Business White Paper

Securing Health Data in a BYOD World

Five strategies to minimize risk

ClearDATA
SECURE • HEALTHCARE • CLOUD

Securing Health Data in a BYOD World

Table of Contents

Introduction

Just as mobile computing has become an indispensible part of your life, so to has it become a standard tool for healthcare providers – equally important as the stethoscope and blood pressure cuff. Smartphones and other types of consumer mobile devices are an increasingly prevalent part of that trend. In fact, nearly 89 percent of healthcare workers use smartphones for work purposes, according to Cisco's *BYOD Insights 2013: A Cisco Partner Network Study*.

But with mobility has come increased security risks, particularly as healthcare workers attempt to access or transmit healthcare data using personal mobile devices. Advancements in consumer technology and the personal preferences of employees are driving more companies (including healthcare organizations) to adopt "bring your own device" (BYOD) strategies to either replace or enhance corporate-issued mobility programs.

In BYOD scenarios, employees use personal smartphones, tablets and laptops to access corporate networks, e-mail, and enterprise applications. In healthcare environments, BYOD programs present many significant risks to the security of protected health information (PHI) and other data that can lead to costly fines and strict penalties.

According to a Decisive Analytics survey published in 2012, 77 percent of respondents allow employees to use their personal smartphones or other mobile devices for work, and they rely on acceptable-use policies to regulate these devices. Unsurprisingly, nearly half of respondents reported a related security incident.

Even companies that expressly prohibit use of personal devices for work purposes have found that BYOD is a reality whether they like it or not. A Fortinet survey on BYOD from 2012 found that 36 percent of respondents would find ways to work around IT policies that forbid the use of their personal devices.

Healthcare organizations must prepare to address the risks and

implications of BYOD programs. Whether a formal program is in place or not, employees will likely access patient data on their personal devices. It is imperative that organizations implement sound policies and procedures to secure personal devices before any data is compromised.

BYOD is pervasive and potentially beneficial, but unmanaged BYOD can be disastrous in a healthcare setting. Here, we'll outline some of the drivers of BYOD adoption, associated risks and challenges, and strategies that healthcare organizations can employ to ensure security in a BYOD environment.

BYOD Adoption Drivers

There are a number of reasons BYOD is taking off in healthcare. Provisioning new corporate-owned devices is simply too expensive for many healthcare organizations. Leveraging hardware that employees already carry can reduce upfront costs and ease training and employee acceptance of new applications.

Many physicians, nurses and other staffers already carry multiple devices – some of them personal, others issued by hospitals and other facilities. Allowing them to condense some of these functions onto their own mobile phone gives them a way to interact with data and applications more intuitively, and can reduce the need to carry additional IP phones, pagers and other devices.

Users also want to be untethered from a single facility and be able to access health data from home, a personal office, other hospitals and while traveling. Many younger employees are used to working on mobile devices, and organizations that don't have this capability may be less attractive to new hires.

The type of real-time access and decision-making enabled by smartphones and tablets can improve efficiency as well as patient care. BYOD can also help companies save money by reducing cellular phone and landline costs. However, there should be a thorough return on investment analysis before making the move to BYOD, or communication costs could actually go up if the program isn't properly designed.

BYOD Security Risks

With corporate-issued mobile devices, IT has full control over the applications on the device and security measures used. Personal devices, however, present a host of potential security risks that have to be addressed prior to adopting a BYOD policy.

Using the device's Web browser, for example, can leave the mobile device open to virus or malware infection. E-mail applications, which provide direct access to corporate networks, are beset by spam and phishing attacks. Calendars and contact lists can be exposed if devices are lost, stolen or otherwise accessed by unauthorized users.

End users may also use their personal devices to store or e-mail PHI in an unsecured manner. That not only puts patient data at risk but also may lead to serious HIPAA violations resulting in fines and penalties, not to mention, damage to the relationship between an organization and its community.

IT departments will also have concerns about software license management and application management. Application updates need to be delivered quickly and efficiently to multiple devices at once, and that requires corporate access to employees' personal devices in a BYOD environment. IT may have objections to supporting heterogeneous devices with different operating systems, and staff may resist giving the company access to their devices.

Healthcare companies have good reason to be worried about how employees might be using their personal devices once they have access to the corporate network. According to the previously mentioned Cisco survey, 39 percent of employees don't password protect their mobile devices, and 52 percent access corporate information via unsecured Wi-Fi networks. A Juniper Mobile Security Report found 29 percent of organizations do nothing to manage applications on BYOD endpoints. Another study by Osterman Research found that only 24 percent of personal smartphones and 21 percent of tablets can be remotely wiped by the corporate IT department.

Even more troubling is this statistic from the 2012 SANS Mobile Security Survey: Only 9 percent of organizations are fully aware of the devices accessing their network.

Five Strategies for Securing Healthcare Data in a BYOD Environment

Even for companies that have policies in place forbidding the use of personal devices for work purposes, BYOD is already a reality. In order to effectively secure data while also leveraging the potential advantages of BYOD, companies should use the following strategies to prepare and implement a their program.

1. Risk assessment

Evaluate all policies, procedures and data flows prior to adopting a BYOD strategy to identify where and when data might be at risk. Any data that passes through or resides on a personal mobile device should be password protected and encrypted at all points, and safeguards should be put in place to prevent users from emailing or sharing PHI through unencrypted channels or on file sharing services like DropBox.

If you know how PHI flows through your environment, you can safeguard the data. Conduct a data inventory and threat analysis, and map the logical data flow of existing policies and standard operating procedures. Additionally, find out how much BYOD activity is already occurring in your organization. By identifying out how users have incorporated personal devices into their work lives, you can better identify potential vulnerabilities and benefits.

Finally, develop metrics so you can determine whether or not the BYOD program meets security expectations once users are on the network and to measure any expected cost reduction or efficiency improvements.

2. Implement BYOD policies before adopting the technology

Clear policies must be in place before rollout so all end users are fully aware of device requirements, their responsibilities and the consequences for violating the policy.

Define the scope of the project, user responsibilities, security and software requirements, IT support capabilities, and define key terms referenced in the policy so that all stakeholders understand the language of the documents.

The policy should outline requirements for mobile device management (MDM) or other software, how physical security of the devices will be addressed, password requirements, employee reporting responsibilities when a device is lost or stolen, and acceptable use of the device when not being used for work purposes.

Generally, employees should not be able to use jail-broken or hacked devices, or share PHI using cloud-based or other file sharing services. The policy should address support during and after work hours, help desk capabilities and self-service options.

Standardize devices and applications as much as possible. It will be difficult to support every platform and operating system iteration without making the program cost prohibitive. Develop an FAQ document for user reference and self-service.

Stipend/reimbursement models are another area where companies struggle to meet employee expectations when it comes to BYOD, and can create an implementation stumbling block. If employees are expected to work on their personal devices, they will expect some compensation. Some companies have addressed this with a flat stipend, or a tiered plan based on job responsibilities. Whatever approach you take, these details should be determined and agreed upon by stakeholders ahead of time.

Privacy policies should also be part of the BYOD plan. Employees may push back when it comes to installing MDM software on their personal phones because they don't want the company to have access to their personal photos or GPS data. The policy should

clearly state what information the company can and cannot access on personal devices. Without these guidelines, you run the risk of undermining employee acceptance of the BYOD program.

Finally, get human resources involved to develop a plan for addressing policy violations. There should be consequences in place for not adhering to the rules, with a clear reporting and documentation requirement.

3. Focus on PHI, not the devices

There are limits to how secure you can make any given device, particularly personal devices. Instead, PHI and other sensitive data should be the focus. Develop strategies and deploy technologies that ensure the data is encrypted and secure, regardless of how it is accessed.

Many legacy architectures can't support the effective protection of information in a mobile environment. Before you open your networks to employee devices, make sure your existing applications and networks can handle the increased traffic and provide the type of access users will expect.

Mapping the flow of data early in the process is critical. Find out who uses the data and when, and ensure you can fully secure it at every point so that end users can access the information they need without unnecessary impediments.

4. Secure data end to end

MDM is critical in implementing BYOD. MDM solutions allow you to "sandbox" corporate data so it remains separate from personal contacts and e-mails, remotely wipe data from devices, push password requirements to devices, manage and update applications on the phones/tablets, place controls on how data and applications are used, and gain visibility into the status of the entire fleet of mobile devices, both personal and corporate-issued.

To ensure PHI remains secure and that organizations remain in compliance with HIPAA, data should be encrypted while in motion over the network and while at rest in a data center or on a device.

Multifactor authentication methods can further secure data more reliably than simple username/password systems. Some solutions also provide the ability to set up role-based information delivery, so that only certain patient data is accessible to certain employees.

There are also virtualization and other cloud-based tools that can provide even more security. A virtual desktop infrastructure, for example, provides access to PHI using remote servers and can eliminate many traditional end device security concerns. Users access the data as a thin client or "dumb" terminal – the data is never present on the mobile device in the first place, and users can only access the system with the proper credentials. There are also Web-based messaging solutions that simply provide access to a portal in order to keep PHI off of mobile devices.

5. Ensure security measures don't impede usability

Some inconvenience is unavoidable; users will have to utilize passwords or multifactor authentication procedures. However, the overall approach should keep ease-of-use in mind so employees can enjoy the efficiency improvements of mobility.

Ensuring employee privacy is also important. Many MDM tools provide ways to separate personal and business data so that only corporate information is cleared when IT performs a remote wipe on a lost or stolen device, for example.

It's also important to have the right support resources in place in advance of the rollout. You are conceivably adding hundreds or thousands of devices and users to the network. IT needs to be sufficiently staffed at the help desk and have enough technicians available to address end user problems and questions during the initial implementation and afterward. The network infrastructure also needs to be able to handle all of the new devices and data traffic.

Other ease-of-use features that can improve BYOD deployments include certificate support for single sign on, automated document management tools, always-on virtual private network technology, and content-filtering APIs to prevent access to inappropriate content during work hours.

About Us

ClearDATA is the nation's fastest growing healthcare cloud computing company. More than 310,000 healthcare professionals rely on ClearDATA's HIPAA compliant cloud computing HealthDATA platform and infrastructure to store, manage, protect and share their patient data and critical applications.

For more information

1600 W. Broadway Road, Tempe AZ
(800) 804-6052
www.cleardata.com

ClearDATA
SECURE • HEALTHCARE • CLOUD