BYOD Policies and Procedures: Keeping Pace with Technology and Keeping Patient Information Safe

Andrea Musker
IPC The Hospitalist Company Inc.
North Hollywood, CA

According to one study, 44% of employees in developed markets use their personal mobile devices for work purposes. The health care industry has not been immune to the “bring your own device” (BYOD) trend. The U.S. Department of Health & Human Services (HHS) and the Office of the National Coordinator for Health Information Technology (ONC) have devoted increased time and resources to mobile devices—the smart phones, tablets, and laptops attached to nearly everyone’s hip—and specifically the need for health care providers to safeguard their mobile devices from potential privacy and security breaches in violation of the Health Insurance Portability and Accountability Act (HIPAA).2

The increased attention on mobile devices from regulators has resulted in welcomed guidance from regulators to health care providers, be it the family physician practicing in small-town America using his tablet to share real-time X-rays with specialists miles away, or the national health care company performing security risk assessments.4 However, federal interest in mobile devices also is a likely predictor that these devices will be the subject of increased scrutiny and enforcement actions.

Mobile device technology has ushered in an era in health care where widespread and rapidly changing consumer technology is being adopted for more-technical medical uses.4 The result is the collision of: (1) workforce demand for access to work information, including protected health information (PHI), anytime and anywhere on the mobile devices of their choice; and (2) organizational demand that users meet HIPAA requirements and keep PHI private and secure.

This article synthesizes some of the benefits and risks of BYOD programs in health care, as well as guidance from federal agencies and the health care technology industry.

Benefits and Potential Hazards of BYOD Programs

The health care industry is not immune from the “viral” BYOD movement, as physicians and other providers capitalize on the benefits of instant access to information and data. Even the White House has weighed in on the benefits of BYOD programs, encouraging federal agencies to adopt BYOD programs to “address the personal preferences of . . . employees, offering them increased mobility and better integration of their personal and work lives,” and to give employees “the flexibility to work in a way that optimizes their productivity.”6 In addition to choice and flexibility, BYOD programs often reduce employer costs. Most BYOD programs do not reimburse the employee for the cost of the device, but may reimburse the employee for service charges.7

Most importantly, in the opinion of many health care providers,8 mobile devices improve the quality of health care. At the 2012 Mobile Devices Roundtable held by ONC, one family practice physician called technology “a great equalizer,”9 as health care providers are able to access health care information and patient data instantly, communicate with specialists worldwide, and monitor patients via devices used in patients’ homes.10 Allowing health care providers to use mobile devices to access, transmit, and store PHI gives them the ability to extend and expand care. Offering health care providers the option to use their personal device gives them instant access on a platform they are comfortable using.

However, advances in technology bring certain risks in the health care industry. HIPAA Privacy and Security Rules require health care entities to protect the privacy and security of patient information,11 regardless of where the PHI is located or on whose mobile device the PHI is stored. The challenge is that “[t]echnologies are being deployed in healthcare organizations without the benefit of having updated policies and procedures for managing them,”12 and without health care entities thinking through the vulnerabilities of mobile devices and the appropriate security measures necessary to protect PHI.

Mobility, the obvious advantage of mobile devices, also may be its greatest risk when the device contains PHI. When a cell phone falls out of a pocket, a tablet is left in an airplane seat back pocket, or a text message is read over a person’s shoulder, a HIPAA breach may occur if the device or the information on it is unprotected.

PHI stored on a mobile device is vulnerable at many levels, including the network, application, database, and device level.13 Viruses and malware are easily and unwittingly downloaded and could compromise emails and other messages transmitted by a device or the information stored on the device.14 Potential HHS enforcement actions for lost or stolen unsecured devices add penalties that can easily reach tens of thousands of dollars.15 The result is a minefield of potential issues for health care providers using their mobile devices.

How to Protect and Secure Mobile Devices

Employers or health care entities may have limited visibility into the security protocols on a user’s device, so thorough organizational policies and procedures are integral to protect PHI. Below are some recommendations from federal agencies and officers, health care providers, and the information technology (IT) industry that may assist health care entities in adopting secure BYOD programs:
**Lock the “Front Door”**

Every mobile device can be locked by a password, passcode, or personal identification number, creating a barrier of first defense against unauthorized access. Strong passwords must be a requirement before any device can access PHI or log into a network that houses PHI, or before the user can register the device for access to corporate email accounts. “1234” or “0000” should not be acceptable passwords. All devices should be set to log off automatically after a short period of time to prevent unauthorized access. If possible, to simplify procedures for busy health care professionals, users could be allowed to use the same credentials, e.g., usernames and passwords, to access their device, email, corporate networks, and corporate applications.

**Consider Limiting Devices to Access Only**

Some health care providers actively avoid storing PHI on devices and use their devices only to access PHI to limit the potential liability resulting from a lost or stolen device. Also, health care entities should consider users’ ability to share files from the device. Proprietary applications created by health care entities can be limited to data entry or access only, restricting the ability of the user to download and save data from the application to the device.

**Encrypt Data**

PHI that is stored or sent should be encrypted. Encryption converts data into a form that cannot be read without a decryption key or password. Encrypting data stored on a mobile device (data at rest) prevents unauthorized access to the data, and encrypting data sent by the mobile device (data in motion) prevents unauthorized access while the data is being transmitted. Email exchanges containing PHI always should be encrypted. HHS endorses the National Institute of Standards and Technology’s (NIST’s) guidance on encryption to help providers meet HHS’ Office for Civil Rights’ standards for rendering PHI unusable, unreadable, or indecipherable to unauthorized individuals.

**Consider Secure Options for Common Mobile Functions**

Nearly every cell phone can send a text message, but text messages generally are not encrypted and therefore are not a secure means of transmitting patient information. Moreover, there is generally no way for the sender to confirm the message has been received by the intended recipient, and messages are stored, unencrypted, by cellular or wireless carriers. Health care entities should consider using a secure texting service that encrypts texts and deletes sensitive patient data from the device after a short period of time. Health care providers should be mindful of if, where, and how long text messages are stored by the vendor or on company servers and should have a strong business associate agreement in place with any vendor who touches PHI.

**Manage Mobile Devices Effectively**

Mobile device management (MDM) is a rapidly growing industry. MDM companies assist users in linking their devices to corporate data and help health care entities customize the management of mobile devices. MDM vendors provide security solutions for devices, applications, and content. MDM solutions allow health care entities to permit users to bring their personal devices to work, while outsourcing technical security and management obligations to the MDM provider. Components of mobile device management include remote wiping, remote disabling, and proprietary application stores.

- Remote wiping is a security feature that remotely and permanently deletes data on a lost or stolen mobile device or a terminated employee’s device. It can be designed to delete only corporate or patient information from the device, leaving personal information untouched. An alternative feature is remote disabling, which locks a lost or stolen device (if the device was not password protected), but permits the device to be unlocked if it is recovered. Remote security capabilities may be built into the device and only need to be enabled by the user, or the health care entity may require the user to download applications that will remotely and/or selectively wipe or disable the device.

- A proprietary application store allows the health care entity to deploy applications (apps) for data entry, patient management, electronic medical records, diagnosis, and any other function that might require access to or use of sensitive patient information. By offering these apps through the proprietary app store, the health care entity has the right to revoke all access to the proprietary apps and the PHI within the apps as soon as a device is lost, stolen, or an employee is terminated.

**Get It in Writing**

To the manufacturer of mobile devices, the personal user is the owner of all data on the device. However, to health care entities whose patients’ PHI sits on users’ mobile devices, the data belongs to the entity, not the individual user. Users may understandably have qualms about institutional access to their personal devices or an employer’s ability to delete data from the devices. To ensure quick, undisputed access to a user’s personal device, health care entities should have each user who will have access to PHI sign an agreement that explains the health care entity’s rights in relation to proprietary information on the user’s mobile device. Health care entities can require users to agree that the entity has the right to: revoke proprietary apps and information from the device, wipe organizational data off the device, access the device to review protected data stored on the device, and/or audit the device to ensure proper security measures are in place. The Healthcare Information and Management Systems Society (HIMSS) offers a sample Mobile Device User Agreement as part of its Mobile Security Toolkit, and MDM vendors provide customizable terms-of-use agreements. Health care entities can require...
click-through agreements or terms and conditions acknowledgments before the user is permitted to access PHI on corporate apps, networks, or email.

A user agreement also can be a tool to communicate the health care entity’s usage policy, including appropriate access at the worksite, data management and storage policies, reimbursement, and technical support availability.  

Educate

Health care entities should train all providers and employees who use mobile devices on how to access, store, or transmit PHI. Training should emphasize general HIPAA requirements and privacy and security awareness, including risks, threats, and vulnerabilities when using mobile devices for work, how to properly implement the security features, and how to avoid potentially costly mistakes when using personal devices.  

Training should be updated whenever the law, technologies, or policies change and must be supported by strong corporate IT and device management processes.

Health care entities and providers can take advantage of the mobile device privacy and security toolkits, videos, tips, and checklists published by HHS, HIMSS, and NIST, or provided by their MDM vendor. These resources will guide health care entities and providers in drafting policies, implementing strong procedures, and educating their workforce.

Conclusion

As mobile technology rapidly advances, it creates an inevitable game of catch up for health care entities and providers to set policies and procedures to protect the privacy and security of sensitive patient information. Health care IT experts remind providers that “[t]he compliance regime that we’re dealing with is primarily risk-based. So, whether it’s HIPAA or whether it’s meaningful use requirement or measures, we’re talking about doing ongoing security risk management.”

As technologies and devices continue to develop, health care providers should focus on implementing the strongest safeguards currently available to secure information accessed by or stored on mobile devices, while developing overarching policies that will continue to apply to new and emerging technologies and to protect patient sensitive data. Only consistent internal processes and enforcement will safeguard PHI and yield a BYOD program that protects patients and providers from the consequences of unauthorized access.

---

3 References in the article to “health care entities” or “health care providers” are meant to include any entity, organization, or individual accessing protected health information, including physicians, clinics, facilities, pharmacies, health insurance companies, billing companies, or any other HIPAA covered entity or business associate.
5 Transcript of Farzad Mostashari, MD, ScM, at ONC Roundtable, supra note 2, at 10-11, l.15-21, l.2-8.
7 Transcript of Steve Heilman, M.D. at ONC Roundtable, supra note 2 at 72, l.1-18.
8 Joseph Conn, Staying connected: Providers and patients increasingly relying on home-based monitoring, MODERN HEALTHCARE, Jan. 18, 2014, available at www.modernhealthcare.com/article/20140118/MAGAZINE/301189929/staying-connected-AllowView=VXQ0UpwZTVdL1dXl1I3TkErT11RajNj4UL4VUmZeFZQk1DRFEx9Q.
9 Transcript of Chris Tashjian, MD at ONC Roundtable, supra note 2 at 56, l.21.
10 Id.
12 Transcript of Lisa Gallagher, Senior Director of Privacy and Security at Healthcare Information and Management Systems Society, at ONC Roundtable, supra note 2, at 50, l.7-10.
14 White House BYOD, supra note 6.
16 Transcript of Chris Tashjian, MD at ONC Roundtable, supra note 2 at 73, l.1-14.
20 HealthIT.gov, Can you use texting to communicate health information, even if it is to another provider or professional? Available at www.healthit.gov/providers-professionals/faq-can-you-use-texting-communicate-health-information-even-if-it-another-p (last accessed Jan. 23, 2014).
23 HealthIT.gov, Tips to Protect and Secure Health Information: Install and activate remote wipe and/or remote disabling, available at www.health-

24 Id.
33 Transcript of Lisa Gallagher at ONC Roundtable, supra note 2 at 81-82, l.16-21; l.1-15 (emphasis added).