July 2013

MOBILE HEALTH TRENDS 2013

BYOD HERE TO STAY

Providers struggle to fit implementations into meaningful use, HIPAA compliance mandates.

TechTarget

BYOD IMPLEMENTATION FORCES HIPAA COMPLIANCE, OTHER PROJECTS

SearchHealthIT's mHealth survey gathers providers' responses about their BYOD practices and how BYOD affects HIPAA compliance. BY DON FLUCKINGER

BRING-YOUR-OWN-DEVICE implementations are forcing health IT leaders to reconcile seemingly opposite objectives: tightening security to meet HIPAA compliance mandates going into effect this fall, while opening up systems to personal smartphones and tablets employees want to use on the job.

Enabling those devices and their simple operating systems to interface with complex back-end data systems tracking federal EHR meaningful use criteria also is a puzzle they must solve.

Such were the results from 240 respondents to SearchHealthIT's annual mobile health survey, which represented a mix of mostly providers, including ambulatory and inpatient healthcare IT staffers. More than two-thirds (68%) indicated mobile health devices are a part of their organization's ongoing IT strategy. More than half (51%) of total respondents said a range of 100 to 1,000 devices will be on their networks by the end of the year with a mix of tablets (81%) and smartphones (70%) overwhelmingly named as the highest-priority implementations, followed by laptops, telemedicine technology and medical devices.

A majority (58%) also said they are increasing budgets to accommodate mobile health integration plans. Almost two-thirds of the time (61%) those plans are drawn up by multidisciplinary teams, including clinical, IT and executive staff.

Some 37 IT staffers at payers also contributed responses to the survey. Several large payers are launching mobile health services, including Aetna Inc. Martha Wofford, vice president and head of Aetna's mobile initiative CarePass, said the back-end implementation took much attention to

data systems interoperability, as well as securing data for HIPAA compliance. The end result: A mobile portal that aggregates data from popular personal health apps such as FitBit, RunKeeper and Jawbone, and also serves as a healthcare provider directory and an appointment-booking tool that plugs into provider practice-management systems.

Aetna rolled out the system, which is available to non-customers as well policyholders, to increase brand mindshare as health insurance exchanges roll out in the wake of the Affordable Care Act (ACA). Wofford said Aetna chose a mobile platform because of its growing adoption among patients and providers alike.

The provider directory and booking tool takes advantage of mobile device-specific features, keyed to symptoms the patient enters into iTriage, one of the apps Aetna acquired and merged into CarePass. “We’re really trying to make that access point easier for people on the go,” Wofford said.

Many organizations are supporting multiple operating systems, with Apple iOS (82%) and Android (68%) leading the way, and Windows Mobile (54%) making a significant showing as well. Less than one-third (32%) of respondents indicated BlackBerry as a supported operating system. Regardless of whether mobile devices are provided by employer or employee, respondents’ issues included securing them, connecting them to EHR systems and application management.

Infrastructure and support are needed to integrate mobile devices in provider IT environments, respondents also said. Data encryption is number one (71%), followed closely by authentication of devices. Clearly many networks are supporting both employee- and employer-owned devices, as 68% of respondents said they were adding back-end authentication of personal devices and 53% said they were improving authentication of company-owned mobile devices. The other infrastructure pieces respondents are adding include wireless access points (53%) and unified wired/wireless access systems (45%).

Many organizations are supporting multiple operating systems with Apple iOS and Android leading the way, and Windows Mobile making a significant showing as well.

As meaningful use moves into stage 2, as the updated HIPAA omnibus rule goes into effect, and ACA quality reporting initiatives come online, respondents couldn’t pick which one impacted mobile device implementations most. Nearly two-thirds (62%) simply indicated, “All of the above.”

HIPAA security requirements, will impact BYOD implementations. John Houston, vice president of privacy and information security at UPMC, said despite the tightening

HIPAA security mandates, the BYOD movement in healthcare can't be stopped. IT leaders can only hope to contain it with well-reasoned, intelligently implemented policies and technologies. One example: To receive email from the health system on your own smartphone you must use Microsoft ActiveSync as UPMC sets it up with password rules and automatic timing out after a certain period of time.

"Bring your own device is reality. You don't have a choice; you can't bury your head in the sand and say, 'No, you can't do it,'" Houston said. "So what we've tried to do is work with vendors and make sure we have the appropriate technology in place to support [BYOD]."

Houston added: "But I look at bring-your-own-device issues really, very simply. We're going to develop common criteria; here's what we expect of you if you want your device to work. If you can comply with those requirements, you can use your device. If you don't want to use your device or you can't comply, you can't use your device on our network." ■

DON FLUCKINGER covers health care IT technology issues for SearchHealthIT.com. His 20 years of journalism experience includes covering topics as diverse as document technologies, hospital safety, nutrition, respiratory care department management and clinical research regulations.

CIOS FACE TOUGH DECISIONS IN SUPPORTING MOBILE

Apple iOS is still the top mobile operating system, but growing use of other platforms creates difficult decisions for CIOs. BY ED BURNS

WITH HEALTHCARE ORGANIZATIONS moving to make many of their critical applications available on mobile devices, determining which platforms to support has never been more important. A new SearchHealthIT mobile health trends survey shows that while Apple's iOS operating system is still the most commonly used in healthcare, other mobile operating systems may be creating more decisions for CIOs.

The poll of 240 hospitals, medical centers, payers and other healthcare professionals, showed that iOS is still on top. When asked what mobile operating systems are used at their office, 81.7% of respondents said Apple's operating system has a presence. Behind iOS, 67.7% said Android was used in their office, 53.7% said Windows Mobile and 32.3% said Blackberry.

When asked if they could standardize mobile device use across only two operating systems, 74.5% of respondents said they would choose iOS. Android was respondents' second choice, at 49.7%, with Windows mobile just behind, at 42.9%. Just 14% said they would choose Blackberry.

Apple products may still be favored at healthcare organizations, but the rise of Android and Windows mobile systems has given providers more options. And even though few would choose Blackberry going forward, many organizations invested heavily in recent years and still use legacy systems. This means healthcare providers must support a wide range of mobile operating systems.

Greg Walton, chief information officer of Silicon Valley-based El Camino Hospital, said he sees clinicians wanting to use the full range of devices. While many use Apple products, he actually sees more Android devices than anything else.

The profusion of devices and mobile operating systems

may raise security concerns. More than 71% of survey respondents said security management was one of their top two mobile device integration issues. Allowing clinicians to use whatever device they want means putting in place security controls for each operating system and making sure every user has updated to the latest version.

While smartphones may be nearly ubiquitous among healthcare providers, organizations are putting more emphasis on deploying tablets in healthcare settings.

Some have expressed concerns that Android products might be particularly risky. The operating system is open source and just about anyone can get an application into the Google Play Store, which may open the door to malware. But Walton said his hospital supports Android devices because supporting a broad range of mobile operating systems empowers clinicians and is a boon to productivity.

"Risk is not black and white; risk is always gray," Walton said. "You have to take measures in your journey through time to mitigate risks with appropriate policies, practices and technology. We're always adjusting to the levels of issues that we face. I'm not terrorized by Android."

Chris Belmont, CIO of New Orleans-based Ochsner Health System, said the growing number of employees bringing their own devices requires him to provide support for a wide range of operating systems, as there is a great deal of diversity in the consumer technology market.

"I've given up on keeping track of devices and device types," he said. "It's kind of a personal device or it's not, and it could be a tablet or a smartphone. The lines are getting really blurry between those devices anyway. So we're trying to figure out how best to address it."

While smartphones may be nearly ubiquitous among healthcare providers, organizations are putting more emphasis on deploying tablets in healthcare settings. Just over 81% of survey respondents said supporting tablets is among their top device integration priorities, while 68.9% said they were focusing on smartphones.

Belmont said Android and iOS devices are open environments, which can introduce some security risks. BlackBerry may be more secure, but few people are buying new BlackBerrys, so it would be difficult to choose to support only those devices. Going forward he will continue to look for ways to safely and securely support a full pallet of devices. ■

ED BURNS, covers health care technology for SearchHealthIT.com. Prior to joining the site, he wrote news stories for a variety of health care clients covering areas such as information technology, wellness, insurance and behavioral health.

MOBILE HEALTH TRENDS SURVEY RESULTS

SearchHealthIT survey results are in, and show mobile technology has a large role to play in healthcare.

MOBILITY ENABLES MEANINGFUL USE

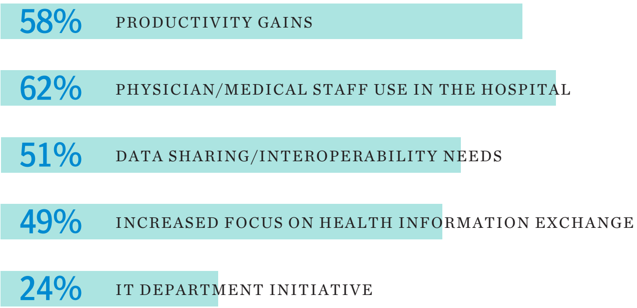
How does mobile technology enable physicians to achieve meaningful use? Allowing physicians to access their EHRs via mobile devices is one of the most obvious ways. But, only a small proportion of physicians are relying entirely on mobile devices to enter data into EHRs. Many are reviewing patient data on mobile devices like iPhones and iPads because of the convenience associated with having mobile devices everywhere. IPads are becoming ubiquitous in the hospital setting. Almost every doctor I know has an iPhone or Android smartphone.

But is the application of mHealth limited to EHRs?

Many mobile platforms now allow physicians to communicate securely with other providers, which helps improve care coordination. Doctors can even communicate with patients through secure mobile messaging platforms. So, discharge instructions and patient self-management tips can be sent via these mobile tools. Plus, patients can access their PHR data on mobile devices, so mHealth is active as an enabler for both patients and providers.

FIGURE 1 Factors driving the use of mobile devices

Total Responses: 164



Source: TechTarget 2013 Mobile Health Trends survey

Mobile alerts can also guide doctors through important clinical decision support—and I'm not just referring to drug allergy warnings. Mobile health can alleviate the alert fatigue burden that may be slowing doctors down when they're trying to treat a patient. Mobile devices can also make the clinical workflow more efficient so that data that is entered into an EHR is used more efficiently. Finally, there are a growing number of mHealth solutions that will help providers with HIE requirements surrounding all that patient data they're collecting in their offices.

Mobile devices can also make the clinical workflow more efficient so that data that is entered into an EHR is used more efficiently. There are a growing number of mHealth solutions that will help providers with HIE.

As buzz around new devices like the iPhone 5 and the rumored iPad mini circulate throughout cyberspace, we know that doctors are paying attention. They want to use the latest gadgets in a meaningful way to improve patient care. —*Joe Kim, M.D.*

» Read more about mHealth and its applications for providers from SearchHealthIT expert Joe Kim

INTEROPERABILITY BECOMES MORE URGENT AS DATA EXCHANGE INCREASES

IT systems will have to become more interoperable, as the healthcare system continues to transition away from fee-for-service payment models. Providers will be expected to collaborate on keeping patients well, which means doctors in different offices and care settings will have to share information with each other.

"The ability to do a query of the data to see what happened to the patient is critical to the ACOs," said Janet Hofmeister, senior program manager for state HIE programs at Harris Healthcare Solutions, which operates the Florida HIE. "They need to know when the patient goes to the hospital" or other care provider.

This means that practices that decide to operate as an ACO will be reliant on systems that can connect to other vendors, either directly or via an information exchange. Hofmeister said she feels there is sufficient infrastructure in place to facilitate this kind of connectivity at the scale that will be needed for the health system to transition to accountable care.

But David Caldwell, executive vice president at San Jose, Calif.-based Certify Data Systems, isn't as optimistic. He said that many of the practices moving to value-based purchasing systems may be disappointed at the availability of the infrastructure needed to connect with partner organizations. ACOs have been "focused more on the model

BYOD Implementation Forces HIPAA Compliance

CIOs Face Tough Decisions in Supporting Mobile OSes

Mobile Health Trends Survey Results

of care than the IT infrastructure," he added. "As they take on financial risk, they're going to wake up."

Assuming that EHR systems become more interoperable in the near future, the role of HIE organizations may change. Currently, they function as intermediaries that take data from disparate organizations and put it into a format that others can use, regardless of their IT system. But if the industry progresses to a point where each EHR system can produce standardized documents and seamlessly share this information with other systems, there will be less of a need for organizations that do this.

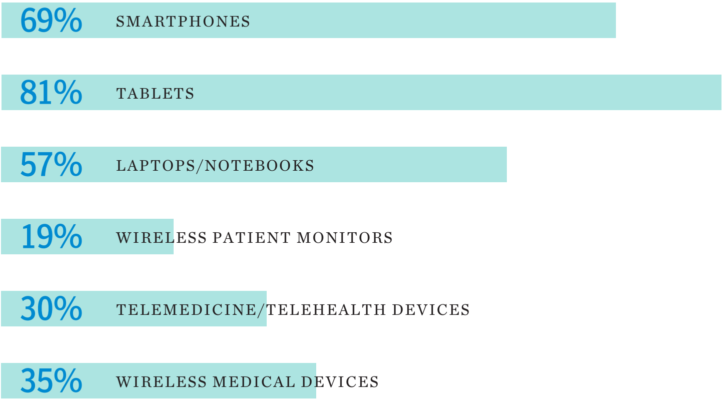
Hofmeister said HIEs will eventually become the "string that holds the pearls." Just as home Internet users still need a line from their cable or phone company piping the Internet to their house, users of interoperable EHR systems will need some kind of infrastructure to carry their information. Hofmeister sees HIEs providing this service.

Caldwell agreed that public HIEs won't disappear, even when their current role diminishes. He said they will become the "network of networks" that will help connect doctors' offices. Within three to five years, all vendors will be offering completely interoperable systems, he added. By this point, providers won't need HIEs to translate documents for them. ■

» Read the full two-part story here.

FIGURE 2 Top device priorities for healthcare

Total Responses: 164



Source: TechTarget 2013 Mobile Health Trends survey

CLINICAL MOBILITY ON THE RISE

Many doctors need access to patient records and health IT systems when they are outside of a hospital setting. They need access from home at any time of the week. Some physicians also need immediate access for when they are taking a lunch break in the hospital cafeteria.

For doctors, clinical mobility is about having access to entire, fully functional health IT platforms from a small, light mobile device that is connected to their health system network. Doctors who travel to different hospitals and

clinics may be faced with using different EHRs and computerized physician order entry (CPOE) systems. Password security and single sign-on are important to avoid patient data breaches. Many doctors are trying to make tablets like the Apple iPad meet their needs, but the Apple iOS doesn't support most enterprise-level applications, such as inpatient EHRs or CPOE systems. Workarounds to address these gaps have been slow and cumbersome at best.

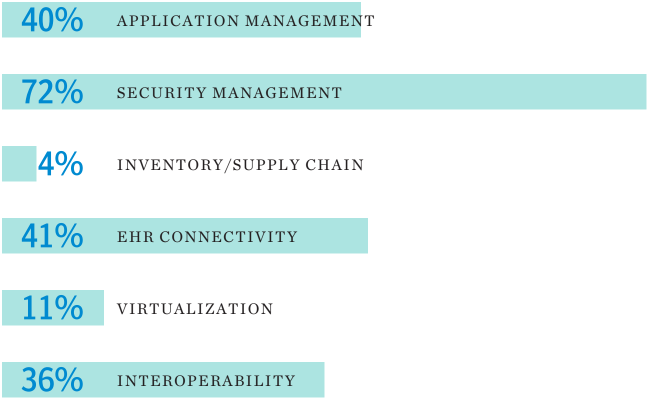
Newer tablets running Windows 8 show tremendous promise for physicians who are willing to be early adopters of an operating system that isn't as intuitive as iOS. Physicians rapidly are discovering that the benefits of having access to a fully functional PC can outweigh the disadvantages. We will be seeing smaller Windows 8 tablets this summer. These devices should be more "pocketable," for example, the popular Apple iPad mini, which has an 8" screen and fits nicely into a white coat's pocket. ■

Health care organizations typically aren't one-vendor shops when it comes to mobile device support.

» Read more on clinical mobility and the growing use of patient monitors and wireless devices from SearchHealthIT expert Joe Kim, M.D.

FIGURE 3 Top device integration issues

Total Responses: 162



Source: TechTarget 2013 Mobile Health Trends survey

MOBILE DEVICES = SECURITY MANAGEMENT IN HEALTHCARE

Health care organizations typically aren't one-vendor shops when it comes to mobile device support.

While Apple Inc. may enjoy a head start in some hospitals, Google Inc. Android smartphones and tablets and the Research in Motion Ltd. BlackBerry often contribute to the mix as well. Moreover, if IT shops don't formally provide handsets and tablets, chances are physicians or other staff

members will bring them on the job. The number of mobile options hitting the market—including hybrid "phablet" form factors such as the Samsung Electronics Co. Galaxy Note—will further cement a multi-platform environment.

"Innovation is happening at an exploding rate in... consumer electronics," noted Gregg Malkary, managing director of Spyglass Consulting Group, which focuses on mobile technologies in health care. "Hospital executives and doctors have the devices, so there is more pressure to support the next-generation mobile devices."

How are health care providers managing and securing heterogeneous devices and the information they access? Health IT executives and consultants suggest a combination of mobile device management, data protection tactics and user education. ■

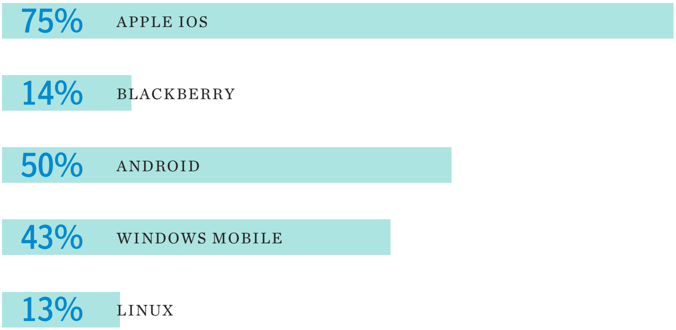
» Read the full management security tip here.

What are the pros and cons of native apps and web-based apps?

Read the discussion on Health IT Exchange.

FIGURE 4 Preferred operating systems

Total Responses: 161



Source: TechTarget 2013 Mobile Health Trends survey

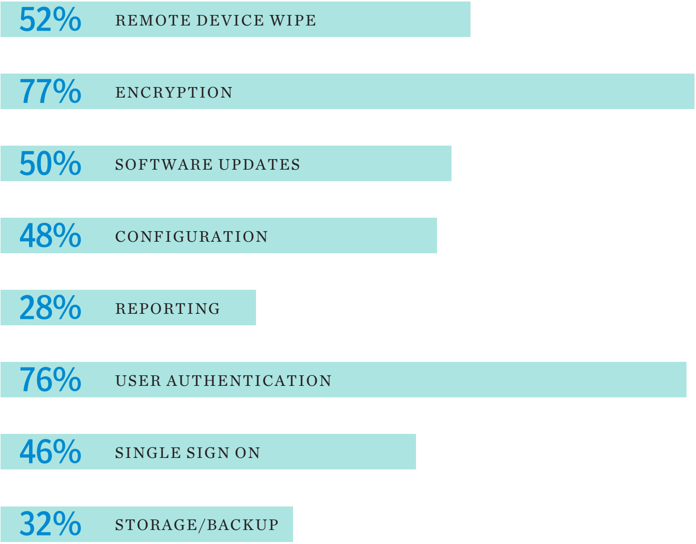
MAINTAINING HIPAA COMPLIANCE

Strategies for maintaining HIPAA compliance while giving clinical staff the flexibility and access to data they need:

- Store as little data as possible on the mobile devices.
- Make the device require a token and a user ID/password.
- Encrypt data in motion.
- Log off users after idle.
- Auto-delete EHR app cache after a specified time.
- Set geographic access boundaries according to role.
- Enable remote controls.
- Require face-to-face encounters for device setup.
- Resolve patient lists for each practitioner.

FIGURE 5 Concerns for device management

Total Responses: 163



Source: TechTarget 2013 Mobile Health Trends survey

BALANCING DATA PROTECTION AND PERFORMANCE

One of the hottest trends in health care organizations is that of using mobile devices to access electronic health records. Although accessing electronic health records (EHRs) through mobile devices provides an unprecedented level of convenience, it also exposes health care organizations to new security risks.

Mobile device encryption helps mitigate security risks. Data must be encrypted while it is in transit, but it must also be encrypted when it is stored. In spite of the need for encryption, some health care organizations have been reluctant to require encryption for mobile access of EHRs for fear that the encryption process will cause a major performance impact.

Currently there are a number of different vendors offering solutions for accessing EHRs on mobile devices such as smart phones or tablets. Most of the mobile EHR solutions do not store large patient health databases on the mobile devices. Factors such as limited device capacity, the need for databases to be centrally accessible and the potential for data exposure if the device is ever lost or stolen have lead most vendors to create mobile EHR solutions to act as a front-end application that interfaces with a back-end database.

Although most mobile EHR applications do not attempt to locally store patient data, mobile device storage encryption is still important. Mobile applications often cache patient health data in an effort to improve the application's response time. Unless encrypted, this cached data potentially could be exposed if a mobile device were lost or stolen.

When it comes to storage encryption, health care

organizations should insist on hardware-level encryption. Although there are a number of software-based encryption solutions for mobile devices, software solutions consume system resources such as memory and CPU cycles, thereby leading to diminished performance. Conversely, hardware-level encryption usually has no noticeable impact on performance.

Most of the major mobile device manufacturers offer hardware level encryption, but there are certain nuances on each platform that IT pros need to be aware of. For example, Android devices offer hardware-level encryption, but only on Honeycomb- and Ice-Cream-Sandwich-based devices. Likewise, iPhones and iPads running iOS 4.0 or later also support hardware-level encryption, but the encryption is not turned on by default.

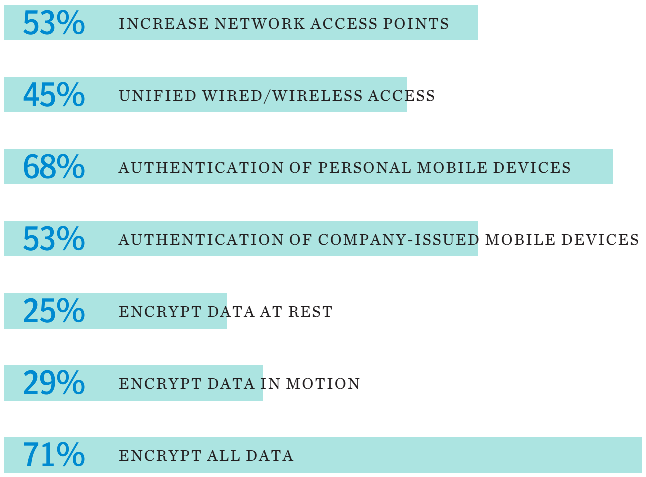
Windows Phone 8 devices support hardware-level encryption that is always turned on. However, because the encryption is based on the use of a trusted module platform chip, Microsoft Corp. chose not to perform hardware-level encryption of removable secure digital (SD) cards. Because SD cards are not encrypted, the Windows Phone 8 operating system will not allow sensitive data to be stored on them. SD cards can only store music, photos, videos and eBooks. ■

» Read the full encryption tip from SearchHealthIT expert Brien Posey here.

FIGURE 6

Infrastructure priorities for device integration

Total Responses: 161



Source: TechTarget 2013 Mobile Health Trends survey

BEST PRACTICES FOR DEVICE INTEGRATION

As mobile health technology advances, such devices as smartphones and tablet PCs, many of which fit into coat pockets, will create more, and more attractive, targets for thieves. When these devices store patient data locally, theft equals data breach. To that end, here are several tips to CIOs creating or tuning up their security schemes for mobile health patient interactions:

BYOD Implementation Forces HIPAA Compliance

CIOs Face Tough Decisions in Supporting Mobile OSes

Mobile Health Trends Survey Results

- **Perform a risk analysis before implementing mobile technology.** Ferret out weak points and buttress them with security. For example, if you are distributing protected health information on smartphones, imagine the scenario of a physician or patient losing the phone, and determine how to protect the data stored on it well in advance of a breach.

- **Create and enforce sound employee policies that prevent improper sharing of information.** Privacy and security are separate things, and require different maintenance methods. Patient privacy typically is maintained by an organization's written policies, which cover everything from password-sharing to data disposal and also need provisions for enforcement when errors are made. Security, meanwhile, is technology, such as encryption, that keeps the bad guys from accessing HIPAA-protected data.

- **Make security simple.** If a password is too hard to remember or figure out in the first place employees and patients either will not use it or will create workarounds. The same goes for routines built around security policies. One example would be a portable, wireless-enabled emergency-room computer workstation set up to log out the most recent user automatically after the computer has been idle a minute or two, keeping unauthorized parties from viewing open medical records. Automated logouts are usually effective, but in this case the frequency is such that it interrupts the workflow of physicians and nurses in a typically bustling environment.

- **Tell them what you're going to tell them with an open messaging system.** Phones and their networks can be less secure than laptop and desktop computers. If you're texting or emailing patients reminders about routine care matters (upcoming appointments, tests or prescription refills, for example) perhaps the most secure HIPAA-compliant method is to make the message itself free of protected health information. One way to do this is to write something along the lines of "Your doctor has an important message for you at ..." and refer them to a secure Web link where they have to log on with a password to get specifics.

- **Use two-factor, bidirectional authentication.** An example of this type of authentication would be checking a password and token at both the device level and the server level. Doing this confirms that the person trying to log onto that Web link to retrieve a message is the actual patient. This authentication method also offers an additional safeguard before HIPAA-protected information is pushed to a smartphone. ■

» For more resources on this tip, read the full story here.

EXPERT BYOD POLICY Q&A WITH JOHN HALAMKA, M.D.

Beth Israel Deaconess Medical Center (BIDMC) CIO John Halamka, M.D., offers his insights and suggestions to SearchHealthIT on bolstering HIPAA compliance with BYOD policy.

How did you get buy-in from the physicians for the BYOD policy, and who had to give them the news?

It was relatively quick. I think it was Rahm Emanuel that said, "Never let any crisis go unused," or something to that effect. When you have a sentinel event, a laptop theft, that is a catalyst for change. That's really what happened with us: A physician's personal device was stolen, and the entire physician community became aware of the nature of the consequences of such a device with cost, patient notification, institutional reputation, etc.

There was broad support at the medical executive committee level across all the senior clinician leadership to move forward with this initiative. I think the person who asked the question is right: If you didn't have a sentinel event and people didn't understand the risk, it would be a harder sell. So your choice is have something bad happen and mitigate, or try an aggressive education program to get buy-in.

How do you "sell" that policy of auto-wiping personal devices after 10 failed password attempts? It must be a hard pill for employees to swallow.

Yes, it isn't "Oh that's wonderful, you're going to erase all my personal data!" It has to be sold in terms of risk. If you look at the regulatory and compliance environment today, the cost of a stolen mobile device can run $300,000 or $500,000 when you're looking at legal, forensics and patient notification.

So you say to the person: "You are ultimately responsible for your personal device. There could be hundreds of thousands of dollars in penalties, some could even possibly accrue to you. Or we could just insure that we auto-wipe the device after 10 tries, because if you put a four-character password on it all somebody has to do is try 9,999 times, and privacy is breached." With that understanding of risk and responsibility, people have accepted the auto-wipe feature.

How can you protect medical devices from hackers? Not necessarily a BYOD question yet, but I am sure you're anticipating that happening as more patients walk in with their own sensors they've purchased accessing Bluetooth, Wi-Fi, etc.

This is a huge issue. You would think, when you buy a device, it's like a toaster: All completely self-contained, it's fine. Nope! A lot of these devices you would buy—like EKG machines, IV pumps, imaging devices—they are like Linux workstations running Apache from five years ago.

What happens, and it's a nasty problem for the country, is that the FDA wants to look at the safety of medical devices and they say: "You've certified with us Apache version 1.0, running on Windows NT. Now if you want to update that with a patch or a new level of operating system, you have to go through the certification program again, at great expense." So you end up with a lot of these appliance type devices that are security nightmares. We've had to build network isolation around them, not connect them to the Internet, and put special monitors for intrusion detection and prevention systems—because they could be spewing viruses all over your network unless you isolate them.

A word on implantable devices, such as pacemakers: They are not safe. They contain microprocessors. They have the same issues—memory overflow, buffer issues, SQL injection—every kind of hack you can imagine on an application in the data center is probably applicable to an implantable device. And that issue has not been well addressed yet.

We use Citrix for remote access; we don't allow remote workers to access the local drive. But that doesn't prevent someone from taking screen shots or saving email locally. How do you address this in a BYOD policy?

Citrix is quite fine for thick client applications that can't run locally, and many corporations use it to protect security and intellectual property inside the firewall. One challenge we all have is that doctors are extraordinarily impatient people, and the startup time for a Citrix session and sometimes the instability over a flaky Internet connection can be a disincentive for doctors to buy in.

A word on implantable devices, such as pacemakers: They are not safe. Every kind of hack you can imagine on an application in the data center is probably applicable to an implantable device.

We have a combination of Citrix for some applications and Web-based applications for others that can be used anywhere on any device. And telling clinicians "You have a policy requirement not to store data locally, not to do 'save as' or print screens," because you recognize that creates a breach situation. To mitigate that breach situation, what we've already done is encrypt the device; so should they "save as" or print screen, in some ways we've gotten around breach reporting requirements. But you wonder, ultimately, if you're going to have to go to a virtual desktop infrastructure so even if you do print screen or "save as," at the end of the session it disappears. But VDI really does have the same issue as Citrix: slow startup time and challenges over low-bandwidth connections.

Meaningful use stage 2 local encryption requirements, just so you know, actually have specific language that says "Yes, the product you use must keep any local data stored or cached encrypted, but if a user does a print screen or a 'save as,' that is really the responsibility of the user." It's not something the vendor or the covered entity has to take accountability for; it's the user's responsibility not to do that and to keep their devices appropriately secured.

Do you run HIPAA risk assessments on every device on your network or how does that work? An example is, did you run testing on the iPhone 5 before allowing its use on your network?

Good news is, the evolution of most of these operating systems is such that you have basic, floor-level encryption and as the OS evolves, it just gets better. So for example, our HIPAA risk assessment says is that we believe we have adequate protection on Apple iOS 4.1 or higher; Mac OS X 10.7 or higher; BlackBerry OS for all of the 200 users we have left in our enterprise 4.5 or higher; Windows 7 Professional or higher and Android OS 2.34 or higher. So in that sense you've created a floor and as new devices are introduced they are grandfathered into that floor.

I will make the comment about Android: Although Apple controls iOS, single vendor control, you don't really have a single vendor controlling Android, so there's really no guarantee new Android devices will work well with our server-side controls (i.e., ActiveSync Exchange enforcing encryption). So often we find that Android devices need to be tested just to make sure they'll work. Not so much that the risk is going to be worse in the newer devices, but that they will even work.

The evolution of most of these operating systems is such that you have basic, floor-level encryption and as the OS evolves, it just gets better.

Do you maintain a list of recommended or mandated devices? Do employees even ask for advice about using their devices?

The challenge with bring your own device is that people view this as their personal device. It's like saying, "We have decided you will drive an economy car, and Prius is the best choice." It's very challenging to do that. Everyone has different values. Everyone has different needs for different applications, for different form factors.

So we set policies for minimum functionality, and how it is you should physically secure the device, and certainly we can provide guidance on an operating-system level. But ultimately it's up to the individual what they choose. If you choose poorly, you could end up with a device that just doesn't work on the network.

How do you control how terribly chatty firewalls can be? Interesting question. What the person is getting at is that, as you put various protections on the server side and the client side, they have overhead. Some protocols, some approaches send lots of data back and forth, and the nature of that data might be “Hello, I’m out here and I’m safe!” “Are you sure?” “Yes I am!” Constantly going back and forth with chatty protocols.

We have tried to avoid the introduction of technologies that have such high overhead that they impact network performance. This is an incredibly rapidly evolving technology stack.

As we do all of our benchmarking of new technologies, we end up using appliances that we put out at client site to look at the nature of bandwidth flows from their sites and look at application performance. We have tried to avoid the introduction of technologies that have such high overhead that they impact network performance. This is an incredibly rapidly evolving technology stack, a huge moving target. Today’s gold star might be tomorrow’s complete failure. The technology is changing daily, do your best to select a winner...we do a lot of testing before selecting a product. ■

TechTarget

Mobile Health Trends 2013
is a SearchHealthIT.com e-publication.

Jean DerGurahian, *Editorial Director*

Don Fluckinger, *News Director*

Jennifer Laurello, *Senior Community Manager*

Ed Burns, *News Writer*

Alex DelVecchio, *Assistant Editor*

Linda Koury, *Director of Online Design*

Stephanie Corby, *Publisher*, scorby@techtarget.com

TechTarget
275 Grove Street, Newton, MA 02466
www.techtarget.com

About TechTarget: TechTarget publishes media for information technology professionals. More than 100 focused websites enable quick access to a deep store of news, advice and analysis about the technologies, products and processes crucial to your job. Our live and virtual events give you direct access to independent expert commentary and advice. At IT Knowledge Exchange, our social community, you can get advice and share solutions with peers and experts.

COVER ILLUSTRATION: VETTA/ISTOCKPHOTO