BYOD-IMPACT ON HEALTHCARE INFORMATION SECURITY

Brian Kyle Marek

Abstract — *This paper focuses on the impact of Bring Your Own Device (BYOD) on Healthcare information security. The impacts of BYOD are many and the research presented covers such topics as regulatory compliance, including the Health Information Technology for Economic and Clinical Health Act (HITECH,) which is a 19.2 billion dollar part of the American Recovery and Reinvestment Act (ARRA) of 2009, which expands the Health Insurance Probability and Accountability Act (HIPAA) of 1996, communication and storage of unencrypted protected health information, loss or theft of devices containing protected health information, and tracking and controlling access to the multitude of devices that are available. Another challenge discussed is the policies that are required to successfully implement BYOD in healthcare while not creating roadblocks for providers. This paper will also discuss basic software that is available to provide support to healthcare organizations utilizing BYOD.*

Index Terms — Electronic Medical Record (EMR,) Health Insurance Probability and Accountability Act (HIPAA) of 1996, Health Information Technology for Economic and Clinical Health Act (HITECH,) HIPAA, Bring Your Own Device (BYOD), Master Data Management (MDM) Solutions, Meaningful Use

I. Introduction

BYOD (Bring Your Own Device) is a growing trend in many organizations. "It used to be that IT departments drove technology, but that has changed dramatically in recent years. The consumerization of IT revolution -- sparked by the iPhone -- has shifted the IT culture so that the users are the ones getting the latest, cutting edge technologies first, and they want to bring those devices to work." [1] While the advantages of BYOD are many, there are many concerns and issues that must be considered when introducing BYOD in an organization. This is especially true in regards to the use of BYOD in healthcare settings.

II. BYOD Defined

"Gone are the days when employees wielded a simple set of tools to get work done. In today's world of anytime, anywhere work, employees use whatever device is most convenient: desktop at home, laptop at work, tablet in a client meeting, or smartphone everywhere. The convenience of mobile devices sets the bar for what your mobile workforce expects: They want access to the Internet and to all their business tools from any location on any device." [2] According to a recent Forrester survey, Smartphones and tablets are the most popular forms of BYOD in the workplace with almost half of the workforce already using Smartphones. Tablet use is on the rise as well, with an expected 905 million tablets in use by 2017. [2]

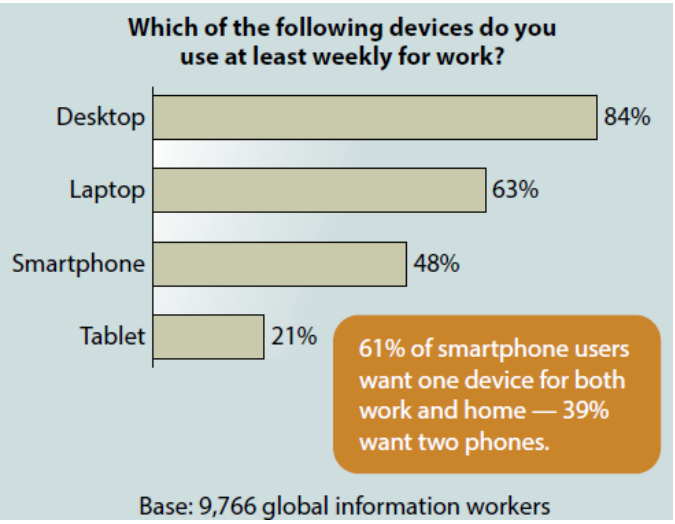

Fig. 1 Devices Used in the Workplace [2]

III. Advantages of BYOD

BYOD in the workplace is advantageous for both employees and the organization. Employees are more mobile and can work flexible hours using BYOD. This often gives companies a recruitment advantage over other organizations that do not allow BYOD. In addition, many employees using BYOD report higher employee satisfaction. "Users have the laptops and smartphones they have for a reason – those are the devices they prefer, and they like them so much they invested their hard-earned money in them. Of course they'd rather use the devices they love rather than being stuck with laptops and mobile devices that are selected and issued by the IT department." [1]

Corporations benefit in the reduced costs of purchasing technological equipment, as employees purchase their own devices. This also equates to less trouble-shooting and support from the organization's IT Department as employees are familiar with and maintain their own devices. The corporation benefits from newer versions of devices. "BYOD devices tend to be more cutting edge, so the organization gets the benefit of the latest features and capabilities. Users also upgrade to the latest hardware more frequently than the painfully slow refresh cycles at most organizations." [1] The increased productivity that employees experience is a win for the organization as well. According to a survey of 1,100 mobile workers, employees that use mobile devices both at home and at work average an extra 240 hours of work per year. [3]

IV. Disadvantages of BYOD

BYOD does not come without concerns. "…IT leaders also say mobile technology come with challenges, especially in a BYOD environment where smartphones and tablets can easily be lost or stolen." [4] Many organizations fear the loss of data or trade secrets. In addition, there are technical issues that may create concerns for BYOD organizations. These "include the use of untrusted devices, networks, and/or applications; support for multiple mobile operating systems; installation of security patches and software updates; and interaction with other systems for data synchronization and storage." [5] While these are issues of concern for all industries, the healthcare industry has had an especially difficult time adapting to BYOD. As the confidentiality and protection of patients' Private Health Information (PHI) is legally mandated in healthcare, the implementation of BYOD is often difficult to adopt. [6]

V. Special Concerns of BYOD in the Healthcare Setting

A. Electronic Medical Records

The Electronic Medical Record (EMR) is a digital version of a patient's paper medical record. There are many advantages of an EMR over a paper record. EMRs have been proven to be more complete due to compulsory fields that must be answered. They are often more legible than paper records which leads to increased patient safety. Past medical history and allergies are stored in the record for convenient access in an emergency. Multiple providers can review the record at one time, and from a variety of locations. [7] It is this increased accessibility that contributes to the concerns of BYOD opponents in healthcare settings. One might think that concerns regarding the EMR and BYOD are only issues in large healthcare systems or practices; however that is not the case. "It's not just big hospitals in major metropolitan centers that are purchasing the new technology. The number of rural hospitals with an EHR system increased from about 10 percent to 33.5 percent between 2010 and 2012, while urban hospitals saw EHR adoption rates rise from 17 percent to nearly 48 percent." [8]

Why are EMRs a concern for CIOs when considering the implementation of BYOD in that healthcare environment? EMRs contain Protected Health Information (PHI.) This is defined as "demographic information, medical history, test and laboratory results, insurance information and other data that is collected by a health care professional to identify an individual and determine appropriate care." [9] There are a number of legal regulations that focus on the security of PHI.

B. Health Information Portability and Accountability Act

Among other things, the Health Information and Portability Act of 1996 (HIPAA) sets forth the legal responsibility to protect personally identifiable health information – PHI. In 2009, as part of the Stimulus bill, President Obama passed the Health Information Technology for Economic and Clinical Health Act (the HITECH Act.) This bill encourages the implementation of Electronic Medical Records and enhances HIPAA. "The HITECH Act also substantially expands the HIPAA Privacy and Security Rules and increases the penalties for violations of HIPAA." [10]

HITECH: New Requirements
Apply the HIPAA privacy and security requirements directly to business associates
Establish mandatory federal security breach reporting requirements for HIPAA covered entities and their business associates
Create new privacy requirements for HIPAA covered entities and their business associates, including new accounting requirements for EHR
Restrictions on marketing and fundraising, and other developments
Enforcement responsibilities

Fig. 2 HITECH Requirements *[10]*

It is apparent that the security of Protected Health Information is a concern in regards to the implementation of a BYOD program. Hospitals do not allow physicians or other healthcare providers to remove paper records from the hospital campus, yet with BYOD and digitization of the medical record, this information can be accessed just about anywhere, from the physician's medical office to the local grocery store. HIPAA and HITECH are in place to discourage the inappropriate sharing of information. The Secretary of the Department of Health and Human Services determines the penalties individuals are fined for HIPAA violations. This may vary based on the level of intent and the harm caused by the transgression.

HIPAA Violation	Minimum Penalty	Maximum Penalty
Individual did not know (and by exercising reasonable diligence would not have known) that he/she violated HIPAA	$100 per violation, with an annual maximum of $25,000 for repeat violations (Note: maximum that can be imposed by State Attorneys General regardless of the type of violation)	$50,000 per violation, with an annual maximum of $1.5 million
HIPAA violation due to reasonable cause and not due to willful neglect	$1,000 per violation, with an annual maximum of $100,000 for repeat violations	$50,000 per violation, with an annual maximum of $1.5 million
HIPAA violation due to willful neglect but violation is corrected within the required time period	$10,000 per violation, with an annual maximum of $250,000 for repeat violations	$50,000 per violation, with an annual maximum of $1.5 million
HIPAA violation is due to willful neglect and is not corrected	$50,000 per violation, with an annual maximum of $1.5 million	$50,000 per violation, with an annual maximum of $1.5 million

Fig. 3 HIPAA Violations and Penalties [11]

C. Meaningful Use

Transitioning to Electronic Medical Records is costly. A recent study estimates that implementation for a five physician practice costs about $233,297. "For an average five-physician practice, implementation costs through the first 60 days after EMR launch were an estimated $162,047, with an average per-physician cost of $32,409 and $85,500 in maintenance expenses during the first year." *[12]* Hospital EMR costs are even more staggering. A Forbes report from 2012 reported that large hospital systems purchasing the popular Epic system expect to pay huge sums of money. "Duke University Health System will shell out $700 million, so will Boston

-based Partners HealthCare; University of California, San Francisco will pay $150 million. Customers, such as New Hampshire's Dartmouth-Hitchcock Medical Center are feeling the pinch. DHMC which implemented Epic last year at a cost of $80 million, expects a weak operating performance in 2012, partly because of expenses related to Epic." *[13]* So are the advantages of an Electronic Medical Record worth the expense? The United States Government believes so. Part of the HITECH Act includes Meaningful Use. "HITECH proposes the meaningful use of interoperable electronic health records throughout the United States health care delivery system as a critical national goal. Meaningful Use is defined by the use of certified EHR technology in a meaningful manner (for example electronic prescribing); ensuring that the certified EHR technology is connected in a manner that provides for the electronic exchange of health information to improve the quality of care …" *[14]*

The government offers incentive money for practices and hospitals that reach the Meaningful Use guidelines. This will help offset some of the costs of the implementation of an Electronic Medical Record. However, there are also penalties in place for organizations that do not reach the various stages of Meaningful Use in the appropriate time frame through reduction of Medicare payments. This is yet another reason for healthcare organizations to focus on the implementation of an Electronic Medical Record.

As more and more organizations gravitate to the Electronic version of records, BYOD will present challenges to healthcare organizations. The information that the law requires healthcare professionals and institutions protect, is made even more easily accessible on BYOD devices by being stored electronically. As mentioned before, mobility is an advantage of BYOD, but can also be a curse. "BYOD has opened a Pandora's box of risks and vulnerabilities, given that mobile devices are easily portable, are apt to get lost or stolen, and open up additional attack vectors into the network that seemingly circumvent traditional network firewalls." [15]

Stage 1: Meaningful use criteria focus on:	Stage 2: Meaningful use criteria focus on:	Stage 3: Meaningful use criteria focus on:
Electronically capturing health information in a standardized format	More rigorous health information exchange (HIE)	Improving quality, safety, and efficiency, leading to improved health outcomes
Using that information to track key clinical conditions	Increased requirements for e-prescribing and incorporating lab results	Decision support for national high-priority conditions
Communicating that information for care coordination processes	Electronic transmission of patient care summaries across multiple settings	Patient access to self-management tools
Initiating the reporting of clinical quality measures and public health information	More patient-controlled data	Access to comprehensive patient data through patient-centered HIE
Using information to engage patients and their families in their care		Improving population health

Fig. 4 Three Stages of Meaningful Use [16]

VI. Recommendations of BYOD Implementation

A. Decision to Implement

With all of the pros and cons of BYOD, it is easy to understand why companies often struggle with the decision of whether or not to implement a BYOD policy. Is the risk worth the benefit? Experts say the real decision is to make the policy official or not. "There's no sense pretending it isn't happening or saying, 'We don't let our employees do that.' The truth is, they're doing it already and will continue to burrow noncompliant devices into your network with or without your permission. Forrester's study of US information workers revealed that 37% are doing something with technology before formal permissions or policies are instituted." [17]

Once the decision is made to move forward with BYOD in the workplace there are essential elements needed to make the program successful and in the heavily regulated healthcare environment, a successful BYOD program is a must. "BYOD should be assessed as part of a much broader strategy to understand how new types of portable and mobile devices enable users to be more productive." [18]

B. Policies

Probably the most important step in the BYOD implementation process is the creation of the BYOD policy. In his CIO.com article, "7 Tips for Establishing a Successful BYOD Policy," Jonathan Hassell encourages the following considerations in regards to such a policy:

1. Specify what devices are allowed.

General technical decisions must be made. What systems and platforms will the organization support?

2. Establish a security policy for all devices.

"Users tend to resist having passwords or lock screens on their personal devices. They see them as a hurdle to convenient access to the content and functions of their device. However, this is not a valid complaint—there is simply too much sensitive information to which phones connected to your corporate systems have access to allow unfettered swipe-and-go operation of these phones." [18] Ensure that per the policy users must have stringent passwords in place that follow criteria for a strong password.

3. Define a clear service policy.

How much support will your IT department provide for personal devices used at work? The policy must draw the line in the sand and make expectations of service on such devices clear for all involved.

4. Make it clear who owns what data.

If your company deploys the process of wiping clean devices that are lost or stolen, you may also be erasing more personal data such as pictures or downloaded music.

5. Decide what apps will be allowed.

"The question here is whether users can download, install and use an application that presents security or legal risk on devices that have free access to sensitive corporate resources." [18]

6. Integrate your BYOD plan with your Acceptable Use Policy.

What is acceptable on the device? Facebook? Youtube? What about other questionable websites? Link this policy with your current Acceptable Use policy for desktop computers to set a clear understanding of what an employee should or should not do on their devices.

7. Plan an exit strategy. [18]

The policy must address how the data will be removed from the devices and access limited once the employee resigns or is terminated.

C. Training

Once the BYOD policy is in place, an organization needs to provide training on the use of BYOD to hardwire behaviors and understanding of the policy. "In the end, it's less the technology being used and more the people using it that leads to protected information becoming exposed." [19]

D. Master Data Management Solutions

Master Data Management (MDM) is a tool that IT experts recommend for organizations allowing BYOD. "Master data management (MDM) is a comprehensive method of enabling an enterprise to link all of its critical data to one file, called a master file, that provides a common point of reference. When properly done, MDM streamlines data sharing among personnel and departments. In addition, MDM can facilitate computing in multiple system architectures, platforms and applications." [20] The advantages of such a solution often include a range of platforms, asset management, remote troubleshooting and remote "wipe clean" functionality. There are many programs available to choose from with various functionalities.

E. Privacy

The healthcare industry's focus on patient privacy is regulated by law. HIPAA and HITECH compliance makes BYOD in a healthcare setting a difficult task, at best. However, another privacy issue has developed from the resent trend to allow BYOD in the workplace – employee privacy.

Some MDM programs use GPS to track employees. This is sometimes done without their knowledge. Eighty-two percent of respondents to a recent survey believed such tracking to be an invasion of their privacy. [21] Others reported concerns about allowing employers to view apps or pictures stored on their devices and having the ability to wipe them clean off the device. Having a very clear policy and employee training may help address some of these concerns. However, this may lead to fewer employees wanting to participate in the BYOD program.

VII. Conclusion

Bring Your Own Device is a growing phenomenon in the world of business. The popularity of the concept stems from employees' preferences to use their own devices on which they are comfortable and often more efficient. The advantages of BYOD includes increases in both employee and employer satisfaction for a multitude of reasons. There are also concerns and disadvantages with allowing employees to use their own devices at work. Healthcare, in particular, faces unique challenges and concerns. While the government continues to promote and enforce the adoption of Electronic Health Records, the protection of such data is mandated by federal law. BYOD can help with accessibility, but makes data breaches a concern. Protecting mobile data is challenge and a must. Organizations wishing to adopt a BYOD policy should ensure that the policy is clear, explicit, and lays out the expectations for both the employees and the organization. Education in regards to the policy and how the devices should be used needs to be part of an education and training session for all employees. It is imperative in this digital environment that the privacy of both patients and employees is protected and respected.

VIII. References

[1] T. Bradley, "Pros and Cons of BYOD (Bring Your Own Device)," CIO.com, 21 December 2011. [Online]. Available: http://www.cio.com/article/696971/Pros_and_Cons_of_BYOD_Bring_Your_Own_Device_. [Accessed 7 October 2013].

[2] T. Schadler, "2013 Mobile Workforce Adoption Trends," Forrester, 4 February 2013. [Online]. Available: http://www.vmware.com/files/pdf/Forrester_2013_Mobile_Workforce_Adoption_Trends_Feb2013.pdf. [Accessed 8 October 2013].

[3] K. Fogarty, "5 Things You Need to Know about BYO Tech," CIO.com, 16 December 2010. [Online]. Available: http://www.cio.com/article/647100/5_Things_You_Need_to_Know_about_BYO_Tech?page=2&taxonomyId=3112. [Accessed 8 October 2013].

[4] * M. K. Pratt, "Hospitals seek healthy balance with BYOD," Boston Business Journal, 2 August 2013. [Online]. Available: http://www.bizjournals.com/boston/print-edition/2013/08/02/hospitals-seek-healthy-balance-with-byod.html?page=all. [Accessed 8 October 2013].

[5] D. Bourque and S. Bentfield, "BYOD in Health Care: A Unique Range of Risk," Source Media, 25 September 2012. [Online]. Available: http://www.information-management.com/news/byod-in-health-care-a-unique-range-of-risk-10023219-1.html#Login. [Accessed 8 October 2013].

[6] SearchHEalthIT, "Use BYOD policies to integrate personal devices securely".

[7] * J. M. McGrath, N. H. Arar and J. A. Pugh, "The Influence of Electronic Medical Record Usage on Nonverbal Communication in the Medical Interview," Sage Publications, 2007. [Online]. Available: http://www.jefferson.edu/emr/documents/infl_emr_medinterview_hij.pdf. [Accessed 9 October 2013].

[8] D. Thompson, "U.S. Hospitals Triple Use of Electronic Health Records: Report," US Newsand World Report, 8 July 2013. [Online]. Available: http://health.usnews.com/health-news/news/articles/2013/07/08/us-hospitals-triple-use-of-electronic-health-records-report. [Accessed 9 October 2013].

[9] "Search Health IT," 2010. [Online]. Available: http://searchhealthit.techtarget.com/definition/personal-health-information. [Accessed 9 October 2013].

[10] Coopersmith, Gordon, Schermer& Brockelman PLC, "HITECH Act Expands HIPAA Privacy and Security Rules," [Online]. Available: http://www.azhha.org/member_and_media_resources/documents/HITECHAct.pdf. [Accessed 9 October 2013].

[11] "HIPAA Violations and Enforcement," American Medical Association, 2013. [Online]. Available: http://www.ama-assn.org//ama/pub/physician-resources/solutions-managing-your-practice/coding-billing-insurance/hipaahealth-insurance-portability-accountability-act/hipaa-violations-enforcement.page. [Accessed 9 October 2013].

[12] J. Byers, "Health Affairs: Study Puts A Price Tag on EMR Implementation in Small Practices," CMIO, 7 March 2011. [Online]. Available: http://www.cmio.net/topics/ehr-emr/health-affairs-study-puts-price-tag-emr-implementation-small-practices. [Accessed 10 October 2013].

[13] Z. Moukheiber, "The Staggering Cost Of An Epic Electronic Health Record Might Not Be Worth It," Forbes, 18 June 2012. [Online]. Available: http://www.openhealthnews.com/news-clipping/2012-06-18/staggering-cost-epic-electronic-health-record-might-not-be-worth-it. [Accessed 10 October 2013].

[14] CDC, "Meaningful Use," CDC, 11 October 2011. [Online]. Available: http://www.cdc.gov/ehrmeaningfuluse/introduction.html. [Accessed 10 October 2013].

[15] K. Villanueva, "HIPAA and the BYOD Challenge," Moss Adams, April 2013. [Online]. Available: http://www.mossadams.com/Articles/2013/April/HIPAA-and-the-BYOD-Challenge. [Accessed 10 October 2013].

[16] eClinical Works, "What is Meaningful Use?," eClinical Works, 2013. [Online]. Available: http://www.eclinicalworks.com/knowledge-center-meaningful-use-what-is-meaningful-use.htm. [Accessed 10 October 2013].

[17] MaaS360, "The Ten Commandments of Bring Your Own Device," MaaS360, [Online]. Available: http://content.maas360.com/www/content/wp/wp_maas360_mdm_tenCommandments.pdf. [Accessed 10 October 2013].

[18] * M. Austin, "British Journal of Healthcare Computing," 28 January 2013. [Online]. Available: http://www.bj-hc.co.uk/views/voxpop-wireless-networking-in-the-nhs/views-

news-detail.html?news=2367&lang=en&feed=125. [Accessed 11 October 2013].
[19] J. Hassell, "7 Tips for Establishing a Successful BYOD Policy," CIO.com, 17 May 2012. [Online]. Available: http://www.cio.com/article/706560/7_Tips_for_Establishing_a_Successful_BYOD_Policy?page=3&taxonomyId=600013. [Accessed 10 October 2013].
[20] K. Murphy, "BYOD adoption requires security education, staff training," Health IT Security, 19 June 2013. [Online]. Available: http://healthitsecurity.com/2013/06/19/byod-adoption-requires-security-education-staff-training/. [Accessed 10 October 2013].
[21] M. Rouse, "Master Data Management (MDM)," Search Data Management, November 2010. [Online]. Available: http://searchdatamanagement.techtarget.com/definition/master-data-management. [Accessed 10 October 2013].
[22] IT Business Edge, "Survey Exposes Concerns About Employee Privacy for BYOD," IT Business Edge, [Online]. Available: http://www.itbusinessedge.com/slideshows/survey-exposes-concerns-about-employee-privacy-for-byod-02.html. [Accessed 10 October 2013].

IX. BIBLIOGRAPHY

B. Kyle Marek is the Chief Information Officer and Chief Privacy Officer at Carteret General Hospital in Morehead City, NC. He obtained his B.S. in Computer Science form East Carolina University in 1998 and is currently enrolled at East Carolina University in the Masters of Science in Network Technology program. He is a member of the Health Information and Management Systems Society and North Carolina Health Information and Communication Alliance. Mr. Marek resides in Morehead City with his wife and two children.