Introduction

The use of mobile devices in healthcare is more than just a passing trend; it is a movement changing “business as usual” in the hospital environment. Healthcare providers (HCPs) are embracing mobility to help enhance patient care and improve operational efficiency, but must also adhere to strict federal compliance standards. Tablets and smartphones are becoming a staple in the daily routines of doctors and healthcare professionals across the industry, transforming the way that they access a number of medical applications, as well as electronic patient health information (ePHI). However, the introduction of mobile devices into this highly regulated industry does pose certain challenges.

In this whitepaper, we’ll explore how mobility is changing the healthcare landscape, the challenges posed by mobility in ensuring the privacy of patient information, and how healthcare organizations can meet these challenges to become a leading mobile healthcare institution.

More than Just a Fad: How Mobility is Changing Healthcare

Implementing a mobility solution in healthcare institutions can prove to be very useful for many reasons. It used to be that physicians, nurses, and healthcare service providers were limited in their access to patient information and health records, but...
mobile access to this information unlocks new methods for delivering improved patient care, and enables increased operational efficiencies for the institutions themselves. Though the majority of physicians are utilizing mobile devices for patient care – subsequently forcing HCPs to embrace mobility strategies – these strategies are still in their infancies. Questions are still being asked about the importance of and how to best use mobile devices and medical apps to provide day-to-day support to physicians, ultimately resulting in improved and efficient patient care.

Physicians, nurses and other healthcare professionals can benefit from embracing mobility in a number of ways, from increasing administrative efficiency to improving patient satisfaction. A few key benefits include:

**Anywhere, anytime access to critical information.** Remote patient monitoring cuts down on unnecessary visits to doctor’s offices and hospitals.

**Collaboration between healthcare professionals and institutions.** Doctors can share patient data with colleagues in different geographic locations.

**Faster, more efficient patient care, administration, and research.** Increased workflow, faster diagnoses and response times as doctors can review test results, design treatment plans, seamlessly transition between patient charts and update information on the go, allowing more time for patient care.

**‘Go Green’ with a transition into a paperless file system.** Patient records, administrative files, presentations, and other documents that typically had to be printed out are now available electronically, cutting down on paper costs.

### The HIPAA Mobility Challenge: Securing the Privacy of Patient Information

Healthcare institutions must be able to ensure the privacy and security of patient health information (PHI) in accordance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) at the risk of penalties, loss of consumer trust and fines exceeding $1.5 million. Mobile devices introduce new challenges for healthcare institutions in complying with HIPAA, so it is important that institutions and professionals alike understand these challenges in order to most efficiently mitigate the risk associated with introducing mobile devices into the network.

HCPs have struggled to keep up with the pace in which mobile devices and associated medical services and apps are demanded. In a race to give physicians and other healthcare professionals what they need, the quality and security of the devices and apps can often be sacrificed for quantity. Without security protection in place to protect patient data that also complies with HIPAA, the full potential of what doctors can do with mobile devices is severely limited.

According to the U.S. Department of Health and Human Services, the number one cause of data breaches is device theft, which can lead to unauthorized access to confidential files. In order to fully educate HCPs on how to comply with the U.S. Federal

---

HIPAA legislation and avoid major fines, IT must implement the proper security measures to make sure that all mobile devices follow four major rules:

- Must ensure privacy of PHI through transmission, storage, secure access to, and management of ePHI.
- IT must enforce strict access controls for administrative purposes.
- Security infrastructure in place to protect against malware, cyber threats, and employee error (lost, stolen, or otherwise compromised devices).
- Business associates, such as healthcare service providers, must comply with HIPAA standards in order to be eligible to work with HCPs.

To be sure that all HCPs are adhering to the outlined HIPAA standards, in February 2012 the Department of Health and Human Services (HHS) launched a program dedicated to randomly performing security audits of HCPs. The HHS conducts rigorous reviews of HIPAA compliance and randomly targets entities of all types, though it encourages covered entities to perform self-audits throughout the year as well. If an HCP is found to be non-compliant, it is referred to the Federal Office of Civil Rights (OCR) for enforcement.

In the case of non-compliance, any healthcare organization can face stiff financial penalties. Some of the most recent HIPAA infractions and associated penalties that the OCR has distributed include:

- Blue Cross Blue Shield of Tennessee – Fined $1.5 million after 57 unencrypted hard drives were stolen from a facility in Tennessee containing PHI of over 1 million individuals.  
- Cignet Health of Maryland – Fined $4.3 million for failing to provide patients with access to their own medical records and subsequently failing to cooperate with OCR investigations.

**How to Establish Trust and Credibility: Managing ePHI on Mobile Devices**

The Security Rule, or “Security Standards for the Protection of Electronic Protected Health Information,” specifies a series of technical safeguards for covered entities to use to assure the confidentiality, integrity, and availability of electronic protected health information. These technical safeguards directly apply to mobile devices and a thorough understanding of these safeguards can help healthcare institutions embrace mobility securely, in accordance with HIPAA.

To protect ePHI, covered entities must carry out the following HIPAA technical safeguards:

**Access Control**

Policies must be implemented to only allow authorized persons to access ePHI. This can be done through Active Directory integration to manage access on multiple levels and prevent data leakage.

**Audit Controls**

Must implement hardware, software, and/or procedural mechanisms to record and examine all activity in information systems related ePHI. This includes monitoring all operative functions, notifications to changes, and system audits on all accessed servers.

---

**Integrity Controls**
Must implement policies and any necessary electronic measures to ensure that ePHI is not altered or destroyed. IT can prohibit the ability to modify, share or restore deleted files, and must perform regular integrity checks.

**Transmission Security**
To guard against unauthorized access and electronic transmissions of ePHI, entities must implement technical security measures to heavily encrypt any data that is in transit and at rest on mobile devices.

Managing hundreds, possibly thousands, of mobile devices throughout a healthcare organization is difficult, especially when IT management activities cannot interfere with clinical duties in risk of losing critical patient data. Understanding the risks and consequences of security threats to ePHI is critical to ensuring that HCPs will properly implement HIPAA compliant technical safeguards to protect all patient data.

**Conclusion**
The number one priority for healthcare institutions allowing the use of mobile devices on the job should be maintaining the confidentiality and privacy of patient information. This not only ensures HIPAA accordance to avoid fines and other penalties, but preserves consumer trust as well. When mobile devices are securely incorporated into HCP networks under HIPAA standards, mobility can generate increased operational, administrative and clinical efficiencies between service providers, which translate to improved overall patient care and experience.

By recognizing the challenges of mobility and taking steps to prepare for them, every healthcare organization and service provider can deliver higher quality care to patients, while also cutting costs and increasing job satisfaction for physicians and other professionals.

**About Acronis**
Acronis® is leading the next wave of data availability, accessibility and protection solutions to simplify today’s complex IT environments. Acronis technology enables organizations of all sizes to manage the always-on anywhere data access demands of users, reducing risk against the loss of valuable corporate data, and controlling management and storage costs. With proven technology for data migration and disaster recovery for physical, virtual and cloud environments, and secure enterprise file-sharing and synchronization regardless of type or platform, Acronis is enabling organizations to embrace new IT strategies and options such as BYOD and Mac® in the enterprise.

For additional information, please visit [www.acronis.com](http://www.acronis.com). Follow Acronis on Twitter: [http://twitter.com/acronis](http://twitter.com/acronis).

For additional information please visit [http://www.acronis.com](http://www.acronis.com)

To purchase Acronis products, visit [www.acronis.com](http://www.acronis.com) or search online for an authorized reseller.

Acronis office details can be found at [http://www.acronis.com/company/worldwide.html](http://www.acronis.com/company/worldwide.html)