HEALTH IT GETS DEFENSIVE

Mobile devices and imaging systems are two concerns for providers trying to maintain healthcare cybersecurity. Find out what they’re doing to stay ahead of data breaches and other threats.

03 Digital Health Images Complicate System Security

07 Cybersecurity Urgent in the Wake of Past Breaches

11 Wearables Hold Promise for Those Who Can Afford Them

15 Healthcare Cybersecurity Expands to Cloud
When I think of healthcare information security for endpoints in hospitals, my mind usually wanders to my own technological setup at home. I’ve got a work laptop, personal laptop, TV streaming stick, smartphone and DVD player all connected to my wireless network. Sometimes visitors hook their phones into the wireless router, too.

It certainly wouldn’t take much for, say, my kid to fool around with my streaming stick and download an HDTV app I didn’t want him watching. That’s an endpoint breach no parent wants to deal with.

It’s also a breach that could happen with me managing only five access points at home. Multiply that by tens of thousands of devices and you get an idea of the mountain that IT pros have to climb to ensure healthcare information security.

In our Pulse cover story, contributor Nicole Lewis talks to a pair of health system administrators about their approaches to endpoint security and how living under the shadow of potential HIPAA violations has the attention of health IT executives.

On a related note, Shaun Sutner looks into security for imaging systems. The abundance of digitized images has increased worries about the security of protected health information contained in those pictures.

Changing gears, Pulse explores how wearable health devices are out of reach for some people who need them the most. For example, diabetes is a widespread disease in the U.S. whose sufferers can benefit from reminders from wearables, yet many patients can’t afford or don’t see the value in owning the gadget, Kristen Lee reports.

Clearly, the ramifications are much higher for diseased patients compared to me and my entertainment options at home. If I don’t add a digital video recorder to my wireless network, I won’t truly suffer for it. But if someone has diabetes and can’t be reminded about blood sugar levels, the situation goes beyond convenience.

Wearables will add a whole new level of healthcare. I’m not sure if each device will serve as an access point into an EHR, but regardless, those devices will push more outside information into clinical systems. For healthcare IT executives, the onslaught continues.

How are you reviewing the security of new endpoints? Let me know by email at swallask@techtarget.com or let me know on Twitter @Scott_HighTech.
Digital Health Images Complicate System Security

Now that vendor neutral archives and PACS are widely installed in big healthcare providers’ data networks, experts say providers of all sizes should look to bolster the cybersecurity of their medical imaging systems.

The proliferation in recent years of digitized healthcare images such as CT scans, MRIs, cardiology videos and ultrasounds has increased anxiety about the privacy, security and integrity of those pictures, which often contain as much sensitive PHI (protected health information) as EHR records and can be used for Medicare fraud, identity theft and other criminal purposes.

“We want to utilize this information and not have it exposed,” said Andy Riley, chief technology officer of data security consulting firm GB-protect Inc., which works with many healthcare industry clients.

Image Sharing Danger
More likely than outside hacker attacks and thefts, security vulnerabilities can arise when physicians and others share images extracted from vendor neutral archives (VNAs) and picture archiving and communication systems (PACS), two systems which are generally secure, Riley said.

That is because when users modify reports or metadata that accompany the images for their specific specialty or purpose, “you magnify the number of locations and the risk,” Riley said.

Scott Erven, associate director, health IT security practice for Protiviti Inc., said many medical imaging systems such as PACS have “poor security hygiene” because their default administrative architecture often isn’t updated for PHI security.

Medical Device Vulnerabilities
As for medical devices connected to integrated delivery networks and hospital computer networks—including image-producing hardware such as MRI machines—they can pose both cybersecurity and patient safety concerns, Erven said.

“Many devices have poor security controls,” he said.

However, Erven noted, radiology machines are usually operated by technicians who need to hit a button to initialize the machine, making it difficult for an outside actor to control it.
Meanwhile, other connected devices, such as bedside infusion pumps, have been shown to be vulnerable to hacks that could harm patients by delivering lethal amounts of medication. Such attacks could also lead to unauthorized entry into larger health system data networks.

Erven noted that many people who are concerned about medical device security were encouraged by the FDA’s recent publication of draft guidance for the cybersecurity of connected devices that are already on the market.

The post-market guidance calls on medical device vendors and users to more vigilantly monitor devices for security holes and to share information about known threats.

**PHI Cybersecurity Tips**

Erven, a frequent speaker on medical device cybersecurity, offers these tips to providers looking to better protect their medical imaging systems and improve cybersecurity in the healthcare industry:

- When looking to contract with vendors, make sure vendors have validated security controls for their devices before they are introduced into clinical settings.

- Ensure that devices’ firmware and software are continuously updated.

- When turning in older equipment for resale, be sure to destroy any legacy data that resides on devices.

  “You can buy stuff off eBay that still have PHI on them,” Erven said.

  As for encryption, Erven recommends using known good cryptography that protects data both in transit and at rest. “I’d highly advise organizations not to build their own.”

  “Don’t roll your own crypto,” he said.

**To Cloud or Not**

Health IT and imaging communities are still debating cybersecurity issues associated with cloud-based medical imaging systems, including hybrid cloud-enterprise arrangements.

While experts agree that the financial imperatives of cloud technology’s economies of scale are impossible to ignore and probably inevitable, they say many large provider systems remain wary of the cloud, especially public clouds.

  “The pure public, Internet-facing cloud is definitely risky,” Erven said.

  On the other hand, for smaller providers, hosted environments provided by reputable cloud storage vendors...
“can be safer than organizations that lack the resources” to store and protect their own digital medical images, Erven said.

For Riley, the cloud question for large healthcare providers is less focused on security per se; it’s more tied to a feeling of losing control of what they consider proprietary images and the integrity of those images.

“You sort of conjure up that you don’t have control and that conjures up security issues,” he said.

Indeed, Riley noted that many larger health systems are already seeing unauthorized use of the cloud by physicians employing public, consumer-oriented cloud products such as Dropbox and Box to easily get access to images, with security an afterthought.

“Doctors say ‘I want to be able to access this,’ ” agreed Cameron Camp, a security researcher for cybersecurity firm ESET North America. “Everything takes a back seat to availability.”

**More Imaging Cybersecurity Tips**

The following are Riley’s key tips for mitigating threats to medical imaging ecosystems:

- Clearly define the authorized use cases and data flows for medical imaging.

- Ensure that authorized use cases have a secure mechanism for moving data and storing extracted data.

- Use data discovery tools to identify image files stored in unauthorized locations.

- Use data loss prevention tools to quarantine and alert on imaging file extensions.

- Conduct user entitlement reviews and game-plan for how user roles could be abused.

- Monitor user access to sensitive information and put alarms on suspicious activity.

- Restrict large files leaving the network outside of authorized and expected data flows.

For Camp, security weaknesses reside not so much in imaging cameras, sensors and other hardware, but in how the data they produce gets packaged. For a criminal, state actor or insider “snooper,” it’s “how can I break into the containers and do something with it,” Camp said.

He said the best way for providers to protect the sanctity of their data—whether it’s images, text or other metadata—is to hire “white hat” hackers.

“I’d be open to third-party penetration testers,” he said. “If you get diagnosed, you have a chance of fixing the problem. Right now, they don’t know what their true state is from the attackers’ perspective.”

—SHAUN SUTNER
Information Exchange

The Health Insurance Portability and Accountability Act, better known as HIPAA, requires healthcare covered entities and their business associates to secure patients’ PHI. SearchHealthIT's reporters asked some security experts how their organizations and clients attempt to achieve this complex goal and received a variety of answers that mentioned authentication, encryption and containerization as steps in the ongoing security process.

“We’re rolling out an app called Duo. The nice thing about Duo is you can push an alert to your phone and you can just approve it without having to type in the entire code once your phone is actually registered to your account with the system.”

— ALLEN HSIAO, M.D., chief medical information officer at the Yale School of Medicine and Yale-New Haven Health

“It’s fairly common to use two-factor authentication. ‘Tap and go’ in mobile applications is very popular and provides security and blends it with ease of use.”

— SCOTT ERVEN, associate director, Protiviti Inc.

“We use Good Technology’s Good for Enterprise. It is a container application that has a self-contained email client, a self-contained calendar client and the Apple Watch component [is] associated with it as well. We use Kanguru Defender Elite for the USB drives [and] Symantec for disk encryption.”

— DAVID REIS, vice president of information services and CISO at Lahey Hospital & Medical Center in Burlington, Mass.

“Encryption is an evolving area [and some clients are using encryption to protect PHI]. But with encryption, even the largest providers have sort of kicked that can down the road.”

— ANDY RILEY, chief technology officer, GBprotect Inc.
Health IT security executives have a battle on their hands. The rapid adoption of electronic health records (EHRs) and the widespread use of mobile devices among providers has increased the endpoint security threat—and there are more vulnerabilities ahead. Now, a new surge of networked medical devices and wearable gadgets present possibilities for exposure to serious security breaches in healthcare, and many hospitals are unprepared to tackle the next endpoint challenge.

In recent years, the U.S. Department of Health and Human Services’ Office for Civil Rights has severely punished healthcare entities that have been lax at securing patient data and violated HIPAA privacy and security rules. These healthcare data breaches, involving endpoints like PCs, laptops and other devices, highlight the challenges of keeping patient data safe.

For example, in August 2015, Cancer Care Group, P.C., based in Indianapolis, agreed to pay $750,000 to settle potential HIPAA violations that occurred three years earlier when someone stole a laptop bag from an employee’s car. The bag contained the employee’s computer, which held unencrypted backup media containing the names, addresses, dates of birth, Social Security numbers, insurance information and clinical data of approximately 55,000 current and former Cancer Care patients.

Another incident in July 2015 highlighted security lapses at St. Elizabeth’s Medical Center in Boston, which agreed to pay $218,400 to settle potential HIPAA violations that occurred in 2012 when workers used a Web-based document sharing application to store files containing the electronic protected health information (PHI) of at least 498 individuals. A separate breach revealed that unsecured PHI was stored on a former employee’s personal laptop and USB flash drive, affecting 595 individuals.

Such security breaches in healthcare—along with research from companies like telecommunications vendor Alcatel-Lucent, now part of Nokia, which reported that 16 million mobile devices worldwide were infected by malware in 2014—have prompted health IT executives to take notice.

Broader Risk Now From Data Breaches

Because health workers can access patient data anytime and anywhere, vulnerabilities have increased and PHI is
no longer managed within the four walls of a healthcare facility, said Sriram Bharadwaj, director of information services at University of California (UC) Irvine Health in Orange, Calif.

“In the old days, you accessed electronic health records from a PC at your desk. There were a very small number of laptops, and login onto the system was controlled,” Bharadwaj said. “Today, that same information is available in a broader, less controlled way, and multiple devices can be used to access the same data because all of these applications are now mobile compatible.”

The IS office at UC Irvine Health—which operates a cancer center, adult and pediatric trauma center, and a stroke and cerebrovascular center—currently manages more than 1,000 devices. These tablets, laptops and other devices are used not only by physicians, nurses and other employees, but also by medical students in residency programs.

Given the frequent rotation of people logging onto the network and the tendency to bring their own devices to work, which increases the risk of a healthcare data breach, developing the right BYOD strategy is critical, Bharadwaj said.

To better secure its network, the medical facility developed what Bharadwaj said is the first-of-its-kind solution at a health system by creating middleware that links facilities’ mobile device management software with a network access control application. When users bring their own devices and attempt to connect onto the network, they must receive service activation from both the software and network access app before they can gain access to the hospital system’s network.

“All devices issued by us to our staff are encrypted,” Bharadwaj said. “We have a BYOD policy for those mobile devices that we don’t own, and they have to be authenticated in our environment. These outside devices have to use our recommended software and abide by our policies, but our first preference is that staffs use our own equipment.”

Among the technologies and techniques that UC Irvine Health has deployed to strengthen its endpoint security defenses include the following:

- Full disk encryption
- Antivirus software
- Workstation timeouts
- Multifactor authentication
- Single sign-on
- Data loss prevention technology
- Security information and event management
- Firewalls

**Hard Stance on Growing Mobile Presence**

Another hospital intent on bolstering its endpoint security management plan is Intermountain Healthcare, a health system based in Salt Lake City that operates 22 hospitals and a broad range of clinics and services. It has approximately 1,400 primary care and secondary care physicians working at more than 185 clinics in the Intermountain Medical Group.

Karl West, Intermountain Healthcare’s chief information security officer, said the acceleration of attacks on health data is unprecedented. He noted that based on the findings of an assessment conducted by an external auditor measuring maturity and compliance, Intermountain Healthcare’s security posture and commitment has increased 35%.
General pain points for PHI security include the following, as noted by West:

- The shift from device identification and protection to data identification and protection
- The cost to shift an entire industry’s “lagging” security posture
- The amount of time required to develop a data dictionary—in other words, an inventory of all data
- Staying ahead of the bad guys, who have high financial motivation to steal healthcare records

Securing endpoints has come with its own set of challenges at Intermountain. The system has 50,000 PCs and up to 5,000 smartphones, and by the end of 2016, West estimated 20,000 tablets will be in use. To fend off security breaches in healthcare from endpoint intrusion and theft of mobile devices, West said the system’s policy is to encrypt 100% of data flowing from laptops, mobile devices, storage and servers.

“Disposal of these devices requires a secure wipe and records validating the device are data free. Asset management policy directs procedures from procurement to disposition. We also control and monitor all ports and the exfiltration of data,” West said.

He also added that beyond the normal usage and movement of devices between departments, workstation categorization polices exist to control the data movement and migration across the enterprise.

But while there is confidence in Intermountain’s security strategy, there is also concern that a large breach could occur in any number of ways, including via malware, phishing, privileged account compromise or insider attack.

There are other, related concerns. Under the stage 3 meaningful use rules, which go into effect in 2017, hospitals must share patient data electronically, such as via email. Intermountain has a secure, encrypted patient portal to meet this requirement. “However, if a patient requests delivery to their personal email, we worry about the risk of their choice … and our liability if the patient account is phished,” West said.

**Connected Medical Device Risks Creep In**

And then there are medical devices and wearables, which boost the risk of security breaches in healthcare. Many industry IT executives are still in the beginning stages of grappling with how they’ll approach securing their enterprise as more connected medical devices begin feeding clinical data into EHRs and other clinical systems.

Intermountain Healthcare is making what West described as “a significant effort” to integrate and secure medical devices that are brought onto the network.
“We have created an inventory of medical devices, established risk based on data capabilities and are beginning to deploy common controls based on risk and features available,” he said.

Certain medical devices—such as pacemakers, insulin pumps, MRI and CT scanners and bedside patient monitoring systems—are deeply integrated into clinical workflows, delivering data to clinical systems like EHRs, said Lynne Dunbrack, research vice president at IDC Health Insights in Framingham, Mass. The worry, she said comes from the possibility of malware being introduced via a compromised medical device to the network.

“There is a concern that these medical devices, which typically are not all that well secured, become a back door for hackers to get into these devices and start infiltrating the network,” Dunbrack said.

Developing a sound medical device security strategy is a nascent phenomenon at healthcare facilities. According to IDC Health Insights’ 2014 Cross Industry Cyber Threat Survey, which polled 94 health IT executives, only 9.6% reported that medical device security is integrated into the enterprise security infrastructure. One in 10 respondents said they haven’t begun to assess the potential security threats to networked medical devices.

Back at UC Irvine Health, the number of endpoints is expanding as medical devices are being integrated onto networks and data from medical equipment is sent to EHRs.

“We manage those medical devices through our network, which has the necessary security software to manage the data in transit and at rest,” Bharadwaj said.

The thought that another class of devices—wearables—will one day permeate healthcare networks and connect to EHRs and other clinical systems means there will be more security challenges, but UC Irvine Health’s IT team hasn’t begun to take on that challenge.

“The increasing use of wearables to collect patient data creates a different level of complexity in managing endpoint security.”

—SRIRAM BHARADWAJ, director of information services at University of California (UC) Irvine Health

“We have seen the proliferation of Fitbits and other wearables, but we do not yet integrate that information into our medical records,” Bharadwaj said.

Looking ahead, he predicted that wearables will become the standard in providing patient data and will ultimately present new security challenges for hospitals and wearable device manufacturers.

“The increasing use of wearables to collect patient data creates a different level of complexity in managing endpoint security, especially if the device manufacturers don’t adhere to the standards that are adopted across the industry to help healthcare entities bring that data into the healthcare environment,” Bharadwaj said. —NICOLE LEWIS

—NICOLE LEWIS
Wearables Hold Promise for Those Who Can Afford Them

BY KRISTEN LEE

WEARABLE TECHNOLOGY in healthcare is a hot topic right now, and the benefits of wearables in terms of helping people improve their health are undeniable.

“Wearables can help by keeping both parties [doctors and patients] engaged, by preventing readmission [and] by preventing chronic conditions from reoccurring,” said David Chou, former CIO at the University of Mississippi Medical Center in Jackson, Miss.

One example is chronic conditions such as diabetes, which the International Diabetes Federation estimates will affect one in 10 adults by 2030.

Unfortunately, the populations that tend to struggle with chronic diseases such as diabetes and could benefit from the use of wearables are the people who can’t afford them. According to the World Health Organization, more than 80% of diabetes deaths occur in low and middle-income countries.

In addition, a 2014 Centers for Disease Control and Prevention study shows there is an obesity disparity among varying racial groups in the U.S., with the highest rates of obesity in the South. The most cases were found in African-Americans, followed by Hispanics. Further, it is well-known that obesity often leads to other significant problems including diabetes, heart disease and cancer.

“Wearables are still in a range that’s out of reach for many consumers,” Iana Simeonov, principal investigator and project director at the Public Health Institute in Oakland, Calif., said.

And Lisa Gualtieri, assistant professor of public health and community medicine at Tufts University and founder of RecycleHealth, a nonprofit, agrees: “I think that the cost is a real barrier for a lot of people.”

But it isn’t the only reason wearable technology in healthcare remains out of reach for the people from these populations—the people who could really benefit from these devices. It’s much more complex than that.

The Financial Factor

Some wearables have a price tag of hundreds or even thousands of dollars—think the rose gold Apple Watch—while others cost around $20, which may not seem like a lot of money to some people.

Gualtieri explained that if people don’t see the value in wearables, they won’t invest in them, even if they only cost $20.
“If you knew that your $99 was going to be well spent, maybe you would go out and make that decision,” she said. “But I think for a lot of people, it’s something that’s really on the periphery.”

That is especially true if someone has to decide whether they should spend that money on groceries or a wearable and they don’t fully understand how a wearable could help them improve their health long term. If that’s the case, chances are that person is not going to spend their money on a wearable.

Not Much Marketing to Low-Income Populations
Furthermore, this population isn’t often targeted or marketed to by wearable device companies.

“I don’t know if anybody goes into business in wearables thinking that this is an obvious market. People that are at risk and underserved are that way because there isn’t a lot of attention being paid to them,” Simeonov said. “You don’t necessarily look at consumers who you think don’t have a lot of money as an obvious market for you. You go after … more people that want your product rather than need it.”

Simeonov added that companies may enter a space to solve a problem, but they are also looking to make money and stay in business. That means they must target and cater to the people who are going to buy their product.

“You can’t fault them for that,” Simeonov said. “Every business has to start somewhere.”

SearchHealthIT tried to contact Fitbit and Withings for a comment but they could not be reached.

Unfortunately, this is part of what causes people of lower-income populations who may have a chronic disease to be left in the dark on how wearables can benefit them and help them get healthier.

Understanding Data From Wearables
On top of all that, the data wearables collect and present back to the user can be difficult to understand.

“The data has to become much more accessible. And by accessible I mean it has to be more easily understood,” Simeonov said. “Right now, you can compare it to getting a printout of your lab tests in the mail … and as an uneducated consumer, those results can be impossible to interpret. What you see there and what a trained physician see[s] there are completely different.”

Simeonov added that the average healthcare literacy in the United States is at a fourth-grade reading level. The companies making and designing these wearables aren’t trying to confuse users—in fact, their goal is to present complex data in a way that the user will understand.
“[But] it can still be really difficult for somebody ... to take a look at that data and understand how that applies to them and make decisions about their health based on that data,” Simeonov said.

“This is especially true for the populations that could benefit from wearables the most.

“The people who’d benefit most from tech have lower health literacy,” said Ahmed Albaiti, founder and CEO of Medullan Inc., a digital health consultancy headquartered in Cambridge, Mass. “They have chronic conditions that they’re dealing with; they are in an age group that [makes it] difficult to pick up new technology and so on. I don’t think the current crop of wearables [has] the kind of utility where they would pick it up.”

**Where To Go From Here**

Historically, the price of technologies has almost always gone down and the same will be true for wearables, Chou, Simeonov and Albaiti all agree. And, ultimately, it will make wearable devices much more affordable.

Regardless, understanding the data remains an issue, Simeonov said. Although wearable devices may become more affordable as time goes on, “unless the nature of the information changes, I don’t believe they’re going to do any good in the present form,” she said. “They’re just too complicated.”

However, Simeonov believes that a lot of thought is being put into how the data is being presented when it comes to wearables right now “because nobody wants to confuse their audience,” she explained. “The current crop of wearables has really ... tried to have unique data visualization tools and unique algorithms, and this is something they’ve spent a lot of time and money doing.”

Wearable developers have also spent a lot of time trying to understand their customer, Simeonov said.

“We now have to spend the same amount of time and the same amount of thought into understanding other segments of the market,” she said. “Perhaps [wearable device companies] have and ... it’s not viable. I don’t know.”

In Gualtieri’s opinion, integrating wearables into the more formal healthcare system and process would help a great deal.

“What if the doctor was able to give someone a device and to say, ‘Let’s see what your baseline activity level is on average for the next week and let’s work on increasing it to 100 steps a week,’” Gualtieri said. “[It’s] really trying to meet people where they are and then [creating] small doable increments.”

Integrating wearables into the normal healthcare process would not only help engage patients in their own health but would also help them better understand their baseline health. However, Gualtieri said she suspects wearables have not yet been fully integrated into the formal healthcare system because of cost.

Although this may not be happening now, Chou predicts that wearables will ultimately become a part of the

“**The people who’d benefit most from tech have lower health literacy.**”

—AHMED ALBAITI, founder and CEO of Medullan Inc.
healthcare strategy.

“Whether you’re an insurance carrier or a health system, [wearables] should be part of your strategy as far as providing that to the patient you want to target,” Chou said. “Giving them a few hundred dollars’ worth of devices in terms of wearables, it may save you thousands in the long run.”

Chou believes healthcare organizations are beginning to think this way, although there is resistance to fully integrating wearables into the healthcare cycle because it means extra work will be put on the providers.

“There’s extra work on somebody to stay engaged with you [the provider],” Chou said. “By having a wearable device, constant communication and constant feedback will always be expected.”

Despite all the obstacles in the way of wearables becoming part of the healthcare system and reaching the populations that could most benefit from them, Chou still believes that “wearables will be part of our lives.”

He believes this because healthcare is moving away from fee-for-service payment models toward value-based care. “Wearables can be a part of that solution,” Chou said. “The challenge is most organizations are still in the fee-for-service reimbursement model. So until we get at least 80% of our reimbursement from value-based care, then it is going to be hard to entice folks to start thinking outside the box.”

Simeonov added: “My own research has shown that [lower-income people who could benefit from wearables] are highly sophisticated users of technology and that there is a real opportunity for using technology to at least increase their access to health information and then potentially deliver care.” —KRISTEN LEE
Techinically Speaking

GET READY

Healthcare Cybersecurity Expands to Cloud

The regular addition of cloud technology services has analysts concerned that health IT departments are being overwhelmed by the speed of these changes and don’t possess adequate resources to be sure their cloud-based workloads comply with HIPAA standards. The adoption of cloud in healthcare has been steadily increasing for some time now. Hospitals, health plan providers and physician groups rely on these services to help reduce some of their infrastructure complexities and reduce costs.

Considering the amount of available cloud services and the number of healthcare entities that are using them, it’s easy to deduce that a large quantity of patients’ PHI (protected health information) resides in the cloud, permanently or temporarily. As providers increase their dependence on cloud and online services, health IT executives face the pressure of constantly certifying that all of their cloud services meet HIPAA standards.

There are two distinct types of services that IT generally deals with when working with cloud providers, and each one deals with HIPAA standards very differently.

Vendors that offer online managed cloud services, such as software as a service, are fully responsible for meeting HIPAA requirements. In these cases, the vendors themselves are 100% responsible for data protection, disaster recovery planning, systems redundancy and all general security practices that are mandated by HIPAA.

Unmanaged cloud services are those that a cloud provider offers their clients that leave the client somewhat responsible for some of the data protection. In this type of service—which can include infrastructure as a service or storage as a service—the vendors are required to cover a baseline of HIPAA security requirements, but their clients must also take full responsibility for satisfying the remainder of HIPAA.

Cloud services offered today by Amazon, Google, Microsoft and several others in the marketplace continue to see an increase in their client bases. Many providers offer tools to help their healthcare clients meet HIPAA standards. There are a few crucial questions that healthcare providers should address to be certain their cloud products are compliant with HIPAA.

- **What systems must meet HIPAA requirements?**

As part of the overall review of systems, a healthcare entity must first identify all systems that interact with PHI. Doing this determines which systems should be evaluated
to establish conformity with HIPAA privacy and security regulations.

**Who is responsible for HIPAA compliance?**

It is common practice for healthcare organizations’ technology vendors that work closely with patient data sign business associate agreements (BAAs). Despite the existence of BAAs, not all cloud providers are responsible for all aspects of HIPAA. So it becomes extremely important for the IT department to understand where its responsibilities begin and end when it comes to systems managed in the cloud.

**Should you rely on cloud security tools?**

The systems that reside in the cloud such as servers and applications are subject to the same risks as any other system. Cloud providers offer and deploy highly sophisticated security systems to ensure core systems are protected from cyberattacks and data breaches. Systems and servers hosted internally by hospitals aren’t protected by cloud providers and are vulnerable to hacks. A health IT department must evaluate security platforms for their server workloads in the cloud in the same way they would for their internal server infrastructure.

**Does the cloud still need to be audited?**

The cloud services offered today are easy to implement, manage and operate, but working with vendors to gather information about how their products meet HIPAA protocols can be difficult. An IT team must be diligent in documenting as much relevant information as possible so they have something to present to potential HIPAA auditors.

**Are the systems automatically backed up?**

The common answer to this question asked by IT departments to vendors is “maybe.” Though cloud vendors usually ensure system availability if any of their hardware fails within their data center, that doesn’t always mean that user data can be restored after it’s deleted. Cloud vendors offer backup and recovery services for their cloud, which means users of the service must plan for cloud backups the same way they do for their internal systems.

Security and the protection of systems is still one of the top priorities for IT executives. As more cloud services are adopted, IT departments are trying to quickly alter their security policies accordingly. Regardless of how popular a cloud vendor is, the services it offers to healthcare clients must still undergo the same review protocol that’s applied to in-house systems. This is especially important because HIPAA requires that all systems, no matter where they are hosted, must meet its standards.

—REDA CHOUFFANI
SCOTT WALLASK is news director at SearchHealthIT. Email him at swallask@techtarget.com and follow him on Twitter: @Scott_HighTech.

KRISTEN LEE is a news writer for SearchHealthIT. Email her at klee@techtarget.com and follow her on Twitter: @Kristen_Lee_34.

NICOLE LEWIS is a contributing writer for SearchHealthIT.

SHAUN SUTNER is news and features writer for SearchHealthIT. Email him at ssutner@techtarget.com and follow him on Twitter: @ssutner.

REDA CHOUFFANI is vice president of development at Biz Technology Solutions Inc. Follow him on Twitter: @healthcareITGuy.

Pulse is a SearchHealthIT.com e-publication.

Scott Wallask, Editorial Director

Shaun Sutner, News and Features Writer

Kristen Lee, News Writer

Nicole Lewis, Contributor

Alex DelVecchio, Site Editor

Linda Koury, Director of Online Design

Stephanie Corby, Publisher, scorby@techtarget.com

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

©2016 TechTarget Inc. No part of this publication may be transmitted or reproduced in any form or by any means without written permission from the publisher. TechTarget reprints are available through The YGS Group.

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 IMAGE: PONKRIT/ISTOCK