Mobility in healthcare: Upholding regulatory compliance with HIPAA, HITECH and more

IBM MaaS360 provides industry-leading enterprise mobility management for healthcare organizations

IBM

Introduction

The number of mobile devices in healthcare facilities is increasing rapidly, as is the diversity of mobile applications, operating systems and communication methods that healthcare organizations must support. In the words of Federal Communications Commission (FCC) Chairman Julius Genachowski, healthcare is being "transformed" by broadband, wireless and mobile technologies.[1] The FCC actively supports mobility in healthcare with strategies that include fostering innovation in networks, devices and applications; encouraging adoption of life-saving technology; and ensuring optimal use for the broadcast spectrum.[1]

Meanwhile, as communications professionals in healthcare begin to recognize the impact of mobile technology in their environments, healthcare providers recognize the benefits that can be achieved from utilizing this technology to its fullest. A survey of healthcare providers[2] revealed three clear expectations for mobile technology in healthcare:

1. Stem the rising costs of healthcare processes
2. Increase staff productivity
3. Improve patient safety

Mobile puts PCs out to pasture with the COWS

In their infancy within healthcare, computing technologies were limited to desktops and workstations. Next came computers on wheels (known as "COWS")—desktop computers affixed to carts that could travel from nurses' stations to patients' rooms. These mobile units were cumbersome, and their popularity was short-lived. Their demise was further hastened by the increasing availability of a newer, more mobile technology: the laptop.

Despite their portability, even today's laptops are becoming obsolete. With anytime, anywhere access to patient data becoming the standard for efficiently and effectively delivering care, healthcare providers consider agile mobility a must. Combined with the preference of many doctors to bring their own devices (BYOD) to work, the need for agility has made smartphones and tablets the preferred mobility tools in the industry.

On these devices, healthcare professionals also use a variety of applications—and they demand the same ease of use, functionality and access to information in their work-related applications that they have on their personal, mobile applications. To this end, the tablet is being looked to as the new patient chart. Patients, too, are using mobile devices and apps to manage their health, connect with providers and access their medical records.

Patient safety and care come first

Improving patient safety is another factor driving adoption of mobility in healthcare. According to a report[3] from the US Department of Health and Human Services, the number and severity of patient safety incidents can be significantly reduced with automated information detection and computerized records. Electronic access to information can reduce the potential for errors, since information is no longer transcribed by hand from document to document.

Mobility can also improve patient care and outcomes, as mobile devices provide easy, quick and accurate access to clinical notes, lab results and patient history. This can enable more productive and efficient patient visits, and more timely decisions about care. With mobile devices, information can easily be shared across the organization and with other providers working with the same patient.

With the low cost of smartphones and tablets compared to desktops and laptops, healthcare organizations can realize a cost savings whether devices are supplied by the provider as part of the corporate computing environment or by users in a BYOD setting.

HITECH and HIPAA demand proper security

While the case for mobility in healthcare is solid when it comes to improving care, increasing productivity and reducing costs, it does face some tough challenges in this highly regulated industry. As the proliferation of devices continues, more and more sensitive information regarding patients and their care facilities is finding its way to the wrong places—creating a struggle for IT departments to properly manage security policies and mobile technology.

Of particular concern for healthcare organizations are the requirements of the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH).[4] HIPAA, enacted in 1996, addresses a set of national standards for the use and disclosure of individuals' health information to provide quality healthcare and protect patients' privacy.

HITECH, enacted as part of the American Recovery and Reinvestment Act of 2009, focuses on patient care and safety and clinical efficacy. According to the US Department of Health and Human Services, many breaches reported since 2009 under the HITECH Act have been the theft or loss of mobile computing devices, resulting in the exposure of patients' protected health information.[5]

Healthcare organizations, and even individuals, that fail to comply voluntarily with these standards may be subject to civil penalties and criminal prosecution. Penalties can vary significantly depending on factors such as the violation date, whether the organization knew or should have known of the failure to comply, or whether the organization's noncompliance was due to willful neglect. Civil penalties can range from USD100 to USD50,000 or more per violation, with a calendar year cap of USD1.5 million, and an individual may face a criminal penalty of up to USD50,000 and up to one-year imprisonment.

Potential risks to patient privacy and healthcare data are tremendous, and noncompliance with these requirements can result in severe financial penalties, criminal prosecution and, most importantly, damage to a provider's reputation.

A mix of healthcare device use cases

The need to uphold regulatory compliance is perhaps as strong as the need to provide security across platforms and across a mix of user-owned and corporate-owned devices. BYOD programs, for example, may lead users to expect support for their devices regardless of make, model or year—when in reality, many businesses support only specific versions of Apple iOS, Google Android or Microsoft Windows.

Increasing the complexity for IT, there are multiple use cases for supporting smartphones and tablets that have been identified in healthcare environments:

- BYOD—managed device: Device ownership is maintained by the user, and device management rights are provided to the healthcare organization.
- BYOD—unmanaged device: Device ownership is maintained by the user, and management rights are generally restricted to only organization (corporate) apps.
- Corporate-owned: Device is procured, distributed and fully managed by the organization.
- Shared device: Device is procured, distributed and fully managed by the organization but shared by several users such as nurses, doctors and healthcare workers

The EMM solution

With so many options and so much complexity, how does a healthcare facility or provider cover all these categories? The answer is enterprise mobility management (EMM).

EMM capabilities are delivered by software designed to secure, monitor, manage and support mobile devices deployed across mobile operators, service providers and enterprises.

The purpose is to provide security on a mobile communications network, while supporting multiple devices with multiple owners. EMM functions include over-the-air distribution of applications, along with data and configuration settings for the full range of devices, including smartphones and tablets.

Consider the doctor who goes out to lunch directly from a patient's bedside—and leaves behind her tablet. Not only has an expensive belonging been left behind, but so have all of its contents, including private patient records. Without EMM capabilities, someone could walk away with the device and gain access to its highly confidential data. With EMM, the doctor can report a loss to IT, and the patient data can be remotely wiped clean, saving the organization hefty compliance fines and embarrassment while preserving patient privacy.

"We had quite a mix of devices in use at the hospital, from those distributed by us to personal ones brought in by the clinical and administrative staff."

—Peter Param, Manager of IT Security, St. Vincent's Hospital, Sydney, Australia

EMM delivered through the cloud

IBM® MaaS360® uses a cloud-based delivery model to manage and secure all types of mobile device platforms used in healthcare facilities, helping enable compliance with HIPAA and other regulations, satisfy auditors and reduce the cost of managing mobility. It provides users with the flexibility to work anywhere, any time, while giving IT the tools to secure, monitor and maintain mobile assets—including facility- and user-owned devices, applications and data—on the network.

With MaaS360, a healthcare provider can configure devices over the air, track assets across the organization, secure access to sensitive patient data, protect chat messages among workers, distribute applications and documents, and ensure that devices are compliant with the institution's policies and industry standards.

The cloud-based delivery model provided by MaaS360 enables healthcare facilities to meet their unique industry demands. Take, for example, the employees who are hired for short-term assignments or who work for multiple healthcare organizations—often using mobile devices that are difficult to support because the owners are not part of the dedicated staff. Operating in the cloud, however, MaaS360 can effortlessly scale up or down to support as many or few users as needed. It can also provide solutions at a lower initial cost, with less set-up expense than on-premises solutions.

In the event that a doctor loses a device, selective wipe is one of the solution's most important features. A doctor using her own device may have personal as well as patient data on it. With other EMM solutions and approaches, the user loses everything when a device is wiped. MaaS360 compartmentalizes personal data from professional and patient data to prevent this.

Laying out the EMM strategy

Healthcare facilities and providers should ask the following questions when considering EMM:

- What kinds of devices are going to be on the system—and what kinds are anticipated in the future?
- How many devices are going to be on the system during its initial roll out—and how many are anticipated in the future?
- What use cases, including BYOD, will be supported?
- Who in the organization will be able to use a mobile device and what type of support will they get from IT?
- What level of security policy management will the organization need for the EMM system?
- What device features do you need to restrict for certain individuals or groups?
- What applications and data are currently needed on devices, and what may be required in the future?
- What type of mobility operations and compliance reporting are required?

Initially, the most important concern is to make sure that the EMM offering meets the requirements of regulations, including a managed BYOD program.

After that, it is important to consider applications, especially those that aid in viewing and managing electronic health records. These usually begin as single, large, system-wide applications, but they are often supplemented with smaller, niche ones used by various departments. As a result, the organization needs an EMM solution with greater capability—not only to lock down devices, but also to manage and secure applications and make sure they are being used correctly, especially when it comes to upholding regulatory compliance.

MaaS360 in action

JourneyCare, a not-for-profit agency headquartered in Barrington, Illinois, has provided pain and symptom management and end-of-life expertise to young and old in 10 Illinois counties. When nurses in the field began utilizing company-owned mobile devices to access patient data and complete point-of-care charting, JourneyCare recognized the need to increase security in order to maintain HIPAA compliance.

As a non-profit agency that handles sensitive personal health information on a daily basis, protecting corporate data is of the utmost importance. A data breach would not only result in extensive fines for JourneyCare, but also compromise its reputation in the field and the funding required to provide end-of-life care for its patients.

JourneyCare's IT team recognized the need for a cloud-based EMM solution to securely support its field organization without incurring the additional costs of implementing an on-site solution. The JourneyCare team researched three solutions to manage their fleet of more than 200 Apple iPhones and iPads. MaaS360 was the only solution that provided the features and security functionality JourneyCare was looking for to handle its enablement and compliance requirements. The team was very impressed with the reputation of MaaS360 in the healthcare industry and with its customer reviews.

"The cloud-based solution was a great selling point," said Eric Jensen, IT network specialist at JourneyCare. "As a non-profit, we would have had to seek additional funding for the required hardware to support an on-site solution. MaaS360 enables us to leverage the functionality of the solution without a significant hardware investment."

Mobile devices are easy to lose, making the need to secure corporate data even more vital for JourneyCare to ensure HIPAA compliance. The location tracking functionality of MaaS360 enables the IT team to track and recover lost devices. Additionally, through the MaaS360 solution, JourneyCare's IT team is able to wipe lost devices remotely to make sure corporate data is not vulnerable.

"The ability to perform remote wipes is priceless in this industry," said Jensen. "A HIPAA violation can result in fines of USD50,000 per patient. The loss of a single phone can result in astronomical fines depending on the number of patients' information compromised."

MaaS360 has enabled JourneyCare to successfully support its remote fleet of mobile devices while maintaining the high level of data security required for HIPAA compliance. Through security features such as location tracking, reporting and the alert center, JourneyCare is able to proactively monitor devices to avoid costly security breaches caused by lost or stolen devices. In the first year alone, JourneyCare utilized these features to recover five to six iPhones.

Nurses can now complete point-of-care charting and remotely check on the status of patients via secure, encrypted patient data. Timesaving applications and documents are pushed to devices. In addition, MaaS360 has enabled IT to make policy changes on devices remotely, without any user interaction, reducing the time and costs associated with travel to corporate offices for remote employees and volunteers. All of these efficiencies have been realized with little to no learning curve for the nurses in the field, allowing them to focus on patient care, not on technology.

For more information

To learn more and for a no-cost 30-day trial of MaaS360, please contact your IBM representative or IBM Business Partner, or visit **ibm.com**/maas360

Additionally, IBM Global Financing provides numerous payment options to help you acquire the technology you need to grow your business. We provide full lifecycle management of IT products and services, from acquisition to disposition. For more information, visit: **ibm.com**/financing

[1] "FCC Chairman Julius Genachowski prepared remarks on medical body area networks George Washington University Hospital Washington, D.C.," May 17, 2012. https://apps.fcc.gov/edocs_public/attachmatch/DOC-314145A1.pdf

[2] "Next-Generation Enterprise Mobility: Putting Mobile to Work," *Aberdeen Group*, October 2012. https://www.ndm.net/mobile/pdf/next-Gen-enterprise-mobile.pdf

[3] "Reducing and Preventing Adverse Drug Events To Decrease Hospital Costs," *US Department of Health and Human Services*, March 2001. http://archive.ahrq.gov/research/findings/factsheets/errors-safety/aderia/ade.html

[4] For more information on HIPAA and HITECH, visit: http://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/

[5] "Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information," *US Department of Health and Human Services*. Accessed June 20, 2016. https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
July 2016

WGW03233-USEN-00