Healthcare BYOD and HIPAA Security
The Issues and a Solution

Introduction

Much has been written on the subject of allowing clinical staff to bring their own devices (BYOD) into a healthcare environment. Typically, the issues that are addressed are the necessity of setting policies because BYOD raises HIPAA concerns like protecting patient information; setting policies that involve IT restrictions; and having security officers to ensure that technical safeguards are in place and non-compliance risk (liability) is managed.

The topic that has been frequently addressed as a possible solution is to have a Cloud-based application as a service where confidential patient information is stored on a secure server, and when a staff member leaves the premises of a medical facility, no patient information leaves with them on their personal mobile devices.

However, when broaching the subject of Cloud-based applications, too often the conclusion is that healthcare institutions each need to have their own IT department develop this Cloud-based solution, or implement an “off the shelf” mHealth package that fits the needs of the facility. As a result, due to excessive amounts of development time and energy, the all-too-often lack of resources, either technical or financial, or the uncertainty of which already developed mHealth application to use (there are over 20,000 mHealth apps available), many healthcare facilities are opting to restrict or completely prohibit BYOD.
The intent of this whitepaper is to first look at BYOD concerns and policies set into motion because of the growing movement of staff at healthcare institutions – across the country and worldwide – using personal mobile devices, like the iPhone and iPad, to take care of their patients; and second to examine how iClickCare, a monthly subscription-based Software as a Service (SAAS), offers an answer to those BYOD issues healthcare institutions are being forced to address.

**What is BYOD?**

According to an article titled *BYOD Issues and Solutions for Healthcare Safekeeping* written by Scott Parker:

“The term ‘Bring Your Own Device’ (BYOD), was initiated in the year 2009 by a top IT company and it pertains to the policy of allowing employees to bring privately owned devices such as smartphones, tablets and laptops into their workplace for use and access to company applications and information.”

As of the end of 2013, Bryan Honigman, in his article *The Major BYOD (Bring Your Own Device) Issues Facing the Healthcare Industry* writes that “…four out of five medical providers were using their own personal devices at work. “BYOD or ‘bring your own device’ is becoming more commonplace across the world as the use of mobile devices continues to rise.”

**What are the Positive Aspects of BYOD in Healthcare Facilities?**

- Requires less or no training on the device
- More reachable clinical staff at any hour
- Less costly than purchasing separate mobile devices for staff and employees
- More convenient to have one device for both personal and professional uses
- The belief that having a personal device at work enhances morale and improves productivity

**What are the BYOD Issues Facing Healthcare Facilities?**

The overriding concern at a healthcare facility is HIPAA compliance – protecting confidential patient data, including both information and images (pictures, videos). Stemming directly from this overarching priority, are these needs:

- A decisive mobile device policy
- Healthcare IT control and management
- Security procedures in place
- Liability coverage due to HIPAA non-compliance
A decisive mobile device policy

A mobile device policy could be a subsidiary or additional document to an existing more generalized computer usage policy. The most important factor in a mobile device policy would be to stipulate that while staff members might be using their own mobile devices to access healthcare data, the data itself is still “owned” by the healthcare organization, and that all activities and apps related to accessing patient data needs to be monitored and logged.

According to a HealthITSecurity article titled ‘Aligning healthcare BYOD security policies with IT infrastructure’, written by Bill Kleyman in May of 2013:

“The idea is a separation of responsibility. The healthcare organization really should focus on the workload that is being delivered – rather than the device that is accessing the information.”

Healthcare IT control and management

The BYOD movement is forcing healthcare institutions to develop and manage or put into place some kind of mobile mHealth app that protects the security of the healthcare facility’s network and, most importantly, manages or controls access to patient data. According to an article written in SearchHealthIT in mid 2012:

“The iPad represents a significant slice of a mobile connectivity pie that will reshape health care, according to Deloitte’s 2011-12 Open Mobile survey, which calls health care the sector most likely to benefit from 4G technology in the coming years.”

IT development, and testing of the mobile BYOD app

The constraint of money and excessive time for a healthcare institution’s IT department to develop, test and deploy their own mobile app, has resulted in healthcare facilities installing and managing already developed mHealth apps:

“Few health IT leaders outside Beth Israel Deaconess Medical Center CIO John Halamka, M.D., or his peers saw the iPad as a health care game-changer upon its release two years ago. Now however, CIOs increasingly view iPad EHR implementations as a way to promote meaningful use compliance among physicians, who love the device. Meanwhile, virtualization vendors are making those implementations more workable.”
Chris Apgar, president of Apgar & Associates in Portland, Oregon, a company that provides expert privacy, information security, HIPAA, regulatory and electronic health information exchange consulting services, says that Apgar sends healthcare clients checklists that security leaders can share with employees who use their own device. It includes items such as:

- I agree the hospital may remotely wipe my device and destroy all data on the device if it is stolen
- I agree if the hospital sees my private information in the course of a security assessment, I will not sue the hospital
- I agree I will turn over my device if it’s needed to conduct a security investigation

Changing mindsets come down to strict adherence to policies and procedures and staff training. “You’ve got to have the staff dos and don’ts,” Apgar said. “Make sure there’s a process. Make sure they know what you’re allowing and not going to allow.”

HealthITSecurity, in its *BYOD BEST PRACTICES GUIDE Tips for Healthcare Organizations Implementing Mobile Strategies Forward*, states:

“In addition to the technology component of securing personal devices, creating tight policies and ensuring that all staff members understand the organization’s BYOD strategy is a key element to allowing these devices onto an organization’s network. Some policies allow staff members to only access corporate emails and calendars from their personal devices. Others allow more freedom but either reserve the right to wipe the phone entirely or have data “sandboxed” so it doesn’t touch other data on the phone. Regardless of what best fits your organization, this guide runs the gamut on the different policies and options that organizations have when deciding to adopt BYOD.”

**Healthcare security procedures in place**

Deciding to allow clinical staff to bring their own devices into a healthcare setting is not only a technical decision but also one that requires strong policies and procedures in place if patient data is going to remain secure.

OnsiteRIS, in their article ‘*BYOD and Healthcare – What you need to know about using Smartphones in your Healthcare practice*’ states that:

“…regulatory entities like CMS and HHS are drafting stringent requirements for the use of Electronic Health Records (EHRs) and interoperable medical IT devices to ensure the protection of valuable company data and protected health information (PHI).

In order to decrease the negative side effects of BYOD, many hospitals’ IT companies are deploying BYOD strategies to prevent information breaches from occurring. It’s essential
that healthcare organizations carefully outline the policies regarding BYOD prior to implementing them.”

The following is a brief description of key security measures that must be aligned with BYOD and EHR systems at healthcare facilities:

**Determination of mobile devices and platforms supported**

This includes bandwidth requirements based on the number of users, locations, transactions in real-time, hardware and storage capabilities, technology, mobile devices and platforms that will run an IT developed app – depending on the requirements of a healthcare facility’s EHR (Electronic Health Record)/EMS (Electronic Medical Services) vendor.

According to Brian Honigman, in ReferralMD’s ‘**The Major BYOD (Bring Your Own Device) Issues Facing the Healthcare Industry**’, “Federal law requires that a healthcare institution deploy a single network to handle the bandwidth created by all these mobile devices, as well as a way of securing all the information passing through this wireless LAN.

Many IT departments must upgrade their existing systems to ensure they’re able to scale with the ongoing needs required from most staff members practicing BYOD.”

**Firewall constraints to control access to patient data**

While firewall settings can only get healthcare security officers so far when implementing technical safeguards, it is critically important for healthcare institutions to install and maintain a firewall as part of the facility’s Internet gateway. To ensure that healthcare data is absolutely protected, the firewall should only allow limited legitimate access to a facility’s network and patient-related data.

**Intrusion detection**

Installing an intrusion detection system (IDS) is intended to prevent unrecognized or non-legitimate traffic, especially attempts of well-known network attacks.

**Substantial network support**

Mr. Honigman writes that,

“According to the Journal of Mobile Technology in Medicine, 91% of healthcare professionals owned a mobile phone of which 87% used it during clinical practice.”
That could potentially be a huge strain on your hospital’s network from staff, as well as the use of mobile devices of patients and their visitors.

The IT department at your facility is tasked with the challenge of ensuring that your hospital’s network can withstand the demand by this addition of hundreds, if not thousands of connected devices. Your hospital’s wireless LAN handles the exchange of the majority of this sensitive information and therefore, must be consistent, continuously available for use and reliable in order to perform correctly around the clock.”

One method of handling the massive strain on a healthcare facility’s network is segmentation of patient data. The intent of this network segmentation is to limit access to only those users requiring connectivity to EHR data.

**Encryption of all patient-related information**

Encrypting all patient data is paramount. Many physicians and healthcare staff use their own devices to store confidential patient data, text colleagues about their patient’s condition or diagnosis, or pass patient photos over the internet attached to an email without realizing that all of their actions are NOT HIPAA compliant, and can result in litigation and liability for themselves and their healthcare facility.

Here is an excerpt from an online article titled ‘Encryption essential to BYOD security’ from Thawte:

“According to tech expert Ken Hess in a security trend watch at ZDNet, encryption is one of the most robust defenses against data breaches between different network devices. It’s the most widely used risk control measure, he reported, and a direct response to one of the primary concerns of technology professionals: unauthorized access to data and resulting data loss.”

**Registration and management of mobile devices being used**

There should be a scheduled review of BYOD user access. Typically, clinical staff at a healthcare facility have few if any administrative rights to an EHR system. Administration of that EHR system would be the responsibility of the IT department, along with centrally managing BYOD user rights.

**Assignment of a unique PIN for staff accessing patient data with a mobile device**

BYOD users should only have access to an EHR system using a strict authentication process (i.e. strong passwords, smartcards, tokens). There should be a scheduled review of BYOD user access.
Remote-uninstall of patient data and app on discharged employees or lost mobile devices

Megan Van Vlack, in THE COMPANY ETHICIST “New Patient Privacy Protections = the End of BYOD for Hospitals?” quotes Kelli Fleming, a lawyer with Burr & Forman in Birmingham, Alabama. In writing for Inside Counsel, Fleming lists “Enable remote device wipe” as one of the best ways hospitals can help “ensure that workers who use their personal devices on the job are compliant with the law”:

“Remote wiping and disabling allows you to remotely erase any data stored on mobile devices or to remotely lock mobile devices. This is an extremely valuable tool in preventing an inappropriate use and/or disclosure of information if a mobile device is lost or stolen, which occurs all too frequently.”

Audit of all actions and patient-related data on a mobile device

Audit the EHR system structure to ensure compliance with strong security standards.

Liability coverage due to HIPAA non-compliance

Ben DiPietro, wrote in the Wall Street Journal, in September of 2013:

“Health care providers and their business associates have to comply with new rules to protect patient information starting this week, and that could complicate how they design and implement policies to govern the growing use by medical professionals of their own devices at work. Under the Health Insurance Portability and Accountability Act and the HITECH Act, violations could bring fines starting at $50,000 per incident.”

Patrick Ouellette, an IT expert and HealthITSecurity.com editor wrote an article in December of 2013 on “2014 Cyber Security Forecast: Significant healthcare trends”.

His list of the top 7 trends includes:

As Cloud and BYOD adoption continues to accelerate, greater accountability will be required for implementing policies and managing technologies.

The development and evolution of Cloud services and BYOD has moved at a whirlwind pace, leaving IT departments scrambling to get out in front of the technologies and employee usage. In 2014, IT leaders will need to work closely with senior leadership and legal counsel to adapt corporate policies in a way that addresses changing legal risks, while effectively meeting the need of the organization.

“Up until now, cloud and BYOD adoption has been like the Wild West – uncharted, unregulated, and few restrictions. However, we’re seeing courts issue rulings that include significant penalties where discovery, disclosure and other legal obligations
aren't being met because of the use of these technologies,” said Brill. “While it's implausible to anticipate every possible risk presented by the use of the cloud and BYOD, companies that have integrated these technologies into their corporate policies, IT security, and risk management plans will be much better prepared to fulfill their legal obligations. Organizations must realize that even if they don't want to deal with this, they're not going to have much choice.”

How is iClickCare an answer to BYOD and HIPAA Security?

What if there already is a Software as a Service (SAAS) application, that has been developed and constantly maintained as a completely HIPAA compliant solution? A service that enables encrypted secure transmittal of text, images, videos and even PDF forms? A service that can ONLY be accessed via an administratively approved unique login or single sign-on (SSO)? And a service that has been optimized for the iPhone and iPad so that device can also be used to take and store HIPAA secure photos and videos?

Cloud-based

iClickCare is a Cloud-based Software as a Service (SAAS) internet application, that has been conceived and developed by doctors for medical providers who need to consult with their medical colleagues and other medical providers to provide patients with the best medical care. In the process, using iClickCare can reduce the need for pre-scheduled video conferencing, the ever-present issue of “telephone tag”, excessive amounts of waiting on the patient's part, misdirected referrals to specialists, unnecessary hospital readmissions and as a result can help to drastically increase the ROI of any size medical facility.

HIPAA Secure on multiple platforms and devices

iClickCare can be used with any modern platform, on a desktop browser or mobile device like smartphones and tablets. Maintained as a completely HIPAA compliant solution, iClickCare is a service that has 128 bit SSL encrypted secure transmittal of text, images, videos and even PDF forms.

HIPAA Secure patient photos and videos

iClickCare has also been optimized, with a user interface that takes advantage of the user experience on both the iPhone and iPad. Optimized to run on the iPhone or iPad also means that the device's camera can be used to take high quality photos, and short videos, which then get stored in iClickCare's HIPAA secure Camera Roll.

To login to iClickCare, you need either a cellular or WIFI connection to the internet.
Unique login and Single Sign On (SSO)

Each medical facility that subscribes to iClickCare, has a selected administrator, personally trained by a ClickCare Consultant. That administrator is responsible for setting up each clinical staff member’s unique login or single sign-on (SSO) access – to only their patients’ information – and for assigning each medical provider to their respective group within the healthcare facility, so that members of a medical facility group, like the ER or the ICU can access their patients’ demographics, descriptions of their condition, and collaborations with other colleagues regarding their patients’ diagnosis and treatment.

Having such a solution has a number of benefits at the policy and decision-making level:

- IT does not need to develop their own application, or research the 20,000 mHealth apps developed for mobile devices, so resources can be devoted to other, more pressing needs.
- Since the solution is Cloud-based and patient information is stored on a remote server, there is no need to have a BYOD security policy related specifically to the use of the mobile app, or security officers to enforce that policy.
- There is no need to register a set number or type of devices, or provide support for only certain platforms, because access to patient information is determined by a facility administrator, and the solution is accessible from any modern browser or mobile device.
- There is no overlap of BYOD personal data and confidential patient data.
- There is no HIPAA non-compliance risk to a medical facility because the staff never accesses the internal network of the facility.
- There is no need to implement firewall settings to ensure the security of internal data or patient information.
- There is no need to develop auditing procedures, as mandated by HIPAA. Every action is captured and stored for auditing purposes.
- There is no need to “wipe” a mobile device or uninstall any software because a device is stolen, lost or a staff member permanently leaves a facility.

Bill Ho, president of Biscom, a market leader in secure electronic document communications and file transfer technology, wrote an article for Hospital Review titled “Mobile’s Impact on Hospital IT Security in 2013: How Your Institution Can Adapt to BYOD”. In the online article, Mr Ho says that:

“According to a recent survey of 130 hospitals by Aruba Networks, 85 percent of facilities support their physicians’ and staff’s use of personal devices at work. The survey also revealed that of the facilities that support their physicians’ and staff’s use of personal
devices at work, 83 percent specifically support the use of Apple iPads on the network. A majority of healthcare institutions will have to address BYOD in the coming year; smartphones and tablets are being adopted at such a high rate that hospitals are almost compelled to support them. Therefore, when a radiologist, a surgeon or an oncologist wants to use his or her device, IT sometimes has no choice but to both support it and secure it. In many circumstances, BYOD can be a net positive for hospitals as it promises quicker responsiveness, more accessibility to physicians and an overall improvement on patient care. However, IT staff responsible for healthcare security regulations now have a new and complex challenge to solve: supporting healthcare professionals who bring their hospital setting while still maintaining the security and confidentiality of personal health information. Hospital IT staff know that it’s not just a technical issue but that BYOD may also require healthcare regulation policies to change and for additional education to be provided to mobile users.”

After coming to terms with BYOD being a reality that healthcare institutions, their IT and legal departments are being compelled to support, reviewing the BYOD issues presented in this whitepaper, you should have the information you need to evaluate how subscribing and using iClickCare can be the BYOD solution you are looking for.
ClickCare LLC and iClickCare at a glance

Who is ClickCare LLC?

ClickCare LLC developed ClickCare Classic in 1995, when a pediatrician needed to advise and assist her nurse practitioners in an off-site school clinic. At the same time, email utilization began spreading, secured lines from schools became a reality, and digital cameras had just become commercially available.

From the consultations with the nurse practitioners, an archive of medical cases was assembled manually to show others the idea of being able to transmit pictures and communicate securely using the Internet. Healthcare professionals started getting excited by the idea.

After trying the then-available telemedicine systems, it became clear that any useful system would need to be inexpensive, accessible via the web, and very user-friendly to be widely accepted. The first providers immediately loved the simplicity and power of Store-and-Forward.

Since its beginnings in upstate New York almost 20 years ago, the mission of ClickCare LLC has always been to improve patient access, provider collaboration, and student education.

What is iClickCare?

iClickCare®, launched in 2010, is a subscription-based app for medical professionals that takes the capabilities of ClickCare Classic to a whole new level. First to market and patent-pending, iClickCare enables any medical provider (such as generalists, specialists, hospital and homecare nurses, school and sports healthcare professionals, etc.) to easily create and archive patient visit records, complete with patient demographics and history, presentation of patient symptoms and condition, including pictures and videos; to create a personalized network of other medical colleagues to consult with on the diagnosis and best treatment plan for the patient; to invite a family member to participate in the patient’s care, and much more.

With the wide adoption of the iPhone and iPad by healthcare organizations, iClickCare was developed both as a mobile iPhone/iPad app and an application that can be run in a standard browser on a computer – all accessing and displaying the same set of patient data stored on a remote HIPAA secure server.
What others have to say...

From Google: The New York Business Development Center selected ClickCare, LLC, owned by Drs. Cheryl and Lawrence Kerr in Vestal, for the Small Business Excellence Award...Their product is a cutting-edge telemedicine service that provides a HIPAA secure transfer of pictures, video and medical information.

Prestonwood Rehabilitation: “With iClickCare we have the ability to refer back to online conversations, visit details and pictures which has assisted in many improved outcomes for patients.

Health2.0News: ClickCare, a HIPAA secure store-and-forward collaboration platform for providers, launched the iClickCare app for the iOS systems. The app enables the healthcare providers to exchange information using text, pictures, video, and PDFs, and creates archives of all cases for future reference.

Bloomberg Business Week: ClickCare, LLC provides a web-based software service for medical collaboration. Its services allow users to collaborate with their consultants using pictures, videos, and texts.

HealthValley: Designed by healthcare providers for healthcare providers, ClickCare focuses on the importance of and increasing need for collaboration within the healthcare industry. Using a desktop or ClickCare’s mobile app called iClickCare, healthcare professionals can have an online avenue for quick consults. Users can share information and media related to patient problems and get instant answers from peers or specialists.

EMR & EHR, Health and Cloud Computing, A Promising Start: iClickCare, a HIPAA compliant SaaS and iPhone application combines pictures, text, sounds, and videos to improve collaboration between healthcare providers. In one instance, at the Wound Institute in PA, 70 patients were treated solely over ClickCare with an overall healing rate of 93% and an estimated savings of $24,000 in transportation costs.

eWeek: HIPAA compliant iClickCare combines pictures, text, sound and videos, and enables healthcare workers to discuss patients securely over the web with colleagues. The whole process starts with a question or a need for collaboration. A healthcare worker just logs into iClickCare from the iPhone, iPad, a laptop or desktop. He/She adds the patient’s demographics along with any number of digital photos, videos, sounds or other media. A question about the patient can be asked or a plan of treatment put forth.

For more information or to schedule an iClickCare demo, talk to a ClickCare Consultant at +1 (800) 814-5840 or email us at info@clickcare.com.