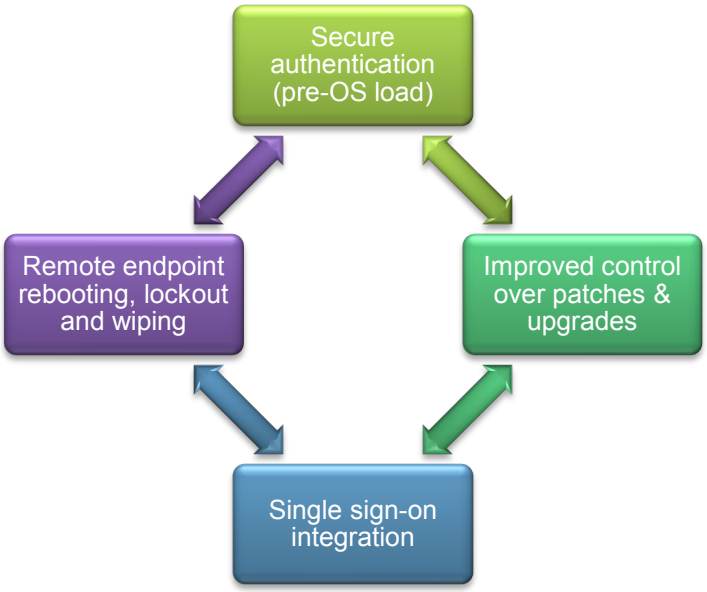


*Figure 3 - Advantages of pre-boot authentication that can help fight both internal and external threats.*

## Conclusion

Businesses in the healthcare industry have arrived at a crossroads. While some are moving backwards down the wrong path, many are idling about trying to determine which way to go. Mobile security is a choice. Every decision you and the other stakeholders make regarding mobile security either moves your organization closer to reasonable information security or farther away. It's critical to see mobile security as an overall information risk issue that impacts the business's bottom line. Treating it any other way will only serve to prolong the problem – especially given the state of flux in the healthcare industry.

Going forward, managing information risks is more than just addressing checkbox items to please auditors and regulators. It's about understanding what you've got, how it's being put at risk and then doing something about it – over and over and over again. Full disk encryption and pre-boot authentication can very likely solve a major portion of your mobile security risks. With all the regulations and expectations of security and privacy in the healthcare industry you don't have the luxury of waiting until the time is just right. Do something about it now and be done with it once and for all.

**About the Author**

*Kevin Beaver, CISSP, is an independent information security consultant, author, expert witness and professional speaker with Atlanta, GA-based Principle Logic, LLC. He has over two decades of experience in IT and specializes in performing information security assessments revolving around compliance and minimizing business risks. Kevin has authored/co-authored 10 books including one of the best-selling information security books Hacking For Dummies (Wiley) as well as The Practical Guide to HIPAA Privacy and Security Compliance (Auerbach). He is also the creator and producer of the Security On Wheels audio books providing security learning for IT professionals on the go (securityonwheels.com). Kevin can be reached at his website www.principlelogic.com and you can follow him on Twitter at @kevinbeaver.*