spōk

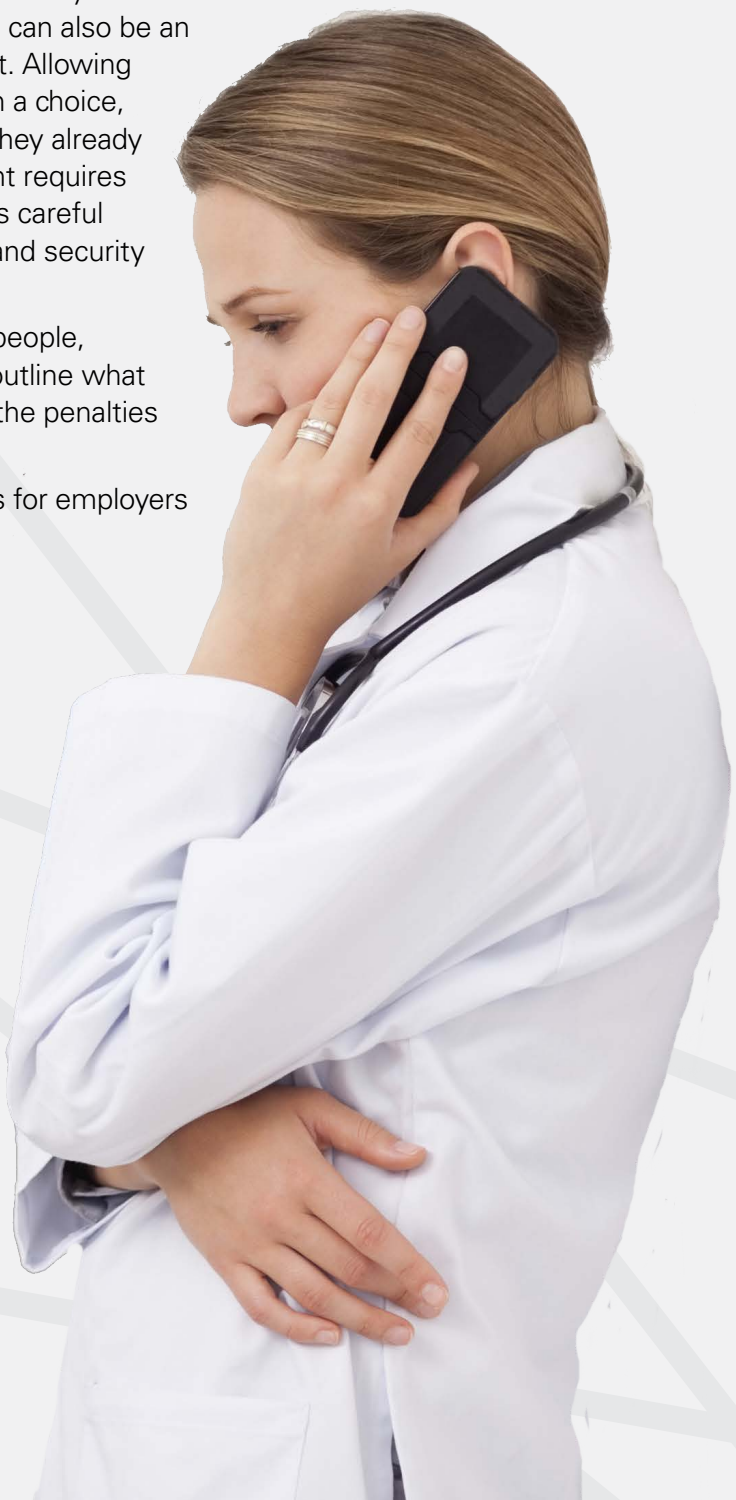
THE 2015 HOSPITAL GUIDE TO BRING YOUR OWN DEVICE POLICIES

Research finds that BYOD policies can save money—but creating a successful BYOD environment takes time, careful planning, and thorough execution to maintain the integrity and security of the patient information being accessed and shared on mobile devices. This guide walks you through the critical points to consider as you design an effective BYOD policy for your hospital.

BYOD – WHAT AND WHY

BYOD, or bring your own device, is a topic of communication and connectivity that touches companies in all markets, from finance to manufacturing to healthcare. The adoption of mobile devices in the workplace has increased rapidly because they can support so many functions. From the early days of simple phone calls and text messages, mobile device capabilities have expanded to include so much more. For clinicians, these functions include drug reference apps, electronic medical record (EMR) access, critical test result notifications, code alerts, and secure communications with colleagues. The question for hospitals and health systems is whether to supply these devices or allow clinicians to use their own.

Gartner researchers have demonstrated that BYOD policies actually do save money, and they estimate that institutions can support nearly three times as many BYOD devices as company-owned ones.[1] Employee satisfaction can also be an important driver for creating a BYOD environment. Allowing employees to bring their own devices gives them a choice, will help with user adoption, and usually means they already know how to use them.[2] But a BYOD environment requires more than just making an announcement; it takes careful planning and execution to maintain the integrity and security of information being shared.



A successful BYOD policy needs to address the people, processes, and the technology. It should clearly outline what behaviors are expected and accepted, and what the penalties are for non-compliance. [3]

When designing a BYOD policy, the big questions for employers and employees generally include:

- Expense allocations (Who pays for what?)
- IT support (If they use it, will you support it?)
- Access (What is effective and acceptable use?)
- Security (Is it safe?)

This guide walks through the topics to consider when developing a BYOD policy within the healthcare space. Though the questions above apply across industries, there are regulatory requirements that make security an especially important consideration for hospitals.
In particular, there are unique needs for physicians who practice at multiple locations.

MAKING THE LEAP (AND THE RULES)

Once a physician group, clinic, hospital, etc. has decided to make the leap into the growing BYOD pool (or realized a documented strategy is needed), drafting a formalized policy will take time, careful planning, and coordination with multiple departments. Creating a clearly defined set of governing rules is a smart investment of time at the outset to prevent misuse of personal devices that could jeopardize the security of patient information and make the institution vulnerable to security breaches and fines.

During the planning phase, input is required from BYOD participants to understand how devices are used, what systems they need to access, and the potential risks.[4] It is important to work with HR to outline and enforce punitive measures in the event an employee misuses the device and/or patient information.[5] Administration coordinates approvals and often the budget. And the IT team is responsible for assessing the risks, determining what tasks should be performed on a mobile device, ensuring the technical implementation, and deciding what support they are and are not expected to provide. Once the design team has been established, a good place to start is the question of who will pay for what.

WHO PAYS FOR WHAT?

One of the hardest parts of developing a BYOD policy is establishing the expectations of employees and employers around who foots the bill.[5] Users are generally expected to purchase personal devices such as smartphones and tablets. In fact, this is the primary cost savings for facilities that choose BYOD over the employer-supplied device model.[6] However, there may be exceptions that warrant consideration, such as offering to cover part of an upgrade cost if it is required for compatibility with certain hospital-approved or purchased apps.

Then the primary questions are around the data and cellular plans. If the personal device being used is essential to the employee's job, hospitals might consider covering part of the monthly expense by paying a flat stipend to employees, paying a percentage of the bill, or reimbursing monthly expenses based on actual usage.[7] The decisions about how a facility structures the reimbursements can be influenced by the Wi-Fi availability throughout the facility (if personal devices are permitted to access it), and how much data the apps necessary for job functions actually use. Health systems may also want to segment the employee population and cover expenses for some staff, but not for others. An example of not paying for device plan costs might be for employees who use their personal devices to access email, but they are not required to do so as part of their job.

IF THEY USE IT, WILL YOU SUPPORT IT?

IT support means two things in this BYOD scenario—which devices will IT provide apps and enterprise access for, and what is the level of help available for end users to register their device, install apps, troubleshoot problems, etc. Ninety percent of organizations will support some form of BYOD by 2017, and researchers predict that by 2018 there will be twice as many employee-owned devices in the workplace as enterprise-owned devices.[8] In a recent survey, 81 percent of physicians indicated that their facility allowed some form of BYOD, yet only 32 percent had access to a dedicated help desk at their hospital with the necessary skills and knowledge to assist mobile users.[9] This lack of support can cause user frustration, create security risks if information protocols are ignored, and might even delay patient care because of disruptions to network access or important system integrations.

Part of the challenge for IT teams at facilities with a BYOD policy is the variety of device types and platforms that employees wish to use. Which ones will be allowed? Smartphones, tablets, laptops, wearables? Apple®, BlackBerry®, Android®? It might be prudent to prohibit devices that have modified control settings—aka jailbroken or rooted devices. One health system's chief information security officer stated that if the device can't be encrypted, employees can't bring it.[10]

Along with the identification of supported devices, there is also a need to decide how much help will be offered and how to provide it. For example, will the IT team offer assistance for new app installations, such as staffing tables in the cafeteria during a big rollout? And what about ongoing support for day-to-day questions about how to integrate with certain systems, how to use a hospital-provided app, and assistance with remote wiping of lost or stolen devices? The hospital may want to provide help only for certain types of questions. For trouble with devices themselves, such as faulty batteries or broken screens, it might make more sense to direct employees to their device manufacturer or service provider.

When deciding how to support a BYOD environment, consider the expertise and bandwidth of the current IT team, how many staff members are expected to need help, and how much support can be pre-designed with template FAQ documents. To give the desired level of assistance, a facility might need to hire or contract additional resources, and there is no one-size-fits-all answer. What works for one institution may not apply to another, and even within a hospital, different employee groups may need different levels of help based on their job functions and the necessity versus nicety of using their own devices.

WHAT IS EFFECTIVE AND ACCEPTABLE USE WHEN IT COMES TO BYOD?

For BYOD devices to be useful, it is important to involve end users in the decisions regarding network access and permitted applications, taking clinical workflows into account. From the clinician's perspective, effective use means devices that help them perform their jobs more efficiently by cutting wasted time from a workflow, or making a process easier. Effective use means better care for patients. From the hospital's perspective, defining acceptable use of devices is as important as making them helpful.

Acceptable use means enhanced security for protected health information (PHI) and better risk management. Some healthcare institutions go as far as requiring physicians to declare, in writing, that they understand HIPAA and how to use their devices to keep data protected.[11] This includes using unique passwords and installing a tracking app with remote wipe capabilities. If a physician does not implement the necessary procedures, he or she is not allowed access to the EMR.

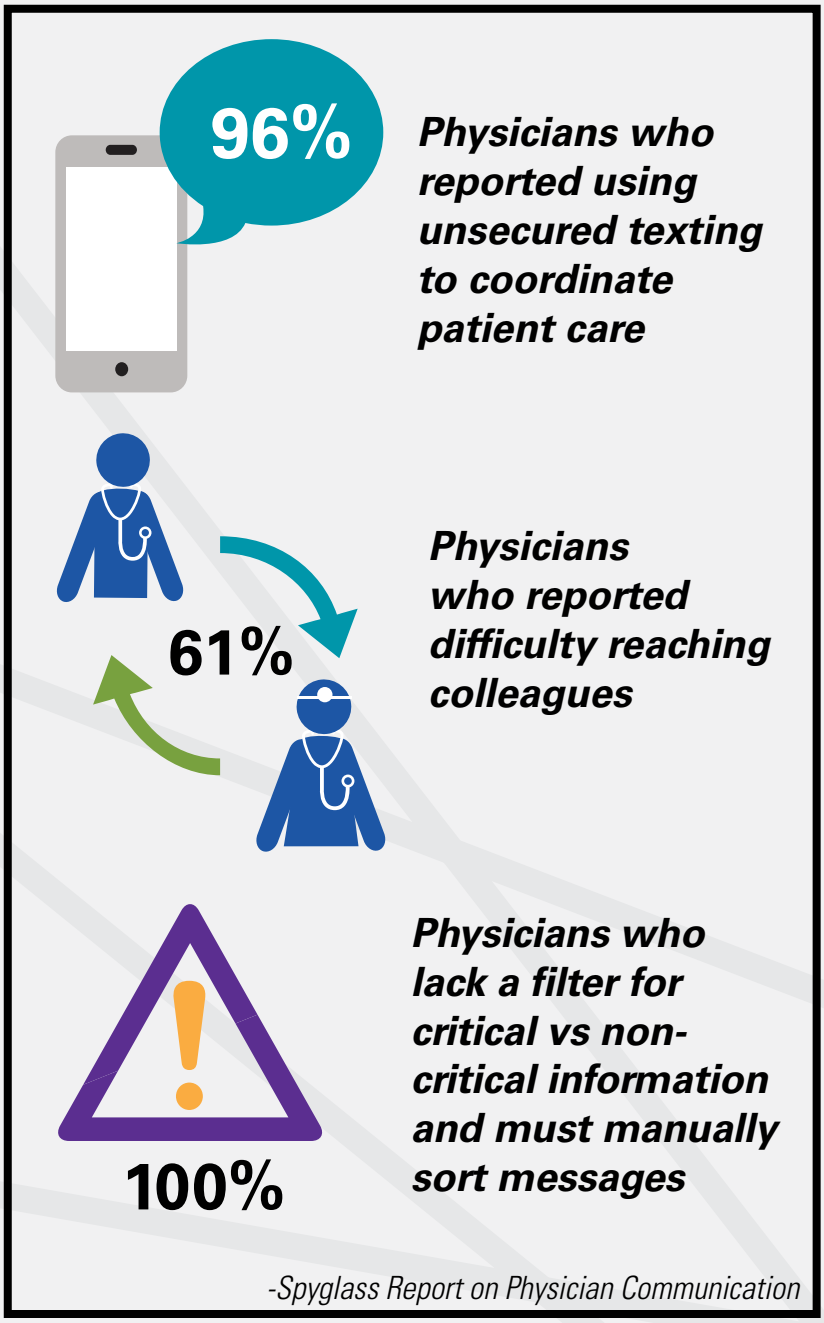
To provide this level of control over personal devices in the hospital, many organizations are getting help from mobile device management (MDM) solutions. An MDM solution can help hospitals keep track of all approved BYOD devices, control access to enterprise networks and systems, and manage app installations and upgrades. Another benefit of MDM systems is that they offer enhanced security. If a device is lost or stolen, or an employee leaves the organization, the enterprise access for that registered device can be terminated and all hospital-related data wiped remotely. Having an MDM solution can, however, raise a lot of questions for employees, and one CIO advises clearly communicating what the organization will and will not be able to access once the MDM client is installed on a personal device (e.g., personal photos, web searches, private email accounts, etc.).[12]

IS IT SAFE?

Though it might be very helpful for staff, full systems access through personal devices cannot always be granted due to data security concerns. The use of personal, mobile devices raises a lot of questions about security: what information is shared, is it secure in transit and storage, can it be saved to the device, or is it only accessible through a portal? Hospitals are concerned because the cost to healthcare organizations for a data breach can range from $10,000 to more than $1 million.[13]

While 88 percent of hospitals permit employees and medical staff to access enterprise systems such as email, 75 percent worry about employee negligence and 40 percent about unsecure mobile devices. Yet there is inherent risk in not providing enterprise access and support. Only 15 percent of physicians in a recent survey claim their hospital's IT team has a mobile strategy to support clinical communications and collaborative, team-based care. So what do the doctors do instead? Ninety-six percent report using unsecured SMS (texting) to coordinate care for patients, which puts physicians and hospitals at risk for HIPAA violations. Since 96 percent of physicians also reported using consumer grade smartphones as their primary device for clinical communications, one answer to help address the risk to patient information is a secure texting application.[14]

Not all secure texting apps are the same, though. Encrypted smartphone messaging software that is specifically designed for healthcare offers far more than just security. It also includes additional levels of service such as integration with the hospital's staff directory and on-call scheduling systems to help providers reach other members of the care team quickly. A secure texting app can be a filtering tool for physicians by organizing messages and alerts based on priority, and keeping work-related messages separate from personal notes and spam. Secure texting applications can also escalate critical messages to another team member if the initial recipient does not responded quickly, and provide traceability to help staff close the communication loop. A good secure texting app delivers effective use to clinicians, as well as acceptable use for the facility.



THE MULTI-SITE DILEMMA

BYOD device management is a unique challenge for physicians who work at multiple locations, especially if the sites are within separate health systems and use different enterprise technologies (EMRs, MDMs, email, etc.). An additional advantage of a robust, secure texting app designed for clinical workflows is that the single app can support a physician within multiple locations. By registering the device at each hospital or clinic, the same app creates and maintains separate profiles, with the data for each one stored securely on the individual servers at each institution. When providers move among hospitals or clinics, they can select the appropriate profile and be authenticated against that location's directory for messaging access. In general, providing a flexible, secure texting app helps tackle the HIPAA security risk by giving doctors a secure and highly useful care coordination solution.

CLOSING THOUGHTS

When planning a detailed BYOD policy and thinking through the big questions outlined here, one CIO offered two pieces of advice—start earlier than you think you need to, because it's a long process from planning through implementation, and learn from others.[15] BYOD best practices are still being developed, but there is collective experience you can draw upon for help. Seek to learn from others who have implemented a policy to find out what worked and what didn't. One solution for hospitals and IT teams is to consider working with a consultant group that has experience in healthcare communications and understands the clinical workflows that BYOD needs to support. This external support can help you coordinate staff for input, assist with planning, and even help with solution rollouts and end user training.

Whether you engage a consultancy, hire additional help for the project, or just research yourself and make some phone calls, creating a BYOD policy is not a simple task—it takes time, planning, and the involvement of all stakeholders to be both useful to users and successful at protecting data. But in the end, the investments will be worth the effort—staff will be happier and more efficient knowing what mobile device behaviors are expected and accepted, and data will be more secure. Ultimately, easier access to information, simpler communications, and faster collaboration among providers means better patient care.

References

[1,6,8] http://www.networkworld.com/article/2854044/microsoft-subnet/byod-is-saving-serious-money-for-it

[2] http://www.healthcareitnews.com/news/4-ways-make-byod-work-hospitals

[3,11] http://www.physicianspractice.com/mobile/byod-and-your-medical-practice/

[4,10] http://www.healthcareitnews.com/news/hospitals-begin-untangle-byod-knots

[5,12,15] http://www.mhealthnews.com/news/fine-art-and-hardest-part-crafting-byod-policy

[7] http://www.itmanagerdaily.com/byod-policy-template/

[9,14] Spyglass Consulting Group. (November 2014). Healthcare without Bounds: Point of Care Communications for Physicians.

[13] Ponemon Institute LLC. (March 2014). Fourth Annual benchmark Study on Patient Privacy & Data Security.

spōk℠

ABOUT SPOK, INC.

Spok, Inc., a wholly owned subsidiary of Spok Holdings, Inc. (NASDAQ: SPOK), headquartered in Springfield, Va., is proud to be a leader in critical communications for healthcare, government, public safety, and other industries. We deliver smart, reliable solutions to help protect the health, well-being, and safety of people around the globe. Organizations worldwide rely on Spok for workflow improvement, secure texting, paging services, contact center optimization, and public safety response. When communications matter, Spok delivers.

spok.com

/Spoktweets