Data privacy and security:

How hospitals and providers view HIPAA mandates and data protection technologies

As the health care industry becomes increasingly tech-driven, the privacy and security of data moving through electronic systems becomes increasingly important and -- simultaneously -- more difficult to achieve.

Requirements through the HITECH Act have led to a surge in IT adoption in health care, including electronic health records (EHRs), computerized physician-order entry (CPOE), medication bar coding, and clinical-decision support. Supplementing the technology is a wave of mobile devices from smartphones to tablets, which allow providers more flexibility in how they are accessing and using patient data.

With this surge has come an increase in data breaches, prompting the government to pass updated enforcement laws under HIPAA. The data breach notification rule requires providers to disclose when unauthorized access to patient information has occurred.

Despite the more stringent environment, there is a lack of urgency for figuring out how to achieve IT security among providers who are confident they're already doing enough. A recent survey of *SearchHealthIT.com* readers indicates that hospital administrators believe they are meeting federal laws with their current policies while, at the same time, they recognize that data protections must be a priority.

Just how much of a priority is the question, however. In the past there has not been a significant amount of enforcement from federal officials, and that's led to some lack of policies in physician practices, according to Robert Tennant, senior policy advisor with the Medical Group Management Association (MGMA). That said, it's likely the Office for Civil Rights (OCR), which oversees the HIPAA data breach rule, will be more aggressive about enforcement in the future.

With more devices and more technology comes the need for more education, Tennant said. To providers who haven't needed to pay much attention to tech concerns, "it's such foreign territory. A lot of folks have no idea what encryption is."

Fixing that requires education, Tennant added. "I think when you explain it to them in practical terms, it's easier."

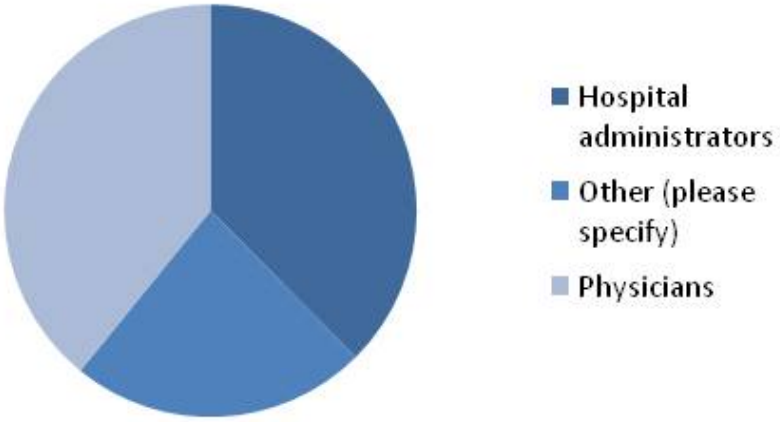
The laws themselves could use some work, as well. Data breaches are becoming significant, but the laws only punish; they are not encouraging anyone to look at their networks to see where and how breaches occurred, according to James Tarala, principal consultant with Enclave Security, a data protection services firm. True network security is different from reporting that laptops have been stolen. "I don't know if the controls are in place."

The *SearchHealthIT.com* survey results explore some of these issues. From what's driving security needs to how systems are being protected, providers explain their thoughts. The results are based on 254 responses from IT professionals and executives at health systems, hospitals, physician practices and other care organizations to an online questionnaire conducted in April 2011.

- Jean DerGurahian, Executive Editor

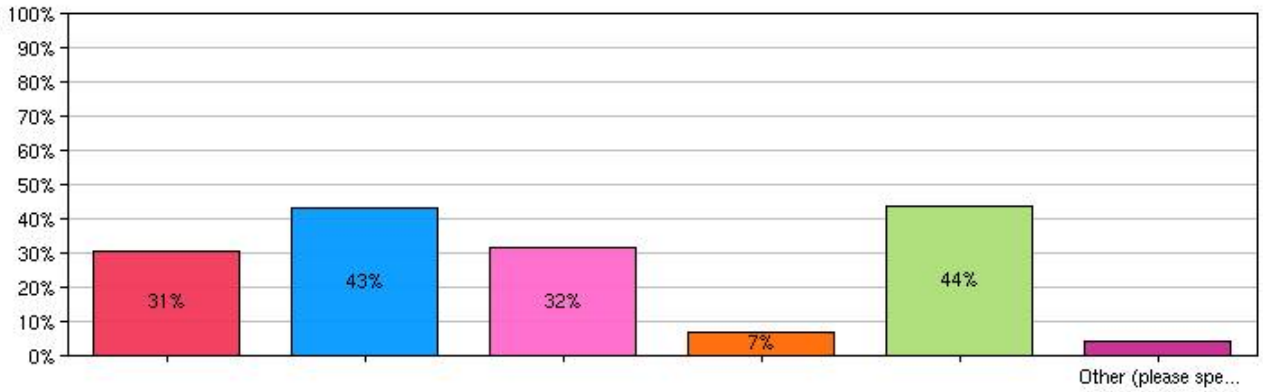
Who is the biggest influence on whether and how point-of-care wireless devices are used in your hospital?

While physicians and administrators are fairly evenly split in driving technology use at hospitals, with 39% of respondents saying doctors and 37% saying administrators do it, several other staff in the organization are also involved.



Some 23% of respondents said device use is a collaborative effort, which includes people from: Information services department; nursing and other caregiving staff; corporate executives; privacy/compliance departments; attorneys; marketing; and manufacturers.

What are you doing to secure your hospital's wireless network?



Value	Count	Percent %
Partitioning it so patient data is separate from everything else.	78	30.7%
Strengthening the authentication necessary to access clinical applications.	109	42.9%
Replacing WEP encryption with more robust WPA encryption.	80	31.5%
We do not have a wireless network.	18	7.1%
We have already fully secured our wireless network.	111	43.7%
Other (please specify)	11	4.3%

Managers are taking steps to secure their networks and are considering which technologies they'll need to achieve that security. While many respondents feel their networks are secure, more efforts will be focused on encryption and mobile devices in the next year. Read the general tips on the following page from health care leaders about what goes into implementing a network.

Improving hospital wireless network implementation in 10 steps

Understand your users' habits as well as their physical environment. Lead-walled radiology departments are probably the toughest wireless puzzle to solve, followed by bathrooms and elevators. Build these thorny wireless-killers into your site survey -- and don't be afraid to press vendors to explain how they will overcome them.

Build future plans into the rollout. Plan extra bandwidth for emerging technologies that will be coming to many hospital wireless networks in the next few years. These include Voice over Internet Protocol, or VoIP, phones as part of unified communications systems; RFID tags; a general proliferation of laptops, tablets and smartphones; and more wireless patient monitoring devices.

Hire a consultant. LRGHealthcare in central New Hampshire, hired an independent wireless systems expert to help conduct a site survey and develop its request for proposals (RFP). This outsider gave them such sound advice, helped them develop such a detailed game plan, and gave them so many ways to grill the vendors that they don't consider the fees an up-front cost.

Make the RFP as detailed as possible regarding future plans. In its RFP, Milford (Mass.) Regional Medical Center specified that its new hospital wireless network would have to support additional devices, as well as voice and video, but not interfere with clinical engineering apps. Not all of that is up and running, but the network infrastructure is there for expansions that probably will happen in the next two to three years.

Consult with other departments. The infection control and safety officers may have input on placement or protection of wireless gear. As you write your wireless network implementation plan, consult them and other stakeholders, such as facilities management.

Check references. Ask for customer references from RFP finalists. Question them about their own RFP process, about how a particular wireless integrator responded to support calls and meeting deadlines, and about how happy they were with the security setup, as well as about physicians' general satisfaction with their wireless networks.

Consider guest use carefully. What information will you collect from guests who log on to the network? How will you limit their use of the network, as well as secure protected patient data from the clinical side? Firewalls, network partitions, strong authentication, wired equivalent privacy (WEP), key management, and expiration can all be part of the plan.

Plan to monitor for rogue access points. Vendors should demonstrate how their wireless controller systems can identify and shut down rogue access points quickly. Sometimes rogue access points are "friendly fire" -- a physician bringing in a router to boost the signal in his office, for example -- not a hacker trying to steal patient information.

Pilot gear from multiple vendors in your environment. All equipment works great on paper, but mileage will vary in real life. Moreover, in testing, not only coverage and bandwidth speed should be evaluated, but also clinical application performance.

Keep the patient in mind. Sometimes among the RFPs, the regulatory compliance, the budget concerns and interoperability issues, the patients get lost in the shuffle. With every decision, don't forget to keep patient care in mind as the final arbiter of your

Read more about these wireless networking issues from interviews with three health IT experts at leading medical facilities on SearchHealthIT.com.

Boost your medical device security

Cybersecurity vulnerability exists whenever the software provides the opportunity for unauthorized access, according to Food and Drug Administration (FDA) software compliance expert John F. Murray Jr.

"Medical device manufacturers spend a large amount of time and money and effort in making safe devices, and cybersecurity represents a hole in that."

Read more of Murray's recommendations on SearchHealthIT.com

Privacy compliance in the networking environment

Health care CIOs are caught between a rock (technology) and a hard place (regulation). On the one hand, demanding patients and increasing numbers of wireless medical devices are requiring they open up their wireless networks. On the other, tighter rules for HIPAA privacy compliance are forcing them to lock networks down with encryption and tighter access control, lest they find their facility's name posted on a government website in connection with a data breach.

For John Cameron, computer technical specialist and wireless technician at the 121-bed Milford (Mass.) Regional Medical Center, accommodating guests while maintaining HIPAA privacy compliance on the facility's new wireless network begins with three technology measures:

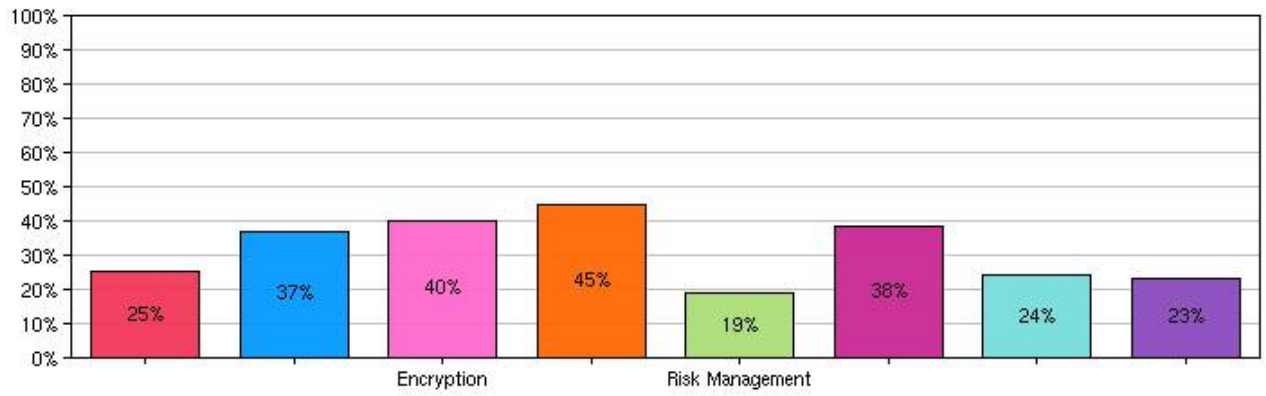
• Partitioning the network and keeping patient data and guest activity on separate partitions
• Limiting guest activity to the browser -- that is, no virtual private networks, or VPN, or other applications
• Using public domain name servers, or DNS, for the guest partition, not the hospital's own

HIPAA guidelines also should be taken into account when the hospital's medical equipment buyers order new wireless gear, Cameron recommended.

Not every monitoring device or wireless intravenous pump has the capacity to encrypt the bits of data that HIPAA protects, such as name and date of birth. That reality should be factored into buying decisions whenever possible. On the same point, all the medical devices in use on a hospital's wireless network should be evaluated and the security settings maxed out, he added.

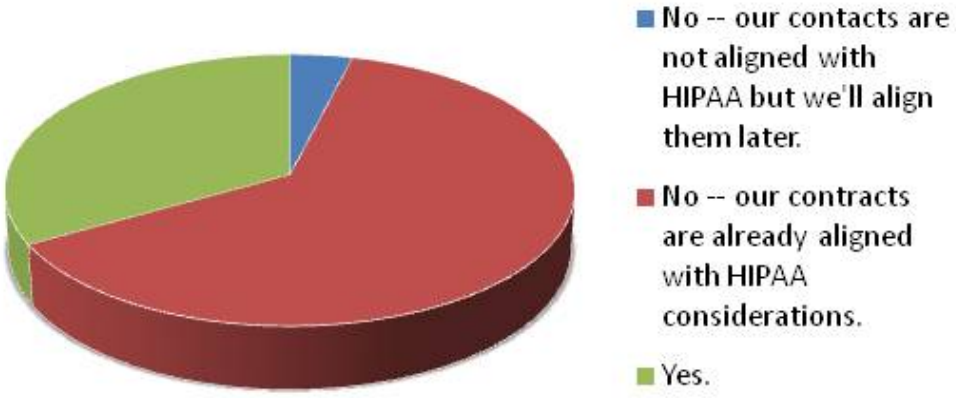
"Work with the [wireless and biomedical equipment] vendors on getting the highest security level you can get with what you have," Cameron said. "Biomedical gear is a couple years behind in the wireless field. Eventually, when they come on to the wireless, we need to make sure they can withstand a certain amount of encryption . . . and make sure it's within the HIPAA guidelines."

Which of the following technologies do you plan to purchase in the next year to help your organization achieve HIPAA compliance?



Value	Count	Percent %
Data Loss Prevention	64	25.2%
Data Backup/Storage	94	37%
Encryption	102	40.2%
Mobile Device Security	113	44.5%
Risk Management	48	18.9%
User Authentication/ID and Access Management	97	38.2%
Vulnerability Management and Assessment	61	24%
Wireless Network Security	59	23.2%

Are you planning to update business associate and third-party vendor contracts in the next two years to reflect HIPAA rules?

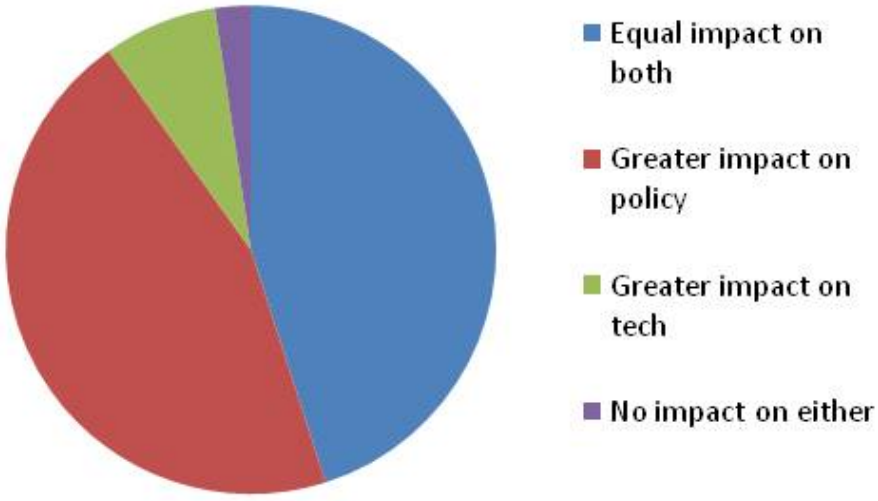


HIPAA legislation applies to those organizations defined as covered entities -- generally, hospitals, doctor's offices or health insurers. The HITECH Act makes HIPAA data breach notification laws apply to business associates as well. Under HIPAA rules, this term referred to a health plan, clearinghouse or other group otherwise involved in the disclosure of personal health information (PHI). The HITECH Act deems subcontractors, health information exchanges, regional health information organizations and e-prescribing gateways to be business associates as well.

Despite these changes, respondents believe they are prepared to meet expectations. While 33% of professionals said they are planning to update business associate agreements to reflect new HIPAA mandates, 63% said their contracts are already aligned and they don't need to change them. Another 4% said they plan to update contracts later.

Most professionals are aware that HIPAA mandates impact both their policies and technology needs. While 45% said they view the mandates as having more of an impact on their policies, the same number of respondents said the laws affect both policy and technology equally. Only 8% said HIPAA mandates have a greater affect on technology, and 2% said they have no impact on either.

Do HIPAA mandates have greater impact on your security policies or tech purchases?



Achieving data loss prevention with encryption techniques

Encryption is the first line of defense for information that needs protection. Software vendors offer different flavors of data loss prevention (DLP) utilities, from network-based gateway systems to host systems that can monitor data traffic inside a network, as well as external communications.

Through analysis engines that look for keywords and other identifying markers, DLP software detects sensitive data -- in motion, at rest or in use -- and the encryption software shields it from unauthorized access. It can also stop disgruntled -- or opportunistic -- employees from transmitting PHI past the firewall, and notify IT staff about such attempts.

Kinder, gentler variations on that theme involve DLP software that queries employees about transmissions that run contrary to company rules. For example, a pop-up window might ask, "Hey, you're about to copy a patient record to a thumb drive; are you sure you want to do this?" and in some cases might require the employee to type in an explanation before the data transmission is allowed. While it might not stop data loss outright, such software can keep honest employees from committing innocent mistakes and refer them to the data protection policy explaining the problems with it.

Don't think of encryption just for data connected to the network. Consider it for backup tapes too. According to Michael Passe, a storage architect at Beth Israel Deaconess Medical Center in Boston, device-level encryption for tape backups is a lot easier to manage than the file-level alternative, which is complicated by key management.

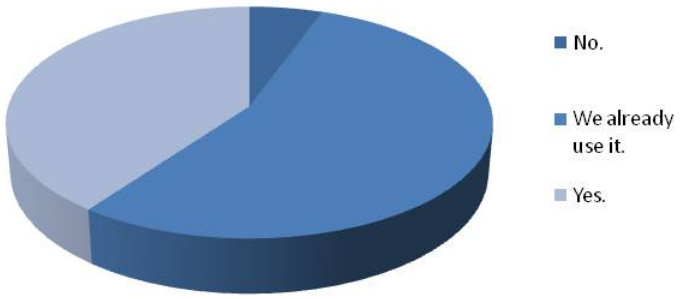
Get the briefing:
How to avoid a health care data breach

At their core, the HIPAA mandates aim to strengthen patients' consent over the use and disclosure of their personal health information (PHI). Providers are concerned that these myriad regulations will be confusing to implement, but they agree that better protections for patients are needed as the industry moves toward adopting more health IT.

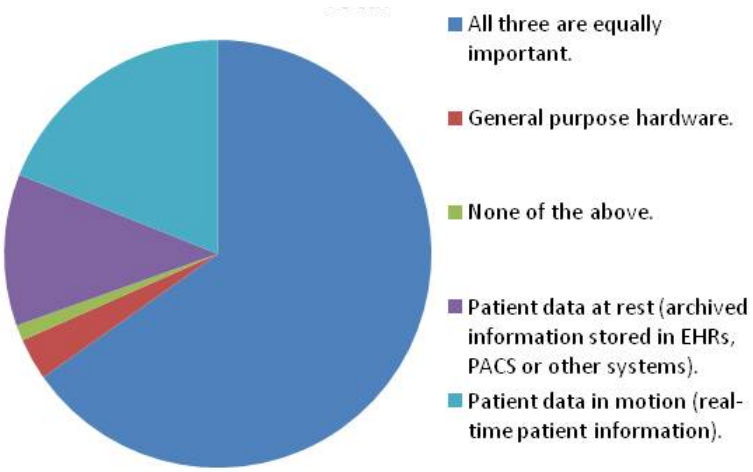
Respondents agreed that the rules naming encryption as the best line of defense against data breaches make them more likely to use the technology. Some 40% of those surveyed said it is exploring encryption while 54% said they're already using it.

Data of all sorts is important to encrypt, as well. Most respondents, 65%, said general hardware along with patient data both at rest and in motion are equally important to protect. Another 19% of respondents said data in motion across real-time systems was the most important to encrypt while 11% said data at rest, or stored in electronic health records and other systems, is most important.

HIPAA officials have said that when encrypted patient data is lost, it doesn't count as a data breach and therefore is not a violation. Will this make your organization more likely to explore encryption software for patient data?

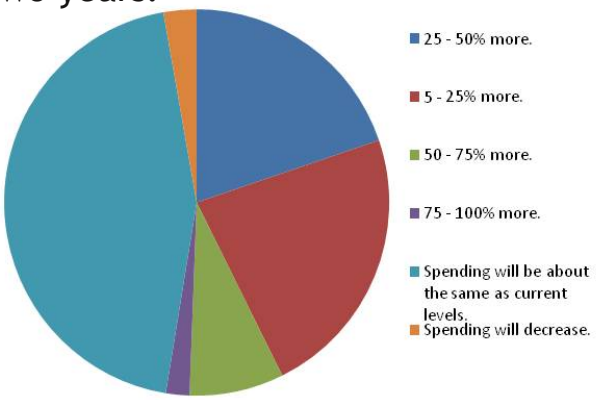


What is most important for you to encrypt?



SearchHealthIT.com

Are you planning to spend more or less on clinical data encryption in the next two years?

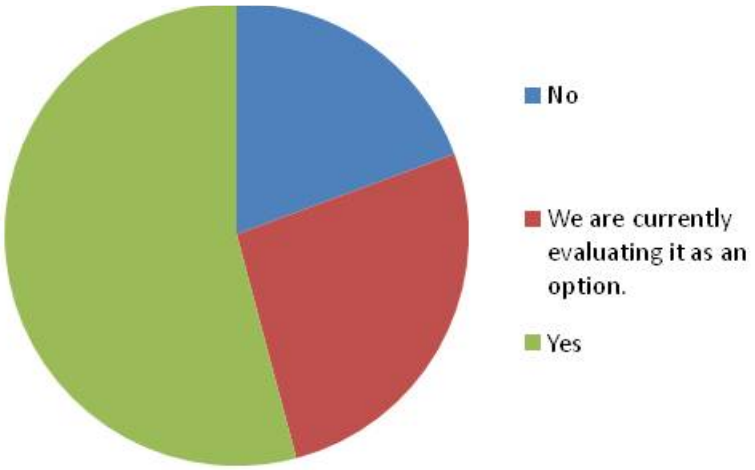


As encryption gains in importance -- especially in clinical settings, where the use of electronic systems is on the rise -- organizations are beginning to spend more to purchase the technology.

About 45% of respondents said their spending levels would remain the same, but around the same number said they would be increasing spending 5% to 25% or 25% to 50%. An additional 8% of respondents said their spending would go up 50% to 75%.

SPOTLIGHT: SSO

Does single sign-on play a significant role in your user authentication practices?



Single sign-on (SSO) technology is emerging as a popular choice for the health care industry. The Ponemon Institute, in a recent survey *How Single Sign-On is Changing Healthcare*, found that clinicians liked the automated login process -- after entering one password, they had access to all their applications, reducing time spent remember logins for several systems, keystrokes and clickthroughs. Of the research institute's respondents, 80% said they'd recommend adopting the technology.

More than half of *SearchHealthIT.com's* respondents said they are currently using SSO while another 26% said they are evaluating it as an option. Only 19% said they aren't using it or considering it.

Parkview Adventist Medical Center, a 55-bed acute care hospital with six affiliated physician practices in Maine, has been recognized for delivering high-quality care while meeting IT efficiencies. This has helped Parkview achieve HIMSS Analytics Stage 6 adoption status for EMR systems. Bill McQuaid, assistant vice president and CIO, explains how and why:

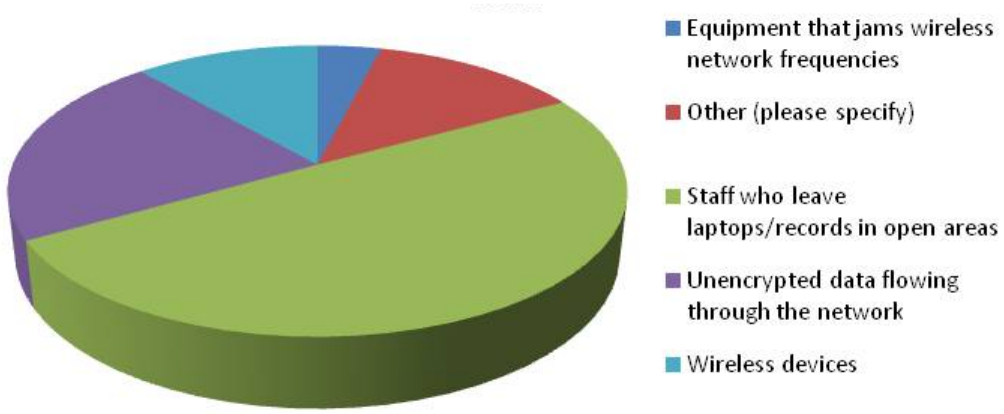
To ensure success, we incorporated a system with strong authentication and single sign-on (SSO) that would integrate with our EMR systems and consequently improve user workflows and speed access to patient data. Only then would we realize the full benefits that using EMR systems can bring in terms of making essential data -- demographics, problem lists, medication lists, diagnostic results and so on -- available in an organized, updated format to any care provider within the hospital system.

Now our team has secure and convenient access to a full set of departmental clinical applications, advanced clinical applications, and the full suite of financial and administrative applications. Clinicians can access records by using finger biometric readers placed on stationary PCs or computers on wheels throughout the hospital and in their practices.

By embracing strong authentication and SSO as critical components of our EMR systems, we have avoided potential roadblocks. Caregivers are delighted with the new system and with the fact that they have access to all electronic patient data from any location with just a swipe of a finger. At the same time, when a doctor or nurse steps away from the screen, it is automatically wiped clean after three seconds, a feature that helps ensure compliance with HIPAA privacy mandates. This implementation has saved the hospital money, improved productivity and increased security.

What is the weakest link in your hospital's security?

Despite IT adoption, it's the low-tech actions of people that are still causing security concerns, according to readers. Half of respondents said staff leaving laptops or medical records in open areas is the weakest link. This claim matches what the OCR has found in significant data breaches among health care organizations. Unencrypted data is another security concern, according to 22%.



While wireless devices and equipment that jams network frequencies are problems, say 11% and 4% of respondents, respectively, another 13% named different security concerns. Those included: staff who didn't follow policies; older, cumbersome network securities; personal devices that are not part of the network; and difficulty in tracking the myriad ways in which data can leave the hospital.

Conclusion

With the health care industry beginning to focus on adopting more technology, using electronic health records, and meeting meaningful use requirements along with a slew of other federal IT initiatives, data protection takes on a greater role.

Providers are aware of how policies impact their technology needs and are making choices based on clinical data considerations, encryption methods, and the growth of mobile devices in physician practices and at other points of care.

Calls for more security are not championed by one group or another, either: Everyone is getting into the game. From nurses and physicians to IT managers and CIOs, various employees are on board with using more technology and determining how best to protect the information flowing through those systems.

While it's clear that the industry still might have some confusion about what needs to be protected and how best to do it, security isn't going away. Data breaches are on the rise and the type of data inside electronic medical systems could become more attractive to thieves, which leads to damage for both patients and the provider. Protection requires vigilance.

EDITORIAL STAFF

Jean DerGurahian
Executive Editor

Don Fluckinger
FeaturesWriter

Brian Eastwood
Site Editor

Anne Steciw
Associate Editor

Jenny Laurello
HIT Community Manager

Craig Byer
Assistant Site Edior

FOR SALES INQUIRIES

Stephanie Corby
Associate Publisher
scorby@techtarget.com
(617) 431-9354

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

SearchHealthIT.com