Hipaa, ePHI and Mobile Devices: Feasibility and Best Practices.

John Hosko
Davenport University
CAPS795
Dr. Lonnie Decker
March 22, 2013
ABSTRACT

The use of mobile devices in the workplace is nothing new. Many years ago with the introduction of the first smartphones, specifically the Blackberry phone, businesses started sending and receiving work emails through corporate servers, to the mobile device. With the explosion of the smartphone and the mobile device industry, these devices are now being used in industries that at one time would be unthinkable. The healthcare industry and the transmission of an individual’s private medical records, is one of the fastest growing users of mobile devices. This paper will explore not only the growth of using mobile devices, which include smartphones, tablets and laptops/netbooks, to transmit this medical information, but the more important security question, does the technology exist, that will allow the end-user to use their mobile devices freely, while following proper security procedures. This would include proper software applications and equipment, available in today’s market that can minimize the concerns that many in the medical industry have regarding this topic, and be user friendly enough that will give the end-user no reason not to use. Users of the mobile devices and the companies that they work for have always battled over the mix of personal use and business use these devices, and with the growing popularity of Bring Your Own Device (BYOD), end-users have resisted the restrictions implemented by the administration at hospitals. This paper will show the results of research, to see if the proper software applications or equipment are available, either now or in the near future, that can resolve this issue. It will also, deliver a comprehensive guide to all the aspects of using mobile devices in the medical field, and the current hardware, software applications, security measures, operating systems, training and policy. Using mobile devices in the medical field is nothing to take lightly, protecting the integrity and confidentiality of a person’s private medical information, is paramount above all else.
Table of Contents

Abstract .........................................................................................................................2
Introduction ..................................................................................................................4
Literature review .........................................................................................................5
Penalties and Fines ......................................................................................................11
Mobile Device Operating Systems and Equipment ....................................................13
  IPhone OS ................................................................................................................13
  Android OS ...............................................................................................................13
  Windows OS .............................................................................................................14
  Tablets ......................................................................................................................14
Network Operating Systems and Equipment ..............................................................15
  Linux .........................................................................................................................15
  Microsoft ..................................................................................................................16
  Hardware ..................................................................................................................16
Method Used to Gather Information ...........................................................................17
Results .........................................................................................................................18
Conclusions and Recommendations ..........................................................................22
References .................................................................................................................26
Appendices ..................................................................................................................29
Introduction

The growth of mobile devices has evolved to an everyday appliance that is a must have by most people, much like a car. In the last decade, smartphones, and almost exclusively the Blackberry, became a standard way to communicate through the corporate server to access email and files. Following that, a new standard of smartphones, tablets and the introduction of the mobile hotspots for the laptop/netbook, introduced a new set of tools to the arsenal of mobile devices. To the surprise of many, mobile devices are now being incorporated into the medical field, not only for transmitting information about patients, they are also being used in the examining room to access and update the patient’s medical record. This record can now be sent or accessed by other healthcare professionals in another part of the hospital or across the country in another clinic or hospital. Mobile devices are also being used to access information that can help diagnose a patient, reach out to a specialist in real time, and get lab results sent directly to the device, all to help with the plan of action for the care of a patient. The list of uses is long and growing each day as new applications are developed and incorporated.

With the use of mobile devices in the medical field though, a whole new set of security concerns have arisen. The protection of the Electronic Personal Health Information (ePHI), proper use by the end-user, and proper security tools, are all concerns that have to be addressed. Because the protection of an individual’s private medical information is paramount to using any mobile device for the use of transmitting, it is important that all protection policies must be followed. The most important policy that must be followed is the Health Insurance Portability and Accounting Act (HIPAA).
Literature Review

Before discussing the types of devices, it is important to review how the HIPAA rules apply and why it is important to protect the ePHI. According to the U.S. Department of Health & Human Services (HHS), this oversees HIPAA, the privacy rule states:

The HIPAA Privacy Rule establishes national standards to protect individuals’ medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patient’s rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.

When allowing mobile devices to store and transmit ePHI, the HIPAA rule is very clear that proper safeguards should be used to protect the integrity and privacy of the patient’s personal health information. The one question that always comes up is what are appropriate safeguards?

The HHS has recognized that the term “appropriate safeguards” can be somewhat vague and have provided additional information to help with any ambiguity. It assigned the authority for this to the Centers for Medicare & Medicaid Services (CMS), not only to offer guidance, but to also enforce the HIPAA Security Standards.

What the CMS requires is proper risk analysis and proper risk management to identify the potential risks and vulnerabilities with using mobile devices onsite or offsite. The management of this risk is focused on three areas: access to the information, storage of the information and the transmission of the information. Each one of the areas should be analyzed individually because each area has its own unique risks.

The access policy should focus on allowing only authorized personnel access to the information and that remote access should only be allow by end-users based on their position in
the organization and their need of the information. Following are some of the common risks and solutions: (“HIPAA Security,” 2006)

**Risk.** Access credentials such as username and password can be lost or stolen, allowing an unauthorized user to access the information.

**Solution.** Implement double authentication when granting access from a mobile device, especially when off site. This can be done with a random key or password generator.

**Risk.** Unauthorized personnel accessing ePHI while working offsite.

**Solution.** Develop procedures that give proper clearance to authorized personnel. Define and establish access roles, according to job duties within the organization, and issue proper access according to policy.

**Risk.** Workstations left unattended both onsite and offsite. Allowing access to ePHI.

**Solution.** Establish proper session termination when workstations are left unattended.

Storage policies will focus on the actual physical devices that the information is stored on and how these devices are moved between users. This not only includes the actual mobile devices, but other secondary devices such as flash drives, or backup devices that are stored in another location in case the information at the main location is lost.

**Risk.** Mobile devices are lost or stolen, which potentially can compromise ePHI.

**Solution.** Identify and inventory all mobile devices that have access to the network. Also identify the personal that use the device. Consider using biometrics, many mobile devices today have that as a pre-loaded feature.

**Risk.** Allowing access to corporate data, from a mobile device, that could result in the loss of ePHI.
Solution. Develop proper back up processes that incorporate encrypted offsite archival storage. This should also include a highly developed disaster recovery plan.

Risk. Data is downloaded to an external device, such as a hotel computer hard drive.

Solution. Prohibit the downloading of ePHI onto remote systems. Properly train personal on the proper procedure of deleting files from these systems, included deleted appropriate cookies.

Transmission policies should focus on the integrity and the confidentiality of the information, and how it is transmitted and to whom it is transmitted. This is a very important area of concern when using mobile devices, because of the possible blending of personal information and business information.

Risk. Data intercepted or modified during transmission.

Solution. Prohibit transmission of ePHI on unsecure networks such as public Wi-Fi.

Mandate proper encryption when transmitting ePHI, such as virtual private networks.

The CMS also has concerns regarding where the mobile device will be used, onsite or offsite. Though much of the same security risks can happen in both places, it is more prevalent when the mobile devices are taken offsite.

Theft of the device is the number one reason that the integrity of the information is compromised. (Jenkins, 2011) This is why it is HHS suggests that all devices be left onsite if at all possible. If the devices are to be used offsite, then it must be done in a way that ensures that the proper security measures and training have been done.

Allowing the use of mobile devices, present numerous management challenges, but the concern increases when allowing employees to BYOD to carry and transmit ePHI. Some of the
more critical challenges include increased privacy and security risks to the data, which can lead to breaches of the ePHI, and unintentional harm to the patient. Therefore, it is important that organizational policies and procedures are clearly communicated and enforced for all workforce members to establish expectations and assign accountability.

Allowing BYOD is not necessarily a bad thing, it has been reported that the user can average a time savings of up to 47 minutes a day and approximately a 10 percent increase in productivity when the user is allowed to use their personal devices. This is attributed to the user being comfortable and familiar with the device.

With that being said, when allowing BYOD, risks can be minimized by establishing appropriate controls by implementing the necessary measures to protect the patient’s ePHI. All healthcare organizations, must establish written policies and procedures covering the use of mobile devices that address the following issues:

- The user signing an annual agreement stating that they understand and agree to the organizations policy and procedure.
- Proper password protection requirements
- Features built into the device, that provide different lock out utilities
- Appropriate use of texting
- Appropriate use of camera and video
- Appropriate use of sensitive information
- Clear policy stating that the devices OS will not be altered(i.e. jail-breaking, bricking, unlocking)
- Clear policy regarding the downloading of software/applications
- Reservations of rights by the healthcare facility to examine the system for compliance and investigation of incidents
Procedures during employee or contractor termination

Most of the technology to secure the ePHI is already available, but the conflict between management and the user, and the patient and user, is where many of the problems arise. Many employees do not like the control that management wants to put on their personal device, because they feel that it is their device, and management should not be able to put controls on how the device is used.

Management has to clearly define who the data belongs to, many practitioners feel that since they are the ones gathering the patient’s information that it belongs to them. Management should resolve any such issue up front and in a written agreement with the user, that clearly states the data belongs to the patient and the hospital, and that proper safeguards are in place to protect the ePHI. When defining who the data belongs to, it is also important to define what constitutes sensitive information. Obviously, anything that identifies the patient, their treatment and/or diagnosis, is sensitive, but to prevent any confusion regarding any other information, it is important to define the term within the organization's policy as a method to establish a common definition as to what constitutes sensitive information.

Most security problems between the patient and the employee goes mostly unnoticed and usually is only discovered when something goes wrong. This usually starts when the patient and the doctors or nurses start communicating via unsecured texting and emailing. Both parties look at this as a great convenience, but never think of the risk that goes along with it.

The area of social media, and what limitations are expected, should also be included in policy and procedure. This is a generational issue that will become more prevalent in the near future, that is why it should be addressed early on.
Practitioners should also understand what are proper rules of behavior and acceptable uses for the use of mobile devices when dealing with ePHI. This would include not transporting any ePHI on the device itself, unless following the proper guidelines established in the policy and procedure. The user should also refrain from using the device to take photographs of the patient, unless it was regarding an injury or was pertinent to the treatment of the patient. It is also important to not photograph any visitors, staff, or the facility, without proper consent.

A device being lost or stolen is a very common occurrence, and the installation of proper tracking software on the device, should be the first software to be loaded on the mobile device, before allowing any work to be done on it. Though the main purpose of this software is tracking, it is not the most important feature. The most important feature is the ability to remotely lock a device, and also wipe the device clean of any information on the device. Many employees don’t like this because they do not have their personal information backed up and will be lost along with work information.

Once the software is installed on the mobile device, it can then connect to a server based management system, usually located at the IT center of the hospital or office. The administrator can then interact with any of the devices, wherever they might be located. There are some higher level software applications that can enable functions such as turning the device on or off, changing configurations, managing applications, enforcing encryption standards to ensure all operations are carried out and that they function correctly. The disadvantage lies in the requirement to install the software on the mobile device. Many users may not want the organization to place management software on their personal smartphone, tablet, or laptop.

Each organization should have clearly defined procedures for the reporting of a device loss or stolen. Organizational procedures should detail who to call, what hours to call, and the
expected details needed to make a report an incident. In the event of a loss or stolen device, users should immediately make notes regarding the incident and what took place. These notes will be useful if any investigation has to done at a later time. Also, a police report should always be made in the event the mobile device is lost or stolen.

Penalties and Fines

If there are incidents of the information being compromised, and HIPAA regulations not being properly followed, the fines can be very substantial. This is why hospitals and administrators do not like using mobile devices to store and transmit ePHI. The federal government is serious about the penalties and as of 2009 the penalties for HIPAA violations were increased 500 times their prior limits. Not only are states allowed to sue and recover $25,000 per violation plus attorney fees, but the new penalties also put in place an incentive for patients to report a violation, by allowing them to receive part of any settlement.

The following chart summarizes the penalty structure:

<table>
<thead>
<tr>
<th>Conduct of covered entity or business associate</th>
<th>Penalty</th>
</tr>
</thead>
<tbody>
<tr>
<td>Did not know and, by exercising reasonable diligence, would not have known of the violation</td>
<td>$100 to $50,000 per violation; Up to $1,500,000 per identical violation per year</td>
</tr>
<tr>
<td>Violation due to reasonable cause and not willful neglect</td>
<td>$1,000 to $50,000 per violation; Up to $1,500,000 per identical violation per year</td>
</tr>
<tr>
<td>Violation due to willful neglect but the violation is corrected within 30 days after the covered entity knew or should have known of the violation</td>
<td>Mandatory fine of $10,000 to $50,000 per violation; Up to $1,500,000 per identical violation per year</td>
</tr>
<tr>
<td>Violation due to willful neglect and the violation was not corrected within 30 days after the covered entity knew or should have known of the violation</td>
<td>Mandatory fine of not less than $50,000 per violation; Up to $1,500,000 per identical violation per year</td>
</tr>
</tbody>
</table>

Table 1 (“HIPAA Violations,” 2009)
Below are two of examples of violations and the fines imposed because data on mobile devices was not properly secured.

The first case involved Blue Cross Blue Shield of Tennessee (BCBST) which was fined $1.5 million for not properly encrypting patient’s ePHI on computer hard drives. In November of 2009, BCNST reported that 57 unencrypted hard drives were stolen from a network data storage closet at a facility that it leased. The data contained the ePHI of over 1 million patients. This information contained names, social security numbers, and diagnosis codes, dates of birth and health plan identification numbers. (“HHS Settles,” 2012)

It was determined that BCBST did not follow the proper safeguards, both physical and administrative, that are required by HIPAA. Even though the network data closet was secured by multiple locks, including biometric security, keycard scan, and a magnetic lock, it was still determined that BCBST did not use adequate controls restricting facility access. The reason given was they did not evaluated or instruct the property management’s security services on proper security procedures regarding ePHI.

The second case involved the Massachusetts Eye and Ear Infirmary and Massachusetts Eye and Ear Associates Inc. (MEEI). They were fined $1.5 million because of a stolen laptop that contained ePHI of patients and research subjects. The OCR investigation indicated that MEEI failed to take necessary steps to comply with certain requirements of the security rule, such as conducting a thorough analysis of the risk to the confidentiality of ePHI maintained on portable devices, implementing security measures sufficient to ensure the confidentiality and the integrity of the ePHI that MEEI created, maintained, and transmitted using portable devices. It also failed to adopt and implement proper policies and procedures to restrict access to ePHI to authorized users of portable devices. OCR’s investigation indicated that these failures continued over an
extended period of time, demonstrating a long-term, organizational disregard for the
requirements of the security rule. (“Massachusetts provider,” 2012)

In addition to the $1.5 million settlement, the agreement requires MEEI to adhere to a
corrective action plan, which includes reviewing, revising, and maintaining policies and
procedures to ensure compliance with proper security rules. An independent monitor will
conduct assessments of MEEI's compliance with the corrective action plan and submit semi-
annual reports to HHS for a 3-year period.

Mobile Device Operating Systems and Equipment

Though mobile devices can include many different kinds of hardware, the devices that are
mostly used are the smartphones and tablets. They have become the front runners because of the
ease of use, portability, and technology. This section describes the operating systems and
hardware.

*IPhone OS*

The iOS has been the most popular of all the operating systems that are used on mobile
devices. This is because it has remained relatively unchanged, except for some minor version
changes, since its introduction in 2007. Up until 2012, the iPhone was the top selling smartphone
on the market. Most of the early applications were all written for the iPhone, which made it the
top selling smartphone for many years. The iOS also runs the iPad that will be discussed later in
this section.

*Android OS*

In 2008 Google released its Android OS and quickly became the top selling operating
systems on the market. One of the biggest reasons for this was that Google allowed different
phone manufactures to use its operating system for their phones. This was in contrast to the iOS
that is only allowed on Apple products. Other reasons for its popularity is the flexibility to be
customized by the user to meet their needs, using multiple home screens, live widgets and its
early use of the 4G LTE technology. Applications for the Android OS are now developed in
tandem with the iOS. As with the iOS, the Android OS is used on tablets and those will be
discussed later in the section.

Windows OS

Microsoft entered the smartphone industry in 2010 and updated its system in October of
2012. The biggest feature of course is its interface with Microsoft Office documents and syncing
them across different devices, there are also some built in features that can help with the needs of
a large company. The leading selling feature for the Windows phones live tiles, allowing the user
can see the newest text or the email without having to open up the entire feature.

Tablets

Of all the mobile devices discussed in this paper, tablets are the devices that are growing the
most in the medical field. They operate on the same OS as their smartphone counterparts, but
offer a larger work area, much like a laptop.

A survey by QuantiaMD that included, 3,798 physicians, showed that approximately 30% of
those physicians use a tablet, compared to 5% of U.S. consumers. (Modahl, 2011) Of those 30%,
approximately two-thirds of them use the tablets in their daily practice. The survey also stated
that of the surveyed doctors, 35% who did not have a tablet were extremely likely to start using
one in the near future. Of the tablet being used, the iPad is the most often used, followed by a
tablet running the Android OS.
Network Operating Systems and Server Hardware

The server and the operating system are what connect the entire network and devices together. With the increase of mobile devices and BYOD, a system has to be versatile enough to work with the different operating systems that mobile devices use. Gone are the days of a system running Windows OS for all the desktop computers in company, and gone is the Blackberry being the only mobile device use to remotely connect to the server. Systems have to be scalable to adapt to the number of devices and operating systems it has to work with. Following are some of the different operating systems and servers available.

Linux

The Linux operating system has been around for a very long time and has been the favored OS for the very knowledgeable, personal computer user, because it is highly adaptable and able to be customized for different operations.

Redhat.com, states that 80% of Fortune 500 companies now use the Red Hat Enterprise Linux (RHEL). (“Enterprise proven,” 2013) It is highly adaptable for organizations with several hundred users to tens of thousands of users. The RHEL OS has also been around long enough that technical support by certified technicians, administrators and engineers are readily available. It is also versatile enough to run on different servers such as rack and blade servers, IBM systems or main frames.

Two other Linux systems that also work well in this environment are the Oracle Linux and the SUSE Linux Enterprise Server (SLES). With Oracle Linux, you get almost the same configuration of RHEL, but you also get the name and support that go along with Oracle. This system is used by small practices with a few locations, as the best fit for their needs.
Microsoft

Microsoft has always had a large presence in the enterprise market. Its name, and that most people have worked with some version of Microsoft Windows operating system at some time, still make them a huge part of the market.

Its newest version is the Windows Server 2012, which incorporates the strong components of previous versions, but improves on virtualization and introduces cloud computing to the system. Microsoft Server 2012 virtualization platform, now allows the user to swap out certain components for third party ones, which if needed, allows for quick reconfiguration. It also recognizes the importance of BYOD, by adding Dynamic Access Control (DAC) for better management tools that are important when working BYOD.

Hardware

Server hardware can be a considerable challenge when setting up a network. The number of companies that manufacture the hardware, the different configurations available, and deciding which is the best for your organization can be a major undertaking. There are, however a few key points that should help in the process.

Scalability: If you plan on growing your business, scalability is where your focus should be. Not being able to increase your server capacity because of server limitations can halt the need or desire to grow, and many times force the organization to invest in a new server to handle the new growth. Proper scalability should be relatively seamless and have minimal disruption. This means maximum storage capacity, support for multiple drives, room for expansion inside the chassis and a capable processor.
Virtualization: This term is new to many businesses, but will need to be a part of any network at some time. Many organizations are finding the benefit of combining multiple physical servers in virtual machines housed on one physical server. Virtualization allows for server consolidation, which saves cost, by reducing the number and type of servers that are needed, to support a company’s business applications. This also leads to less power consumption by the server and the cooling systems that are needed for the servers.

Data Redundancy and Fault Tolerance: No Business can afford to have any interruption or downtime in their day-to-day operations. Data redundancy and fault tolerance are ways to keep data intact and servers functioning in the event of a disaster such as disk drive failure. Data redundancy and fault tolerance systems are being replaced with newer technology, but included here because of price constrictions that may keep some of the smaller practices from moving to higher end systems.

Price: Your budget is going to be a major factor in with any server you select. But when deciding which other factors are important, scalability would be the first one to look at when deciding what to purchase. Being able to grow cost effectively is very important. Other factors such as virtualization and data redundancy and fault tolerance can always be working into the system as it grows.

Method Used to Gather Information

Secondary research was the method used for gathering information for this paper, by using published articles on the internet. This included government websites, online newspaper, and product review online articles, also software and hardware manufactures websites.

The government websites, The Department of Health and Human Services and The Centers for Medicare & Medicaid Services, were used because they are the government departments that
wrote and enforce the HIPAA rules and regulations. They were also used to gather information about HIPAA, its privacy rules, and how those privacy rules relate to mobile devices, including information about fines that have been assessed to organizations that have been found in violation of the privacy regulations.

The commercial websites; Cisco, IBM, AT&T, and Microsoft, were used because of the prominence in the marketplace for developing these technologies.

CNN, Technology Review, Forbes, PC Mag, zDet, are news and review websites that were used as a neutral reference, to verify, confirm or refute any information if needed between the government information and the commercial information. These sources are either trusted sources in the news industry or specialize in technology.

Results

Research demonstrates, that most organizations and practitioners agree that the use of mobile devices should be used in the healthcare industry, and that it is revolutionizing the medical field. Several years ago, the University of Virginia School of Medicine, required all third year medical students to have a recommended mobile device for the coursework, but before the requirement went into effect, it was found that 90% of the third year students had already had purchased a mobile device and were using it in their studies. A 2011 report by Jackson & Coker report also showed that four out of five doctors now use some type of mobile device, when interacting with patients. They attribute this to the affordability, ease of use, and quick access to patients charts.

On March 16, 2011, Bulletin Healthcare released a study that showed the breakdown of doctors using mobile devices by specialty.

- Emergency Room Physicians – 40 percent
• Physician Assistants – 4 percent
• Cardiologists – 33 percent
• Urologists – 31 percent
• Nephrologists – 31 percent
• Dermatologists – 30 percent
• Gastroenterologists – 30 percent
• Psychiatrists – 28 percent
• Optometrists – 28 percent
• Radiologists – 24 percent
• Rheumatologists – 22 percent
• Endocrinologists – 21 percent
• Oncologists – 20 percent
• Clinical Pathologists – 16 percent.

The report suggested that part of the reason for the increase of doctors using mobile devices was that both the Apple App Store and Google’s Android Market now have entire sections devoted to healthcare apps that practitioners are finding invaluable.

The technology to secure and transmit ePHI has been in place for a few years, but not being properly used. This leads back to the original question, is there new technology available that would allow the end-user and patient to follow proper policy and procedure while still having the freedom to use their mobile devices without any inconvenience?

What the research found was that the technology does exist that can resolve the conflict so that there is no reason that proper security procedures should not be used by the user and patients.

*Web portals*

Communication between the patient, hospital and practitioner was being done via email, texting and fax, all very convenient, but all very insecure. Many hospitals are now adapting the use of web portals as a secure, centralized website that allow the patient to securely communicate with the doctor or nurse through the portal using email. With the portals, communication between the practitioner and the patient should no longer be done through either party’s private
email. The portals can also be used to make appointments, refill prescriptions, see your and your family’s medical records, billing and insurance information, and other administrative options. (See FIG. 1 and FIG. 2 in Appendix 1)

Though the use of viewing information and communicating online has been in place in many hospitals, they were mostly used as an intranet function, only to be used by the practitioner. Many hospitals also had different systems, which required multiple logins, depending on the information that was needed, and none of these allowed the patient access to any of the systems.

The use of web portals is now becoming more prevalent in the medical industry. The need for a centralized site and the technology that develops and strengthens the relationship between the hospital, its physicians, staff and patients not only strengthens the security of the ePHI, but also drastically reduces the administrative cost that these tasks require.

Not only do these portals allow for a single location of all the information, it allows the patient to access their medical information, anytime and anywhere there is internet connection. This is extremely helpful if a patient were to need medical treatment in another state or country.

**Dual Use Applications**

Allowing the user to access and transmit ePHI information through a mobile device contain a certain amount of difficulty in assuring the integrity and confidentiality of the ePHI. The potential of the user’s personal data being combined with the company’s information is a concern.

Many companies try to control this by supplying the user with a company owned mobile device such as a laptop or smartphone that is configured to only connect to the company secured network, allow certain applications, or only have access to limited websites. Many times, this process required the user to carry multiple devices, or have stringent controls over the user’s personal device.
This posed a problem, especially with the newer smartphones and tablets that are available. The user wants to enjoy the uses that today’s mobile devices provide, and didn’t want to be told what applications they could or could not download.

Near the end of 2012, AT&T introduced a new virtualization-style technology that has minimized this concern. It is an application called Toggle, which partitions the phone into two sections. Toggle lets a user enter the work side of their phone by clicking an application icon. This allows the user to access work-specific e-mail and text messaging, document attachments are encrypted, and the Toggle work partition also includes its own secure Web browser. Data is pushed from company applications to phones over SSL, and administrators can view all the details of devices connecting to the network and enforce permissions, set policies at a company-wide or group level, and perform a screen lock or remote wipe on the work partition, while leaving the personal partition untouched.

With Toggle installed on the device, the user taps the home button twice to flip between personal and work modes. The personal mode behaves like a regular phone and is fully under the user’s control. The work mode looks like a separate phone with its own desktop and suite of apps. It also allows IT administrators, to set up a centralized location called a Toggle Hub, which can be customized to the organization, where users can choose and download approved applications. Once an application is on the device, IT can disable it if necessary. If a device is lost or stolen or the employee leaves the company, all the data can be removed.

Though originally designed to work on the Android OS, it has recently been configured to work on the iOS and will be on the Blackberry OS and Windows OS very soon. (Brodkin, 2012) There are some fees that AT&T charge for the use, but these are minimal compared to what it does for the mobile device industry and all other industries that need information properly secured.
VMware also has a product being developed called Horizon Mobile, but at this time it is not available on the market, though it should be by the end of 2013. (“VMware Horizon”, n.d.)

Conclusions and Recommendations

This paper covered many areas of using mobile devices in the healthcare industry. It was focused on the security of the patient’s information, and the concerns of using the devices. A patient’s ePHI should be protected at all cost, but finding the tools to do that can be difficult at times. We are at a very exciting time in the healthcare industry, with the possibility to care for the patient like never before. We can now find and share information regarding the patients care around the world and in real time. Be able to find diagnosis and treatments outside the hospital’s walls that can save or improve someone’s life. The use of mobile devices is critical to the success of the healthcare industry, now and in the future. That is why it is imperative that large hospitals down to the one doctor office embrace this technology to better care for the patient. This research has shown that the tools are available, and the cost affordable, that the time is right for HIPAA, ePHI and mobile devices to be used.

While a primary intent of this research was to determine if appropriate technology existed to allow mobile devices securely in the healthcare industry, another benefit provided is to suggest recommendations for equipment and software applications.

Mobile device and operating system

Only three operating systems were included in the research, Apple’s iOS, Google’s Android OS and Windows OS. There were two additional operating systems that were not included, which were the Palm OS and the Blackberry OS. At this time these systems cannot compete. The Palm OS, though still around, does not provide the technology needed for any business needs. The Blackberry OS, which was the mainstay of corporate America, has lost its
position in the market in the last two years. Its security is still one of the best on the market, but its lack of adaptation to the market place makes it a non-player.

The Windows operating system was listed as one of the top three, but that is mainly because of the time and money that has been recently put into the development of the OS by Microsoft. It might be a useful OS for a niche market, but when it comes to overall business use, and especially in the medical field, it has yet to show up in any reports at this time.

Though both the Apple OS and the Android OS are popular systems, research shows that the Android OS is the overall better system, as it allows the user to do more and have a choice of different devices from many manufactures. It has an open platform which means developing a new application, is a simpler process. Conversely the Apple OS is a closed platform, this can make development of new applications a difficult process.

According to a report by comScore, the last quarter of 2012 shows Apple as the top seller of mobile devices, 36.2%, but it is the Android OS that is on most of the mobile devices, 53.4%. (“U.S. Smartphone”, 2013) This is because the Android OS is run on mobile devices from many manufactures.

Server OS

Though the Linux seems to be making its way into the large server network industry, Windows Server 2012 would be recommended. Its release has been highly rated and delivers many new features and capabilities along with an extensive list of enhancements for existing functionality. for the number of new features such as updated processors, more memory and scalability. The new design for Windows Server 2012 was determined by the three core themes of continuous availability, cost efficiency and management efficiency.
Server

The Cisco organization has put a lot of development resources into the healthcare industry by introducing its unified computing systems. They offer a wide variety of server systems that are specifically tailored for healthcare. The Cisco UCS 5100 Series Blade Server Chassis is the flagship server that many hospitals now use, because of its scalability and flexibility.

Centralized web portal

When it came to a centralized web portal, there were few companies that have developed products that did variations of a portal, from a centralized system for a small to medium size medical practice, to large systems for hospitals. The smaller ones did not allow for the patient to interface with the system externally, but was more a network that was used from the examining room to the different areas of a practice such as the front desk and billing.

The number of companies that could provide a more robust system is limited. The research showed that there was a system that integrated the needs of a centralized portal, it was a company called Epic.

Epic makes software for mid-size and large medical groups, hospitals and integrated healthcare organizations. Its electronic health record system is based on a 44-year-old programming language called Massachusetts General Hospital Utility Multi-Programming System (MUMPS).

Epic software is quick to implement, easy to use and highly interoperable through industry standards. With that being said, it is basically a closed platform, which means that it provides many helpful tools, but it does not interface with outside software that might currently be in place at a facility that is thinking of implementing it. The transferring of the information into the system does add additional time and cost, but it is rated at the top for ease of use and scalability. It has recently been implemented at the University of Michigan Hospital System, and the author had the opportunity to use it personally. I was able to order prescriptions, see my medical
records, make and confirm appointments, communicate with my doctors and find educational materials.

*Dual use application*

The Toggle system by AT&T is real the only system on the market today that offers exactly what is needed when using mobile devices, especially BYOD, in the healthcare industry. The mobile device user will have no excuse why they wouldn’t follow the security procedures when working with ePHI.

While there are security concerns in utilizing mobile devices in the current healthcare environment, it is clear that doing so is not only possible, but also can increase productivity and satisfaction of customers and employees.
References


http://www.medseek.com/body.cfm?id=850&action=detail&aearcldieid=638&aeproductid=client_mscorp10026

Massengill, S. (ND). *Can Portals Deliver for Hospitals and Integrated Delivery Networks?*. Retrieved December 2012, from himss.org:
http://www.himss.org/ASP/ContentRedirector.asp?ContentID=68755

http://www.quantiamd.com/q-qcp/quantiamd_research_tabletssettochangemedicalpractice.pdf

http://www.forbes.com/sites/zinamoukheiber/2012/04/18/epic-systems-tough-billionaire/

https://www.myuofmhealth.org/MyChart-PRD/

*Small client base, huge global impact.* (ND). Retrieved January 2013, from epic.com:
http://www.epic.com/about-index.php

*VMware Horizon Mobile.* (ND). Retrieved January 2013, from vmware.com:


Waters, J. (N.D.). *Virtualization Definition and Solutions.* Retrieved February 27th, 2013, from CIO.com:
Virtualization Definition and Solutions
Appendix 1

("My U of M," n.d.)