WHITE PAPER

The Healthcare Industry: Embracing BYOD for Success

Sponsored by: AT&T

Denise Lund Lynne Dunbrack
August 2015

IDC OPINION

Adapting to the evolving mobile environment is a challenge for any organization. For today's healthcare organizations – whether payers or providers – the challenge is particularly pressing. Clinicians overwhelmingly prefer to use mobile devices at the point of care, and more physicians than ever are using their own personal smartphones and tablets to care for their patients. Indeed, clinicians are using their own devices more than they are using devices provided by their organization.

As a result of the sizable and growing presence of employee-liable mobile devices, healthcare organizations must embrace this bring-your-own-device (BYOD) world. Doing so first and foremost necessitates that management evaluate the end-to-end impact of BYOD on the organization, particularly in terms of security, privacy, compliance of applications, content, data access, and employees' mobile device usage policies. Just as important, healthcare organizations need to select a solution provider partner that has flexible, scalable solutions; a broad ecosystem of partners; and proven professional expertise across a range of mobility aspects, including network, services, security, and devices.

AT&T, among other solution providers, is focused on these types of BYOD solution differentiators, placing the vendor in the consideration set of healthcare organizations.

Mobility in the workplace will not stand still. Planning for the current and future state of mobile network strategies and device, content, and application management solutions is crucial for BYOD to be a success. For healthcare organizations, the regulatory and privacy implications serve to increase the urgency for management to begin the process of embracing BYOD.

IN THIS WHITE PAPER

This white paper discusses the growing list of challenges that face healthcare management in increasingly BYOD environments. The white paper also discusses the diverse solutions available to manage such challenges of BYOD environments, paying particular attention to solutions that can mitigate the financial, security, and operational risks involved. The white paper concludes with IDC's recommendations for decision makers charged with managing BYOD environments.

August 2015, IDC #258498

SITUATION OVERVIEW

BYOD in Organizations Is a Growing Reality

Businesses of all types are finding themselves face to face with employee-owned devices that use a wireless network to access organizational data, content, and applications. In fact, according to IDC's 2014 *U.S. Mobile Enterprise Services Survey,* over one-third (38%) of U.S. enterprises report that they have employees bringing in devices of their own choosing to use for work purposes. On average, 60% of employees who have mobile phones — regardless of whether the employer or employee procured that device — use mobile applications other than email or messaging. As a result, the burden is on management to ensure that mobile access is secure, devices are managed, and policies for employee usage and reimbursement are in place. Enterprises of all types continue to have heightened interest in security and device management solutions.

Businesses face many risks because of the BYOD trend. Many employee-owned devices do not yet have the software and services that allow management to implement and enforce access and usage policies. Further, reimbursement regulations in California have tipped in favor of the employee who must use a mobile phone for work calls. It is now the responsibility of the employer to bear the burden of financial reimbursement in such situations. The blurring of the line for financial responsibility between employee and employer is happening at warp speed, leading many organizations to formally address and implement new reimbursement policies. Just which BYOD mobility solutions are best for organizations varies by the specific challenges an organization faces. Organizations in industries such as healthcare face a growing set of BYOD challenges. Given the intensity of the regulatory complexities and patient privacy implications, nowhere are the security and compliance risks of BYOD more apparent than in healthcare. Over time, the security and compliance issues faced by healthcare organizations are expected to continuously evolve, further adding complexity to the BYOD trend.

As with most mobility trends that organizations face, management hopes that the benefits of BYOD outweigh the challenges. As employees become increasingly mobilized, organizations can expect to achieve improved customer care levels, increased quality, and contextualized patient interactions. In addition, a growing number of clinicians and staff want to use their own mobile device to access healthcare organizations' networks and applications. Often, clinicians and staff prefer using their own personal device over the corporate-liable device. In other cases, physicians who have admitting privileges at multiple hospitals may opt for their own device simply because they don't want to carry multiple devices. As the use of these employee-liable devices gains traction in healthcare organizations, BYOD will create additional mobile security, policy, and regulatory challenges. However, the potential benefits of BYOD can easily outweigh the risks in the healthcare organization if management chooses partners that bring a breadth of on-target BYOD strategies, expertise, and solutions.

BYOD Challenges and Solutions

When it comes to BYOD, healthcare organizations typically face major challenges in four distinct areas:

- The healthcare regulatory environment (i.e., federal and state regulations such as HIPAA and privacy concerns)
- The security of the device and security and access to business and clinical content and applications, including the unique challenges facing clinicians in time-constrained and sterile environments

- Updates, policy changes, and support issues, such as mobile device management (MDM) issues that can arise with clinicians who require mobile devices to access networks in multiple hospitals where they are contracted to practice
- Financial implications of voice and data usage, including the financial implications of porting an organization-provided mobile phone number to a clinician's personal mobile device

Each challenge as well as the appropriate solutions available to help healthcare organizations is described in the sections that follow.

The Healthcare Regulatory Environment

While the healthcare industry is well known for its complexity, management must now contend with the intersection of mobile devices and the intense privacy and regulatory requirements. Access to and disclosure of clinical content are highly regulated under HIPAA. In addition, business data also needs to be secured and is regulated under other legislation (i.e., credit card information falls under the Payment Card Industry [PCI] Security Standards Council). Clinicians and other healthcare professionals who bring their own mobile devices to work put a spotlight on these regulations — regardless of whether or not their organization has a formal BYOD policy. Of particular concern are regulations governing clinical content because of the potential for negative consequences should such content be compromised. Accreditations by the Joint Commission, formerly the Joint Commission on Accreditation of Healthcare Organizations (JCAHO), pertaining to healthcare training and practice facilities are common requirements. Audits by the U.S. Department of Health & Human Services' Office for Civil Rights can require the healthcare organization management team to produce documentation on communication channels, forms, and network usage in its organization.

Solutions

Solution providers run the gamut from those that install security on the device or within the application itself and those that offer network-oriented security to those that offer mobile life-cycle management (MLM) services. IDC defines mobile life-cycle management services as mobile device, connectivity, application, and security solutions that are offered by third parties to manage the efficiency and effectiveness of mobility in the organization. Mobile life-cycle management services include a variety of elements that are hosted either on or off customers' premises. Many of the managed elements leverage enterprise mobility management software, which is licensed by the third-party service provider and/or resold to the customer, as the foundation on which an organization wraps its mobile life-cycle management services. Solution providers such as AT&T, with proven experience in making the solutions come together by leveraging network services and devices, sit at the nexus of these solutions. The solutions, whether deployed at the network level, device level, or user level, help organizations minimize the chance or degree of policy infractions and security risks.

Securing the Device, the Business Content, and Access to Business Applications

With the BYOD trend come serious security implications. Malware from employee-liable devices that access healthcare organizations' networks can compromise proprietary data. In addition, there are risks associated with the loss or theft of the mobile devices themselves. In fact, until the large-scale hacking incidents in 2015 (i.e., Anthem and Premera reported that 80 million and approximately 11 million member records, respectively, were compromised), the most common data breach resulted from lost or stolen devices including laptops and mobile devices. Such losses have put patient data at risk through unauthorized disclosure, with the organizations themselves facing the real possibility of litigation and stiff financial penalties.

In healthcare as well as in other industries, employee-liable devices challenge management to enforce security policies on devices that are not owned and managed by the IT department. These concerns intensified when the HIPAA Omnibus Rule, which resulted in more stringent privacy breach notification, minimum use, and disclosure reporting requirements, went into effect on September 23, 2013 (go to **www.hhs.gov/news/press/2013pres/01/20130117b.html**). Under the rule, the risks and liabilities associated with privacy breaches increase and annual penalties for violations can total up to $1.5 million per provision, up from $25,000. Security policies must consider the complex healthcare environment with its highly mobile and transitory workforce. At the end of the day, the BYOD trend raises the need for healthcare management to pursue an evaluation process — from the organization's network to its underlying infrastructure — for protecting applications, content, and data on mobile devices. To this end, organizations must establish policies and procedures for mobile security to ensure compliance among all employees and their devices.

Solutions

According to IDC's 2014 *U.S. Mobile Enterprise Services Survey,* decision makers in organizations are increasingly prioritizing secure mobile access to corporate resources and content among employees. Connectivity and policy management solutions help ensure organizations that employees are able to access approved business content and applications while minimizing risks to the business. These solutions include a heavy emphasis on security processes and are aimed not at the device itself but at the applications employees use via the mobile device. Services include, but are not limited to, distribution of applications, integration via APIs, email and personal information management (PIM), and content sharing management and policy enforcement. Management of applications, when not at the holistic device level, is either via a containerized approach or at the application level. Certainly, implementing enterprise application stores can mitigate any kind of security risk; IDC research on healthcare organizations reveals that a third or more of the organizations have begun planning to implement an application store. In these situations, management can operate with added comfort, knowing that employee-liable devices can be prohibited from downloading applications from public application stores outside the firewall.

Even with solution providers such as AT&T available to help organizations implement private business application stores, employees may still find ways of using their own device to access applications via other channels outside of the organization's firewall. Mobile device management software and mobile application management software are essential pieces of a holistic BYOD environment for healthcare and other organizations. These services are provided by solution providers such as AT&T and enable organizations to more fully control devices and corporate information, whether those devices are employer owned or BYOD.

AT&T Advanced Solutions offers a managed service to help enterprise clients address challenges and opportunities to drive business transformation through mobility. AT&T offers end-to-end solution services in mobility consulting, BYOD, enterprise mobility management, device life-cycle services, mobility managed services, and network and technology transformation. Solutions such as these have been thoughtfully cultivated to accommodate organizations looking for solutions that can grow with them as their needs evolve. AT&T allows management to pick and choose the most appropriate capabilities that best meet the organization's specific needs. AT&T has a list of trusted providers, including AirWatch by VMware, MobileIron, and OpenPeak, that bring unique strengths as part of AT&T's enterprise mobility management focus. AT&T's ecosystem brings together a range of solutions, from those that focus on traditional mobile device management and security to others that focus on containerization and PIM. AT&T has gone so far as to preintegrate with security threat assessment vendors such as FireEye and Blue Coat Systems.

End-user, or enterprise employee, 24 x 7 support services are often part of mobile life-cycle management services and are very much a part of AT&T's offering. This type of solution provides healthcare organizations with efficiencies when addressing the many support-related questions that need to be fielded over the life of the device. By having 24 x 7 end-user support, organizations can focus on core competencies without hiring internal staff with the bandwidth and expertise required to provide end-user device support. Online support is basic, and phone support may be available.

Maintaining Updates and Policy Changes

Across a wide range of industries, mobile device usage in the workplace has evolved from a two-way communications tool into a tool that heavily utilizes organizational knowledge bases, applications, and other content that sits behind a firewall. Healthcare organizations are continuously required to update technologies and processes around electronic information and access points. The stakes are significant when it comes to patient privacy; therefore, management should evaluate the organization's environment and BYOD use cases for risks. Doing so may require the help of a knowledgeable partner that has in-depth expertise in the types of risks that may crop up. Knowledgeable partners can help the healthcare organization conduct a mobility risk assessment, including defining mobile worker profiles to understand who needs access to what data, where, how, and on which devices to identify potential security risks.

The mindset within IT can be that "We're going to save money with a BYOD strategy," but that isn't always the case if the strategy is not implemented properly. Indeed, organizations should determine up front how they will provide support to employees who use their own devices for work. IDC research reveals that, at best, the majority of healthcare organizations provide limited IT help desk support for business applications or FAQ-oriented, self-help options for these employees. The impact of downtime among employees stands to wreak havoc on an organization's priorities — customer care, efficient and effective access to knowledge bases, records management, and productivity and quality of care all can be adversely affected. Support for employee-liable devices is a requirement for healthcare organizations that want to embrace BYOD successfully, yet the quantity and availability of knowledgeable IT support resources can be a challenge in some organizations.

Solutions

Professional and consulting services are essential in the BYOD solution design, implementation, and life-cycle management phases. Vendors with these capabilities partner with the healthcare organization's management and IT team to help that organization operate as a center of excellence. Even more importantly, these vendors can help an organization create and execute an overall strategy to address BYOD risks while maximizing opportunities. Enterprise Mobility Management Services (EMMS) from AT&T, for example, provides services that are aimed at fulfilling this highly strategic partner role. The vision that the healthcare organization's management and IT team has is shaped by AT&T at the outset of the organization's relationship with AT&T around BYOD solutions. Essentially, AT&T offers a mobility systems integration function within its EMMS team, offering three tiers of tech support focused on the management and IT team's support needs (i.e., enterprise mobility management configuration support) rather than end-user support. (That support is provided by a different team within AT&T.) AT&T then provides the follow-up phases of installation, configuration, training, and even full remote administration of the EMM platform. AT&T has multiple years of experience in risk mitigation strategy design services and systems integration functions as well as related implementation and support.

Healthcare organizations will need to scale their rollout of the BYOD strategy over time. Consultation and workshops between the BYOD services provider and the healthcare organization's management and IT team are crucial. The openness of the strategic services vendor to this type of relationship is a

key decision criterion that organizations should have in mind. Professional and consulting services teams that are worth their weight in gold are those that will help the organization discover the hidden costs in one BYOD solution approach versus another as well as recommend a phased approach to embracing BYOD in the organization.

Addressing the Financial Implications of Voice and Data Usage

Employees in the healthcare environment, particularly clinicians, often prefer to use their own mobile devices rather than devices provided by the organization. Employees are tied to their organization-provided mobile phone number in many cases because it is on business cards, in clients' hands, and otherwise made available as emergency contact info. Clinicians and the organizations they are tied to face the dilemma of how to retain these clinician numbers while accommodating the use of clinicians' personal mobile phones. Often the healthcare organization is faced with incurring financial costs to port the number to the personal device or to not permit it at all. Nonetheless, the expectation may exist that the healthcare organization, at a minimum, will compensate for the increased mobile plan usage on the employee's BYO device. A court ruling by the California State Court of Appeals *(Cochran v. Schwan's Home Service)* on BYOD mobile plan usage reimbursements firmly sided with the employee. The ruling essentially states that employers in California must reimburse the voice usage in situations where employees are required to use their own device for work purposes. It is up to employers to deal with the complex task of determining the appropriate amount of BYOD usage in an efficient and effective manner.

IDC research reveals that across all healthcare organizations in the United States, nearly one-third of providers (31.1%) and 25% of payers pay the monthly voice and data plan directly to the mobile operator for employees with employee-liable devices. For the remainder of organizations, the changing tide may require increased compensation for employee-liable mobile device usage. This will add incremental burden on the organization as it has to process a stipend payout per employee, manage receipts and subsequent reimbursements per employee on a monthly basis, and even manage the process by which employees verify work-related usage. There are numerous inefficiencies in these sorts of manual processes, which may end up costing the organization time and money that could be spent elsewhere.

Solutions

A provider such as AT&T has the ability to drive cost efficiencies and security mitigations across the network as well as at the device level. AT&T has also come to market with a highly targeted solution — AT&T Work — designed to address the challenges that organizations face with the separation of personal and business content and number portability when it comes to employee-liable, or BYO, devices. The solution allows management to preset voice and data spend limits on employee-liable phones, making it ideal for any organization required to compensate or interested in compensating BYOD employees for device usage. Ultimately, AT&T Work data can be applied at the application level, helping management mitigate the financial risks posed by employees who use their devices while at work to access nonbusiness content. AT&T Work can be integrated with trusted EMM solution providers, affording healthcare organization management a choice of solution providers that will best meet the organization's needs while ensuring that these AT&T Work capabilities function. Further, AT&T Work allows employee-owned devices to have a separate, organization-owned mobile phone number and voicemail in addition to a personal phone number. This capability helps reduce compliance challenges while streamlining the reimbursement process. This functionality works regardless of what mobile operator network the employee-owned device is on, helping make the AT&T Work solution that much more compelling to organizations.

FUTURE OUTLOOK

Mobilizing employees no longer means simply providing smartphones to executives and field service workers and enabling basic voice and data communications. Mobility in the enterprise is far beyond this stage, now involving provisioning and securing multiple device types (i.e., smartphones and tablets) for employees across a wide range of job functions. Increasingly, mobilization also means managing and monitoring devices brought by employees as part of the mix, which in turn involves monitoring and securing access to business applications and content. Complexity and cost implications have increased dramatically for enterprise IT departments in terms of managing the mobility life cycle. Optimizing the usage and cost of the services and enabling access have become massive tasks because of the proliferation of mobile devices in the enterprise. A recent IDC survey confirmed that 53% of U.S. enterprise employees are using smartphones in the workplace, up from 38% in 2013 (see *The Enterprise Is Fully Onboard with Mobility, Now Looks to Security and Services: Key Findings from the 2014 U.S. Mobile Enterprise Services Survey,* IDC #250570, August 2014).

Acceptance of BYOD is commonplace in businesses globally today. However, IT administrators are struggling to balance the potential productivity and employee satisfaction benefits of BYOD with the security risks to networks and content. Ultimately, policy monitoring and management and security are as important to a successful BYOD strategy as is access to corporate applications and content. Many healthcare organizations have a mix of devices brought by employees and devices provided by the enterprise. Service providers such as AT&T recognize the need to balance access to applications and the risks that come with BYOD devices and have designed the modules of their mobile life-cycle management services with this in mind. The vast majority of service providers offer connectivity and policy management services that are able to handle devices brought in by employees in addition to corporate-provided devices. Container management and dual-persona software and services are targeted to BYOD environments.

CONCLUSION

The move toward BYOD environments is expected to grow and evolve over the next five years. Decision makers who are faced with BYOD at healthcare organizations have numerous considerations, including how to provide network access, how to secure healthcare and patient data accessed by BYO devices, how to facilitate device updates, and whether and how to facilitate reimbursements to clinicians and healthcare staff who are using their own devices for work. The following management considerations are essential to embracing BYOD successfully:

- **Create a plan to prioritize and leverage a range of BYOD solutions.** Such solutions should both protect and optimize an healthcare organization and its resources today and grow with the organization's future needs.
- **Discuss, evaluate, and assess options with a chosen strategic solution partner, such as AT&T.** Such discussions can and should be business oriented rather than technically focused, thereby helping management take a leadership role in driving the organization successfully forward within a BYOD environment. Having confidence in the solution provider's ability to demonstrate deep technical support functionality behind the scenes is even more essential.

- **Engage solution providers in discussions and plans around goals for BYOD.** Consider the scope of BYOD functionality such as scheduling, time management, and health records. Take into account the impact that mobilization will have on how the organization currently operates. Look for service providers that have the ability to apply healthcare industry solutions when and where most appropriate.
- **Choose solution providers that offer a broad set of capabilities through an ecosystem of partners.** Solution providers such as AT&T, as well as some systems integrators, focus on providing a diverse set of products and consultative services that can help yield financial, security, and operational efficiency. AT&T has focused intently on ensuring that its clients don't rely on a single provider: Clients can select from a broad set of solution and partner vendor expertise as part of AT&T's diverse mobility service offerings.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-insights-community.com
www.idc.com