Physicians
& Cybersecurity Risk

A cybersecurity handbook for healthcare CEOs

AT&T Business

With threats and fines mounting, it is becoming increasingly critical to deploy technology and partner with key players.

Recent years have seen an uptick in cyberattacks, ranging from international interference with U.S. political institutions to spectacular large-scale consumer account hacks. The healthcare industry, meanwhile, proved that it remains extremely vulnerable. The health records of approximately 150 million Americans have been compromised since 2010.[1] In August of 2016 alone, the Office of Civil Rights reported, more than 8.7 million EHRs had been exposed to hackers or stolen.[2] That's no surprise: A healthcare record, rich with personal, medical and financial detail, may be 50 times more valuable to a cybercriminal than stolen credit card information.[3]

The threats are diversifying. In early 2016, foreshadowing a new approach to extortion through crypto-ransomware attacks, Hollywood Presbyterian Medical Center paid $17,000 in bitcoins[4] for a decryption key after hackers paralyzed its communications system. Later in the year, a health IT news organization described U.S. healthcare as "ground zero" in a global phishing campaign that deployed fake billing documents as Word attachments.[5] That same month, an Arizona physician became lead plaintiff in a class-action suit alleging that a health system's response to hacking of data involving as many as 3.7 million patients was inadequate.[6] Meanwhile, Advocate Health Care Network set a new record in HIPAA settlements: $5.55 million.[7] The vulnerability of network-connected medical devices was highlighted in October, when the St. Jude Medical company established an advisory board, including physicians, to address what it called "irresponsible" reports that its cardiac implants were easy targets for security breaches.[8]

No healthcare CEO wants to be associated with these sorts of stories. Yet many organizations are inadequately armed to stay out of the news. According to a 2016 HIMSS survey,[9] fewer than 60% of providers are using network monitoring tools or mobile device management—just two examples of technology that must be used to prevent breaches.

Healing healthcare's security ills requires leadership, funding, reorganization, board buy-in and deep changes to corporate culture. It requires the right mix of prevention and treatment technologies, from threat detection to email scanning to user behavior analytics to remediation strategies. Finally, it requires that hospital leaders recognize that the human factor—fundamental to healing patients—is critical to healthcare security. That, in turn, involves close partnering with physicians, who are uniquely powerful agents in the security universe.

1 JAMA, *Data Breaches of Protected Health Information in the United States*, April 2015; Forbes, *Data Breaches In Healthcare Totaled Over 112 Million Records In 2015*, December 31, 2015; U.S. Department of Health & Human Services, Office for Civil Rights Breach Portal, February, 2017.
2 U.S. Department of Health & Human Services, Office for Civil Rights Breach Portal, February, 2017
3 Medscape, *Stolen EHR Charts Sell for $50 Each on Black Market*, April 28, 2014
4 Hollywood Presbyterian Medical Center, *Letter from the President and CEO*, February 17, 2016
5 Healthcare IT News, *Massive Locky Ransomware Attacks Hit U.S. Hospitals*, August 19, 2016
6 Modern Healthcare, *Banner Health Cyberattack Draws Class-action Suit*, August 9, 2016
7 HHS.gov, *Advocate Health Care Settles Potential HIPAA Penalties for $5.55 million*, August 4, 2016
8 REUTERS, *Hired Experts Back Claims St. Jude Heart Devices Can Be Hacked*, October 24, 2016
9 HIMSS, 2016 HIMSS Cybersecurity Survey

What's Inside

The Unique Role of Doctors in Cybersecurity

In the course of a normal day, doctors move through nearly all of your hospital's critical-information systems—patient records, test results, surgical monitoring, and more. They bring phones and tablets and apps with them, and they work in a system in which the number of network-connected devices is exploding, often without proper security precautions in place.

"Healthcare seems to be one of the biggest adopters of cloud and mobility, in order to drive the efficiencies for care," says Bindu Sundaresan, Practice Lead for AT&T Security Consulting.

The technology boom meant that, according to one study, the number of medical devices in U.S. hospitals had increased 62% between 1995 and 2010, with many hospitals having 10 to 15 devices per bed.[10] By 2014, at least 1 in 4 were linked to the network,[11] feeding information to the EHR. The use of connected devices has accelerated since then, resulting in a security challenge on a scale that financial institutions, for example, simply don't face. The problem, Sundaresan says, is that underlying technology systems are often outdated. "Hackers know these are the people, this is the type of industry which has legacy systems."

On top of that, many doctors are not employees but business associates who connect their own often antiquated technologies and networks with hospitals' IT systems. The hospital network is vulnerable—and HIPAA-liable—to problems those weak links present. →

A Day in the Life of a Doctor

Spear phishing vulnerability

6:05 A.M.
At home, physician clicks on an email from IT asking him to verify his logon: "Routine hospital security exercise."

THREAT
The email wasn't from IT but from a hacker, who now has the password. Phishers can mimic in-house emails and tune attacks to physician's personal and professional life, including international research collaborations.

SOLUTION
Ongoing phishing training, including simulated campaigns. Use network to scan and quarantine email containing patient data going to another country for additional scrutiny. Implement threat detection and notification if a breach does occur.

10 GE Healthcare, *How Clinical Asset Proliferation and Low Utilization Are Draining Healthcare Budgets*, 2012
11 American Bar Association, Medical Device Security in a Connected World, 2014

For all those reasons, making doctors a productive part of your security solution requires not just a robust technology suite, but a rethinking of their relationship with your security apparatus. Given the right training, doctors can be a core component of your front-line cyber defense. Their reputations are tied up in the reputations of the hospitals in which they work.

"We now have a lot of physicians on staff who work with us and with their colleagues to get them to understand the need for this type of security," says Chris Van Gorder, President and CEO of Scripps Health in San Diego. "And doctors don't want to see the violations themselves. So I'm not getting the pushback that I used to get from them. In fact, I'm getting a lot of collaboration and support from them."

Working with physicians, however, inevitably reveals a Hippocratic complexity: A doctor's first duty is to patient outcomes. "Doctors are focused 100% on the health of the patient and getting to see more patients," says Terry Hect, Chief Security Strategist for AT&T Healthcare. "So any time they can skip a step to go faster, they will."

Bottom line: An effective audit of your security system must recognize the unique role of doctors before you can determine where quality of care and quality of security can best converge. ■

A Day in the Life of a Doctor

Failure to partition devices

1:30 P.M.
Physician accesses patient data using a personal tablet.

THREAT
Applications (work and personal) on the doctor's tablet could run in the background, deploying malware into the hospital's patient database, or just sniffing unencrypted data or passwords.

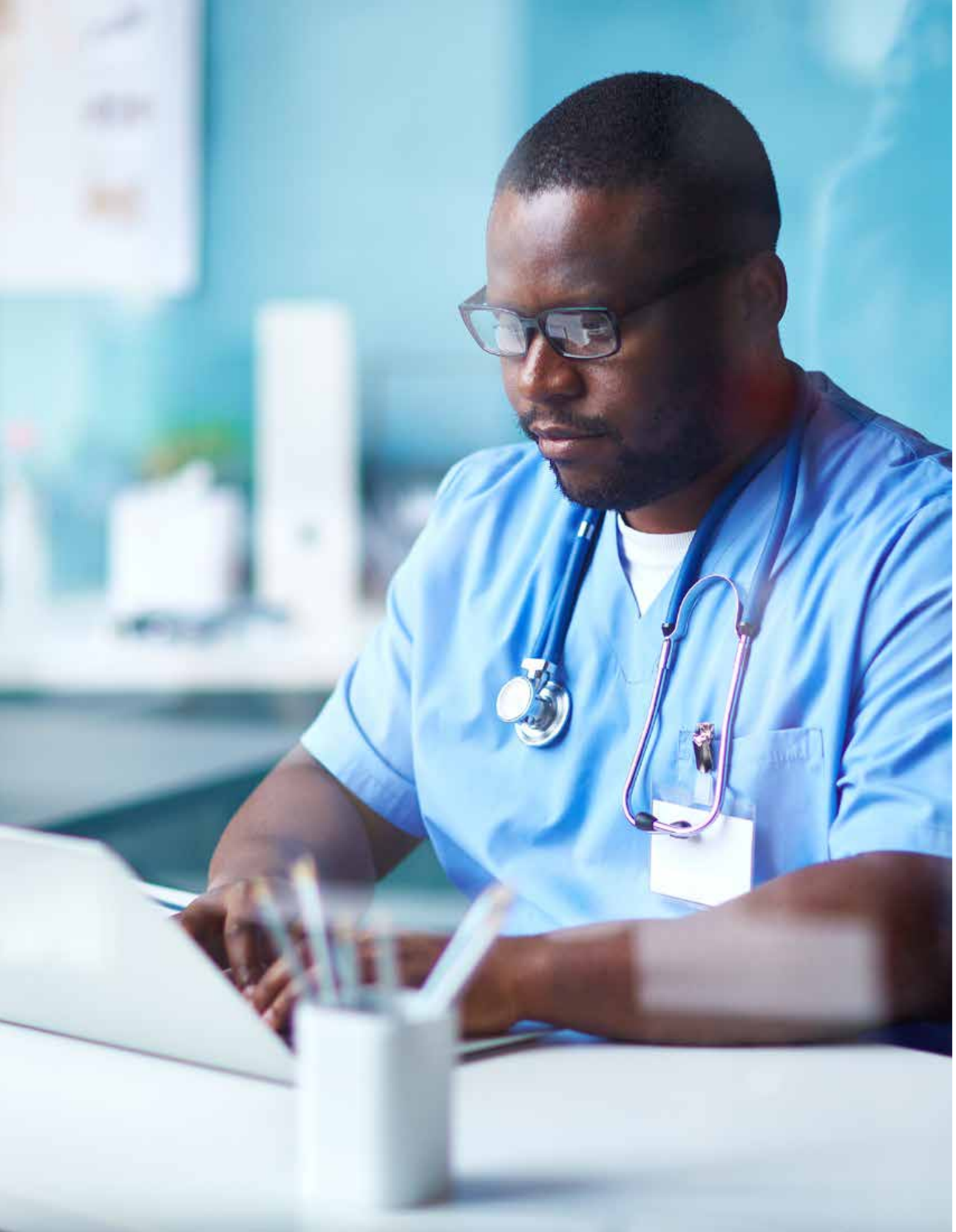
SOLUTION
Segregate the tablet into work and personal partitions. Ensure that the work partition includes two-factor authentication, remote wiping, and encryption of any stored data if the device is lost or stolen.

10 Best Practices

for End-to-End Healthcare Security

A strategy to improve security is only effective in the context of a robust, end-to-end approach that begins with an audit and ends with a holistic program that includes ongoing implementation, monitoring and response functions. This plan should function largely in the background, with two goals: Don't interrupt or compromise patient care, and don't allow the bypassing of protocols or mechanisms that are designed to eliminate vulnerabilities in networks and systems.

1. Conduct a holistic third-party audit. First understand the system you're protecting, and expose its vulnerabilities. This requires an independently drawn picture of your security state, including devices, permissions, network architecture and security practices. This is required for HIPAA compliance, but HIPAA compliance—designed to protect privacy—isn't enough.
2. Use your tools. As one CEO put it, hospitals are basically information systems. Every intelligent device will eventually become connected, so use your network and security tools (routers, switches, firewalls, anti-malware, etc.) to quickly identify attacks, control data flow, and mitigate and control disruptions.
3. Protect your endpoints. From phones to laptops to desktops to connected medical devices, everything must be included in a defense plan.
4. Structure and segregate your data access. Implement robust encryption and authentication technology and protocols, and isolate medical devices, which may use outdated OS or security technology.
5. Deploy user-behavior analytics. Is a doctor—at the hospital yesterday—trying to access data from Russia today? It may not be the doctor.
6. Analyze inbound and outbound traffic. Data can identify and stop attacks whose fingerprints have been identified elsewhere. A global analytics model helps find threats that are directed toward, or even coming from, your hospital.
7. Test the system regularly for vulnerabilities. This includes mock phishing exercises, penetration testing, social engineering, vulnerability scanning, etc.
8. Train your people. A strong security culture starts at the top. Training must be systematic and relevant. Make it a repeating fact of work life.
9. Manage your vendors and associates. They can be a key weak point, and you may be liable.
10. Create your breach response plan. Your network will be—or has been—breached. Actions taken after identifying the breach determine and limit the extent of the harm.



Understanding Your Clinicians' Data Needs

At Mission Health, a six-hospital system based in Asheville, N.C., President and CEO Ronald A. Paulus, MD, is both a physician and former software developer. So he has a keen understanding of how the needs of IT and clinicians can intersect, and how to make that intersection productive instead of adversarial. In 2014, he instituted a program called Walk a Mile in My Shoes that required administrators to shadow clinicians to better understand their operational challenges—not just around all cybersecurity, but all technology. Paulus even joined in, doing four-hour shifts in the ER. Seeing things close up, in real time, the tension between managing information and providing care was revealing.

"I was watching what people did and was thinking to myself, 'My Lord, this is crazy,'" he remembers. "I was standing beside a nurse and she was trying to interact with a patient. She had two screens open, and also a device, but she ended up writing things down on a napkin. What struck me was how hard it was to do so many simple things."

The Walk a Mile in My Shoes program addressed a common vulnerability in hospital security strategies: insufficient awareness of how doctors actually work, how they access data, and when and why they look for workarounds.

Charles Sawyer, MD, chief medical officer and a working internist at Mission Health, says that doctors today understand the security threat, but "At an emotional level, when we're trying to take care of patients and get through a busy day, security protocols look like a nuisance and a hassle."

Traditionally, IT departments regard risky but common behavior—such as sharing passwords or installing insecure apps—to be the result of ignorance or carelessness. Physicians, being human, aren't immune to either, but it's likely they're making many decisions based on medical expediency or a simple time crunch. "We've seen physicians share patient information through text—very scary to think about," says Sundaresan. "But I cannot stop you from sending text messages. So what I have to do as a security team is to give you an option to encrypt the message. Let me use a technical solution to help you address that challenge."

Bottom line: Make sure your security team understands how data and devices fit into a physician's work day. Examine workarounds or bad practices to understand their function. Don't assume laziness or malice. Shadowing doctors is one tactic. Another is to make doctors an active part of your security team. ■

A Day in the Life of a Doctor

Inadequate media policies

2:33 P.M.
Physician plugs USB stick from home into a hospital laptop.

THREAT
A virus that could have been planted on the USB stick from another machine now has a clear path into the hospital network. Also, misplacing a USB stick can be a significant breach of protected health information.

SOLUTION
Implement a removable-media policy (USB, memory card, CD/DVD, etc.) that covers proper acquisition, management and secure disposal of removable media. Prohibit unapproved media from operating in hospital systems.

Giving Doctors a Seat at the Table

Every night at 9 p.m. at Boston's Beth Israel Deaconess Medical Center, a systemwide malware and virus scan swept through all machines on the hospital's network. This was a necessary but process-intensive security procedure. Everything slowed during the scan. Reviewing medical records, placing lab orders and admitting patients became prohibitively slow. Doctors couldn't even dictate clinical notes into their transcription application.

Larry Nathanson, Director of Emergency Medical Informatics and a board-certified emergency medicine physician, recounts that a lot of ER physicians said that IT should refrain from scanning the ER computers at all, because the impact was too great. He worked with the doctors to find a compromise: Malware scans across the rest of the hospital would continue to occur nightly at 9 p.m., but scans for the emergency room would be moved to 4 a.m. so that patient care wouldn't be compromised. The lesson learned at BIDMC? "Painful security measures can't be something you impose on people or they're going to try to find ways to subvert them," Nathanson says.

Nathanson is a member of the Information Systems Steering Committee, which includes many physicians. The group gives all stakeholders an opportunity to interact and guide decisions about security and privacy policy. It revealed a new vulnerability: Doctors were documenting wounds and healing progress using smartphone cameras because it was a quick, convenient way to do so. But photos and video stored on phones can be lost or stolen, and cloud storage through a cell phone provider or app typically isn't protected by a HIPAA-mandated business associate agreement.

"When they take a picture of an X-ray," confirms AT&T's Terry Hect, Chief Security Strategist for AT&T Healthcare, "and they send it to their radiologist pal in Milwaukee—whose opinion they value—they are getting around all these controls." In other words, a physician, working inside the virtual walls of your secure network, can innocently push private patient data outside that network.

Recognizing their doctors' needs for photo sharing, BIDMC's IT department teamed up with clinicians to create a secure phone app called Photo Consult, which uploads photographs into the secure electronic medical record and deletes them from the phone.

Bottom line: Create formal systems and structures for physician involvement in security decisions. Collaboration does not happen automatically, especially when security has been traditionally the purview of IT, who may rarely interact with doctors in the context of their actual work. ■

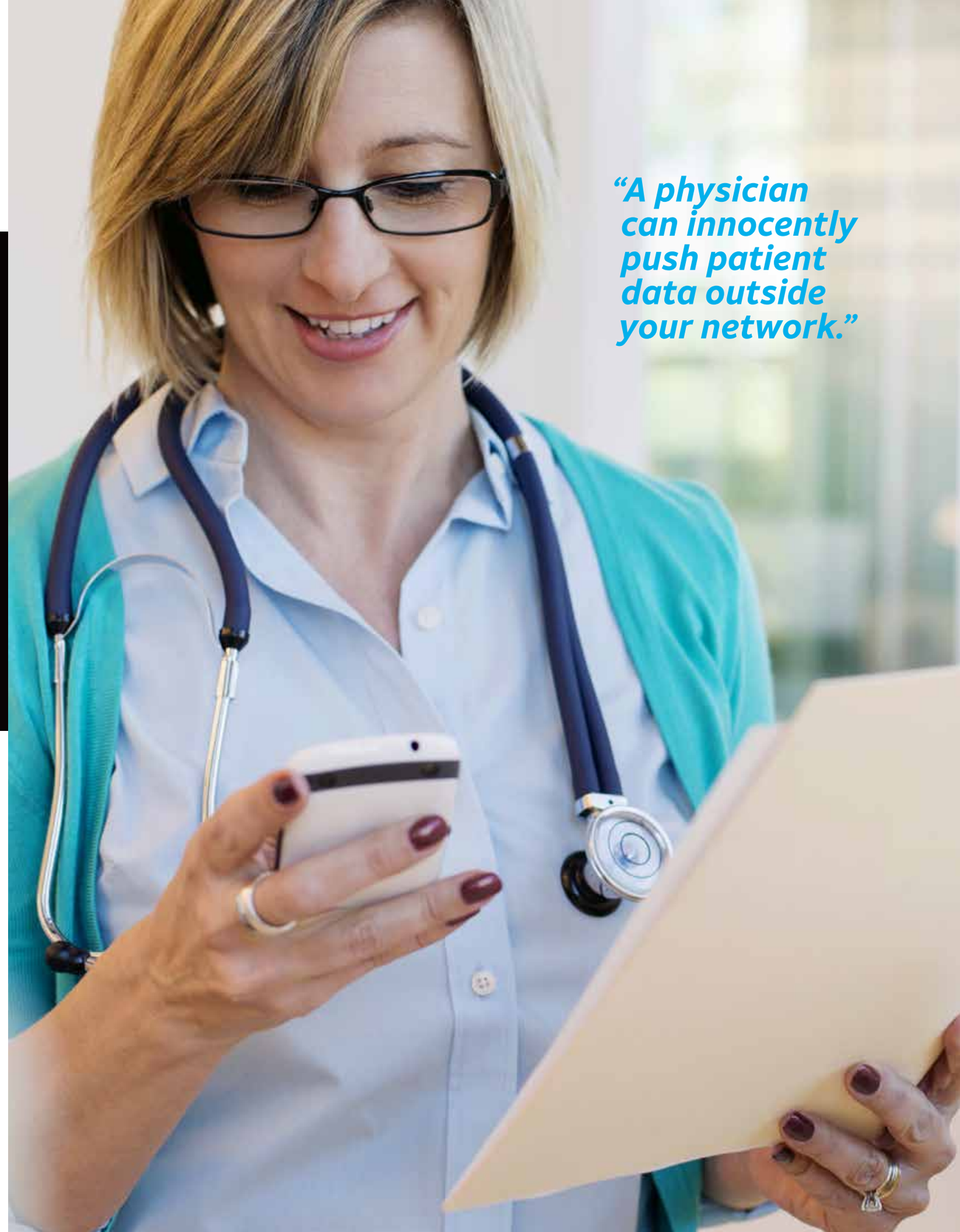
A Day in the Life of a Doctor

Low security awareness

3:18 P.M.
In a rush, doctor writes down new password to access hospital EHR database and passes it to a nurse.

THREAT
The password could be visible to anyone, or left behind—a violation of privacy standards that could lead to a significant fine. The physician could be held legally and financially responsible.

SOLUTION
Use two-factor authentication whenever possible to eliminate the possibility of shared passwords and password-hacking or guessing. Implement a comprehensive password policy that includes training about threats and consequences.



Securing Doctors Outside Your Walls

The number of third parties who must touch—or because of poor security can touch—patient data makes hospital security a vexing challenge. Advocate's $5.55 million record HIPAA settlement in 2016 related in part to its failure to "obtain satisfactory assurances in the form of a written business associate contract that its business associate would appropriately safeguard all ePHI in its possession." In the first eight months of 2016 alone, 30% of reported hospital breaches came in through third parties.[12] The offices of small private practices can present special risks.

To be HIPAA compliant, your organization will already have established rules for clinics to tie into your networks. Physicians' offices should conduct regular IT risk assessments. And securing your hospital's network will ensure that data flowing in and out—from associates and anywhere else—will be tracked. The question is whether relying on associate contracts and minding your own store is sufficient.

"I've seen cases where a doctor's high school-aged son was managing the IT infrastructure from his PC," says Axel Wirth, healthcare solutions architect with cybersecurity giant Symantec. "Especially among one- or two-physician practices, security seems like a luxury. This is why we are seeing smaller organizations move towards hosted or managed services to minimize their on-premises infrastructure—and exposure."

Financial pressures on small clinics exacerbate the problem. Clinics may do the bare minimum to meet HIPAA privacy requirements but miss gaping security holes. "Many [doctors' practices] purchased a HIPAA security manual online or from a salesman, but a lot of times the book sits on the shelf gathering dust," says Christopher Allman, Director of Risk Management, Compliance and Insurance at Garden City Hospital in Garden City, Mich., who frequently assists newly allied practices in conducting assessments. In such offices, HIPAA-mandated training often is lacking or non-existent. Simple risks—such as thumb drives left lying around—are commonplace.

"When you explain to physicians what you've found [after a risk assessment], they kind of get the deer-in-the-headlights look," Allman says. "But when you break down what it may cost them if they do have a breach, they generally get on board pretty quickly."

Bottom line: Looking beyond the boundaries of your enterprise is the only way to truly mitigate risk. Work with private practices to develop an action plan based on risk factors uncovered, and ensure that all groups make progress over time. The manpower for offering this guidance may not be accounted for in your staffing, and you need to be cognizant of Stark rules against providing financial assistance to physician practices. ■

A Day in the Life of a Doctor

Medical devices insecure

4:13 P.M.
Physician downloads data from patient's wireless medical device.

THREAT
If the link between the medical device and the tablet is unencrypted, hackers sniffing wireless signals could gain access to the device and modify it or shut it down.

SOLUTION
Require vendors to provide a secure, encrypted and authenticated link to all medical devices. Implement a Remote Access Policy that covers management of remote users, access methods and best security practices requirements.

12 Protenus, *4.5M Patient Records Breached Due To Third-Party Incidents*, September 20, 2016

Arming Doctors with Training and Education

A 2016 study found that 36% of healthcare organizations and 55% of business associates that have been breached point to unintentional actions by their employees as the cause. In November 2016 alone—a record month for breaches—54% were caused by employee error.[13]

Security, like proper hospital hygiene practices, won't become ingrained without training and education. This is a paradigm that clinicians—who must update their medical knowledge to maintain accreditation—understand. They will react to clear information about the risk and prevention of cyberattacks. This needs to move beyond introductory training sessions for new employees and partners to regular updates and refreshes.

"Physicians respond best when they understand why something is important, what the outcome could be and what the risks are. Then they become partners in the solution," says Julian M. Goldman, MD, an anesthesiologist at Massachusetts General Hospital.

At North Carolina's Mission Health, James Kelly, information security officer, says simulated phishing campaigns are proving effective at teaching clinicians about what risks look like in the real world. The campaigns, often administered by a third-party vendor, are sting operations that mimic real phishing attacks—emails from a colleague, a researcher, a billing company or even a daughter's soccer coach.

Doctors tend to be grateful for the lessons learned. "They understand that it could have led to a very, very bad outcome," Kelly says. "They may be a little frustrated, but it does create a new awareness."

Just as hospitals routinely run disaster drills, preparing for a bus crash or an earthquake, so too should they run IT-focused scenarios. What if the network went down for three hours? What if you were locked out of the EHR database during a ransomware attack?

A Day in the Life of a Doctor

Failure to encrypt

2:19 P.M.
Accidentally hits "reply all" to an email about a complex patient case.

THREAT
Unauthorized recipients see confidential protected health information.

SOLUTION
Automatically encrypt any email containing patient information. Put in place a secondary email application for emails containing patient information that validates the message's recipient.

Sharing news about incidents when they happen is also important. No department wants to go public with what looks like a failure, but the C-suite can support transparency by reminding everyone that breaches are as inevitable as any other kind of infection.

Bottom line: Hospitals have left themselves vulnerable to breaches because of a longstanding failure to train staff and partners. Training and regular updating are necessary because of the dynamic complexity of the healthcare environment. ■

13 Ponemon Institute, Sixth Annual Benchmark Study on Privacy and Security of Healthcare Data, 2016

CONCLUSION

Creating a Culture of Security

In a 2016 annual survey, 81% of healthcare CEOs expected cybersecurity threats against their organizations to increase in the coming year, and most planned "considerable" or "some" budget increases to combat those threats.[14] But money, scarce as it is, won't reduce vulnerabilities on its own. Leadership from the top is a critical factor if security investments are to truly reduce risks. Executives interviewed for this handbook all agreed that, for security to become an urgent priority among doctors and staff, leaders must demonstrate that urgency from the top. An end-to-end security approach must be implemented and then publicly championed by both the board and executive leadership.

When that happens, "It rolls downhill very well and people across the hospital are willing to listen," says Garden City Hospital's Christopher Allman.

Rich Miller, President and CEO of Marlton, N.J.-based Virtua, agrees: "We have 9,000 employees. In an organization this size, the journey to cybersecurity has to start with the CEO. I can't be afraid to go out and discuss the issue with employees and physicians."

In tight economic times, nothing says you're serious like a significant and touted reallocation of budget.

"The way you allocate resources is an indication of what your belief system is," says Ronald A. Paulus, MD, the physician-CEO at Mission Health.

"For security to be an urgent priority among doctors, you first have to demonstrate its importance to you."

Hospitals have had more than a century to develop and implement, with their physicians and staff, the basic protocols to prevent the spread of germs. Now they face a different sort of dangerous infection. They're operating in a cyber hot zone. Doctors can be trained for this sort of battle, but need to understand the pervasive nature of the threat. From understanding, training, investment and leadershtip come effective change.

14 Modern Healthcare, *Cybersecurity Rising as Health IT Concern*, February 27, 2016

For more information visit

att.com/healthcare